قابلیت های امنیتی ویندوز ۱۰

ترجمه و تدوین: اشکان پزشکی

خلاصه

در ویندوز ۱۰ ما شاهد تغییرات شگرفی در تمام زمینه ها بالاخص مباحث امینتی هستیم تفکر و برنامه ریزی فوق العاده ای برای ساخت ویندوز ۱۰ صرف شده است. تمام این انرژی در زمینه ایجاد اکوسیستمی امن برای شما ایجاد شده است. مایکروسافت زمان زیادی را در جهت توجه به موارد اعلام شده توسط مشتریان صرف کرده، ایجاد تنظیمات و تغییرات مثبت درسطح سیستم عامل در جهت رضایت کاربران صورت گرفته است.

استفاده از پارامترهای بیومتریک برای هویت سنجی اولین و شاید مهم ترین بخش برای سنجش هویت افراد و انجام آن به صورت بیومتریک است. ویژگی منحصر به فردی که امنیت را به صورت ایده آل برای شما عرضه می کند.

در قسمت شناسایی صورت با ویندوز Hello، مایکروسافت یکی از پیشروترین کمپانی ها در این زمینه می باشد تا امنیت بی نظیری را به مصرف کنندگان هدیه دهد.

در قسمت Device Guard ما ترکیبی از قابلیت های سخت افزاری و نرم افزاری را مشاهده می کنیم که جهت پیکربندی ترکیبی بین سخت افزار و نرم افزار اتفاق می افتد. وقتی Device Guard پیکربندی شد دستگاه قفل شده و فقط برنامه های مورد اطمینان اجرا خواهند شد.

در بخشی از کتاب ما با مایکروسافت آژور آشنا می شویم و میبینم که این سرویس چگونه در حال نفوذ بوده و چه راهکارهایی در جهت محافظت از کاربران برای استفاده از این سرویس مایکروسافت به وجود آمده است.

راهکارهای سازمانی در جهت استفاده مجزا از برنامه ها به طوری که برنامه های مربوط به سازمان رمزنگاری شده و برنامه های شخصی بدون رمزنگاری باقی می مانند همچنین به محض خروج دائمی کاربر از سازمان تمام اطلاعات Wipe شده و عملا هیچ گونه اطلاعاتی مربوط به سازمان در کامپیوتر کارمندان باقی نمی ماند.

قابلیت جدید ویندوز ۱۰ با نام Enterprise Data Protection – EDP –که توسط مایکروسافت ارائه شده است تجربه ی کاربری دلنشینی را برای ما به ارمغان آورده است. همزمان به شما کمک می نماید تا فعالیت های سازمانی خود را از فعالیت های شخصی کاملا تفکیک نمایید.EDP به سازمان ها کمک می کند

تا از برنامه ها و سرویس های خود در برابر سوء استفاده محافظت نمایند بدون اینکه از کاربر بخواهند تا تغییراتی را در سیستمی که با آن کار میکند اعمال نماید.

تا زمانی که کامپیوترها با قفل های نرم افزاری قدیمی کار میکنند هکرها در تلاش هستند تا از این قفل ها عبور نمایند. با ویندوز ۱۰ مایکروسافت این معضل را به بهترین شکل ممکن مرتفع ساخت تا شما با استفاده از حداقل های سخت افزاری و نرم افزاری بیشترین امنیت را برای خود فراهم نمایید.

امیداورم این کتاب به اندازه کافی مورد توجه شما قرار بگیرد و از خواندن آن لذت ببرید.

اگر نقطه نظرات و اشکالات و ایرادات وارده در مورد این کتاب را با ایمیل Ashkanp@Live.com برای بنده ارسال بفرمایید قطعا موجبات خوشحالی اینجانب را فراهم خواهید ساخت. مسلما حمایت های شما سبب قوت قلب و ایجاد انگیزه در جهت نشر مطالب بیشتر خواهد شد.

اشکان پزشکی

مهرماه ۱۳۹۵

معرفی قابلیت های امنیتی ویندوز ۱۰

برای کاربران کامپیوتر موضوعات مرتبط با امنیت همیشه یک دغدغه پر رنگ بوده است. کما اینکه در طول چند دهه ی گذشته شمار تهدیدات امنیتی به شدت افزایش یافته است.

درست زمانی که شما فکر می کنید بهترین سیستم امنیتی را برای کامپیوتر خود فراهم نموده اید متوجه می شوید که هیچ کاری انجام نداده اید. چرا؟ به خاطر اینکه چشم انداز تهدیدات سایبری به سرعت در حال تغییر بوده و نرم افزارهای امنیتی پیرامون شما کاملا معمولی هستند.

خرید یک سیستم امنیتی جدید برای کامپیوتر شخصی شما در کوتاه ترین زمان ممکن امکان پذیر می باشد. ولی به این نکته توجه بفرمایید که آپدیت های امنیتی بسیار مهم و ضروری هستند.

تهدیدات سایبری هر روزه پیچیده تر شده و حملات بیشتر، جنبه حیله گرا به خود گرفته اند. برای مثال ویروس ها و Malware ها توانایی های جدیدی برای مخفی و ناشناس ماندن پیدا کرده اند.

حملات سایبری در مقایسه با چندین سال قبل دقیقا زمانی که هکرها آرزو داشتند خرابی های سطحی و معمولی ایجاد نمایند بسیار پیچده تر و هدفمندتر شده اند.

امروزه دسته های خرابکارانه ای همانند کلیک های تقلبی و دزدان ID ها فعالیت های خود را به جهت رسیدن به سودهای غیرقانونی ادامه می دهند. ما فعالیت هایی را در گروه های اینترنتی مخرب مشاهده می کنیم که هدف آنها ایجاد اختلال در ارتباطات می باشد همچنین در سطوح پایین تر دزیدن مدارک شناسایی جزئی از این ناهنجاری ها است.

در این چشم انداز وحشتناک، مایکروسافت به چالش جدیدی جهت حفاظت از کاربران کامپیوترها قدم گذاشته است. با ویندوز ۱۰ ، سطوح بی سابقه ای از امنیت به صورت یکپارچه در داخل سیستم عامل قرار گرفته است.

هدف من از تحریر این کتاب نگاه اجمالی به امنیت داخلی ویندوز ۱۰ بود تا با امکانات و کارکرد آنها آشنا شویم.

پیوستگی بین Microsoft و FIDO

واژه FIDO (Fast Identity Online) معاهده ای می باشد که در سال ۲۰۱۲ شکل گرفت. راهی برای ایجاد همکاری متقابل بین احراز هویت مستحکم دستگاه ها و مشکلاتی که کاربران در به خاطر سپردن کلمات کاربری و کلمه های عبور خود دارند.

شرکت های PayPal و Lenovo، دو نام بزرگ در این صنعت می باشند که از اعضای FIDO می باشند. یک سال بعد از شروع اسم های بزرگ زیادی به این معاهده پیوستن بعضی از این شرکت ها شامل Google، Blackberry،Visa و Microsoft می باشند.

بنابراین معاهده FIDO چه نقشی در ویندوز ۱۰ مایکروسافت خواهد داشت ؟

برای رسیدن به این پرسش، ما باید چند مرحله به عقب بازگردیم، که چرا مایکروسافت تصمیم گرفت به این معاهده بپیوندد؟

مشکلات امنیتی دستگاه های ما در حال افزایش روز افزون می باشد، قسمتی از این مشکلات به خاطر حملات malicious بوده و قسمتی هم به خاطر نوع رفتار کاربران با این حملات می باشد.

زیاد دیده شده کلمات عبوری که شکسته شده اند. کاربران کامپیوتر اغلب دچار یک بی نظمی و سهل انگاری بوده و رمزهای عبور خود را با یکدیگر به اشتراک می گذارند.

اگر چه این تنها مشکل نبوده و قسمت دیگر این پازل وب سایت هایی هستند که ما از آنها بازدید می کنیم. موضوع فقط ناامن بودن این وب سایت ها نیست بلکه بیشتر آنها کاملا امن می باشند. این درست است که ژن تنبلی ما ظهور کرده و یک کلمه عبور یکسان برای استفاده در تمام وب سایت ها انتخاب می نماییم.

چرا ما این کار را انجام می دهیم؟

به این خاطر که انتخاب کلمه عبور پیچیده برای هر وب سایت سبب صرف زمان شده و ما باید همه ی این کلمات عبور را به خاطر بسپریم. مغز انسان توانایی دارد اطلاعات زیادی را نگهداری و این اطلاعات را در مواقع حساس به یاد آورد. وجود پسوردهای متعدد باعث می شود که ما آنها را یادداشت کرده که همین امر باعث در هم ریختگی و کاهش شدید امنیت می شود.

وقتی ما برای تمام سایت ها از یک نام کاربری استفاده می نماییم مسلما شرایط بسیار سهل و ساده ای ایجاد می نماییم برای کسانی که درصدد دزدن اطلاعات ما هستند. حمله کنندگان مخرب به سراغ سایت هایی می روند که از لحاظ امنیتی ضعیف بوده و به راحتی قابلیت هک شدن را دارند در این صورت جزئیات اطلاعات شما به راحتی فاش می شود از این مرحله به بعد دیگر نیاز به نبوغ خاصی جهت حدس زدن اینکه شما در چندین و چند سایت دیگر با همین نام کاربری و کلمه ورود استفاده کردیده اید نمی باشد!

شما ناخواسته به آنها یک کلمه عبور باز داده اید، یک کلید اصلی که به همه چیز دسترسی دارند.

تکه نهایی این پازل، دستگاهی است که شما از آن استفاده می نمایید. منظور خوب یا بد بودن دستگاه نمی باشد. یعنی تا وقتی که دستگاه شما وجود دارد هر برنامه ای می توان بر روی آن اجرا کرد، بدون در نظر گرفتن محتوای برنامه اجرا شده.

در شرایطی یک برنامه نمی تواند اجرا شود که فایروال و یا آنتی ویروس آنرا مخرب شناسایی کرده و از چرخه اجرا حذفش نمایند. وقتی شما آنتی ویروس بر روی سیستم نصب نکرده اید و یا از راهکارهای ارائه شده توسط مایکروسافت بر روی ویندوز استفاده نمی نمایند. معنی این جمله آن است که بدافزارها در شبکه افزایش پیدا کرده و متوقف ساختن آنها بسیار مشکل می شود.

چگونه مایکروسافت تصمیم دارد این مشکل شایع را حل نماید؟ PKI ها (Public Key Infrastructure) در حال حاضر بسیار گران بوده و پیچیدگی های خاص خودشان را در نگهداری دارند و در بیشتر موارد مورد حملات مختلف قرار می گیرند. در حال حاضر CA ها (Certificate Authority) هم مورد حملات مخرب قرار می گیرند.

یک مهاجم می تواند قبل از اینکه شما توکن خود را از IDP (Identity Provider) بگیرید اطلاعات مربوط به Certificate شما را بدست آورد. اگر این مرحله کافی نباشد، به صورت محدود شده از

MFA (Multi-Factor Authentication) جهت بدست آوردن نقاط ضعف استفاده میکند.

در ویندوز ۱۰، مایکروسافت شرایط آسان تری جهت لاگین ایجاد کرده و این در حالی است که امنیت بیشتری با استفاده از MFA به وجود آمده است.

با ترکیب بایومتریک ها، PIN های دسترسی و tying asymmetrical key pairs برای دستگاه های خاص، هدف مایکروسافت این است که هیچ کسی به جز شما نتواند به منابع و برنامه ها دسترسی داشته باشد.

با ویندوز ۱۰، مایکروسافت نسل جدیدی از اعتبارسنجی کاربران را به بازار عرضه کرد.

ما در این کتاب یک به یک این موارد را مشاهده خواهیم کرد.

نگاهی به ویندوز ۷ و ویندوز ۱۰ و ۸ قابلیت امنیتی جدید

به دلایل بسیار زیادی مایکروسافت در ویندوز ۱۰ رویکردهای جدید امنیتی ارئه کرده است.

اول: مشکلات امنیتی و چالش ها با سرعت بسیار زیادی در حال تکامل می باشند و کاملا مشخص است که این چالش ها باید حل شده و برای کاربران شفاف شوند.

کاملا واضح است که برخی از این چالش پیچیده تر از ویندوز۷ و ۸ می باشند و نیاز مبرمی جهت حل و فصل دارند.

یک بازدید سطحی و گذرا به جدول زیر، تفاوت های اساسی امنیتی بین ویندوز ۷ و ۱۰ را برای شما نمایان می سازد.

وظایف	ویندوز ۷	ویندوز ۱۰
حفاظت از هویت Identity protection	سرقت کلمات عبور امری عادی و معمول می باشد. در حال حاضر راه حل چند منظوره Multi-Factor خیلی گران و سخت جهت پیاده سازی می باشد.	راه حل چند منظوره Multi-Factor برای راه اندازی بسیار آسان بوده و با قابلیت هایی مثل anti-phishing و anti-thief سازگار می باشد. حفاظت از پسوردها و PIN ها شامل این راه حل است.
حفاظت از دیتا	ارائه دهنده گزینه های قابل تنظیم ازجمله رمزگذاری دیسک اما قابلیت DLP را ندارد. از نرم افزارهای جانبی می توان استفاده کرد و نمی توان انتظارات مثبتی داشت.	پیشرو در جهت رمزگذاری دیسک ها با قابلیت مدیریت کامل به همراه دریافت آپدیت های امنیتی. جداسازی دیتاها و کاملا با DLP ترکیب شده است.
تهدیدات مقاوم Threat Resistance	برنامه ها همیشه مورد اعتماد هستند مگر زمانی که یک تهدید شناخته شوند به خاطر بسپاریم که راهی برای شناسایی صدها هزار تهدید امنیتی جدید موجود نمی باشد.	دیسکتاپ ماشین ها می توانند توسط گوشی های موبایل مان قفل شوند. این قابلیتی می باشد که ما میتوانیم بعضی از برنامه ها را اجرا کرده و بعضی دیگر را نا امن بدانیم و از اجرایشان جلوگیری کنیم
امنیت دستگاه	پلتفرم به صورت امن ساخته شده است اما نرم افزارهای ایجاد شده بر روی آن قابلیت این را دارند که malwareها درون آنها مخفی شده و تهدیدات امنیتی بوجود آورند	پلتفرم ساخته شده با سخت افزار و نرم افزار تجمیع شده و لایه های حفاظتی از زمانی که دستگاه روشن می باشد شروع شده و تا خاموش شدن دستگاه ادامه دارد

مایکروسافت نگاهی جامع به امنیت دارد و تصمیمات جدی جهت رفع بسیاری از چالش های امنیتی گرفته است. با ویندوز ۱۰ طیف گسترده ای از راهکارهای امنیتی پیاده سازی می شود که از نرم افزارها و سخت افزارها محافظت می کند.

- **Windows Hello & Windows Passport handle ID**
- **BitLocker & Enterprise Data Protection**
- **Device Guard & Windows Defender protect**
- **UEFI Secure Boot, TPM 2.0**

باید نگاه عمیق تری به تمام این قابلیت ها داشته باشیم.

چگونه ویندوز ۱۰ از هویت شما محافظت می کند

اولین فاکتور، حفاظت از هویت است. سرقت هویت Identity یکی از نگرانی های عمده ی کاربران کامپیوتر می باشد.

هر روز داستان های جدیدی در مورد افرادی می شنویم که هویت آنها به سرقت رفته و از آن در جهت ارتکاب جرم و تقلب استفاده شده است. این وضع برای بسیاری از کاربران غیرقابل تحمل است. ویندوز ۱۰ دست به اقدامی زد تا کاربران با خیالی آسوده از کامپیوتر خود استفاده کرده و احساس امنیت زیادی داشته باشند.

ویندوز۱۰ – حفاظت از هویت شما و کنترل دسترسی ها

موضوع بعدی برای بحث راه حل جدیدی است تا از هویت افراد محافظت شود. راه حلی که روش های کهنه و قدیمی احراز هویت مانند کلمه عبور را کنار می گذارد. این راه حل حافظ شماست در زمانی که قرار است رخنه ای در دیتاسنترتان رخ دهد.

اگر دستگاه شما در خطرباشد و توسط حملات phishing مورد آسیب قرار گیرد از دیتاهای شما محافظت می شود. وقتی اقدام به ثبت نام در سیستم می نمایید، دستگاه شما به یکی از دو فاکتوری که نیاز دارد تا احراز هویت انجام پذیرد تبدیل می شود. Pin Number و یا بایومتریک اطلاعاتی همانند اثرانگشت.

سیستم های Windows Hello و Windows Passport دو سیستمی می باشند که در جهت حفظ و حراست از هویت کاربران با یکدیگر تعامل دارند.

برویم تا کمی عمیق تر و ریشه ای تر به این دو سیستم نگاه کنیم.

این راه حل امنیتی مزایای زیادی برای مصرف کنندگان و کاربران تجاری دارد. راحتی استفاده از یک پسورد را برای شما به ارمغان می آورد بدون اینکه در تمام مدت دغدغه ی فراموش کردن پسورد و یا به خاطر سپردن آنرا داشته باشید. مایکروسافت امنیت را در سطحی کاملا جدید و با استفاده از احراز هویت چند فاکتوره Multi Factor Authentication برای مصرف کنندگان ایجاد کرده تا هویت آنها حفظ شود.

اجازه دهید نگاهی داشته باشیم به سیستم انتخابی مایکروسافت و چرا ما باید این سیستم ها را مورد استفاده قرار دهیم. اولین، بیومتریک است. دقیقا این کلمه به چه معنی می باشد؟ بیومتریک ها بررسی ویژگی های بیولوژیکی هستند که می توانند مورد آزمایش و اندازه گیری قرار بگیرند. در امنیت کامپیوترها، بیومتریک ها ابزاری هستند تا امکان هک شدن سیستم ها را سخت تر نمایند و در مقایسه با سیستم های حفاظتی قدیمی همانند پسوردها بسیار موفق بوده اند.

در این مثال بیومتریک ها به مشخصه های فیزیکی گفته می شوند که به راحتی قابلیت چک شدن را داشته و در برابر اطلاعاتی که در سیستم ذخیره می شوند. تعدادی از روش های احراز هویت که توسط بیومتریک ها مورد استفاده قرار می گیرند:

صورت: تجزیه و تحلیل مشخصات صورت های متفاوت

اثرانگشت: تجزیه و تحلیل اثر انگشت هر شخص

هندسه دست: شکل دست و طول انگشتان

شبکیه چشم: تجزیه و تحلیل عروق مویرگی پشت چشم

عنبیه چشم: تجزیه و تحلیل حلقه رنگی اطراف مردمک چشم

امضاء: چگونگی امضا یک فرد

رگ های خون: الگوری قرارگیری رگ ها در پشت یک دست و پا

صدا: تن و زیر و بمی صدا و فرکانس صدای افراد

بیومتریک ها به طور نسبی در حال توسعه می باشند. اما باید توجه داشت که این توسعه با سرعت چشم گیری در حال انجام است و به زودی به یکی از المان های اصلی تامین امنیت در سیستم های کامپیوتری تبدیل می شوند.

جوانب مثبت و منفی بیومتریک ها:

هر مدلی از احراز هویت بیومتریک دارای معایب و مزایایی می باشد. با توجه به اینکه مایکروسافت اهمیت خاصی به این نوع از احراز هویت می دهد بهتر است مروری بر روی این مدل از تکنولوژی های امنیتی داشته باشیم.

استدلالی که برای استفاده از احراز هویت به صورت بیومتریک وجود دارد بر سه محور کلیدی قرار گرفته است. اولین و شاید مهم ترین بخش برای سنجش هویت افراد انجام آن به صورت بیومتریک است. ویژگی منحصر به فردی که امنیت را به صورت ایده آل برای شما عرض می کند.

دومین استدلال برای استفاده از احراز هویت بیومتریک آن است که دیگر نیازی نیست کاربران رمزهای طولانی و سخت را به خاطرسپرده و یا با دوستان خود به اشتراک بگذارند. رمزهای عبور کاهش پیدا کرده و استرس های ناشی از فراموش شدن و یا هک شدن با احراز هویت بیومتریک از بین می رود.

سومین استدلال، همان گونه که میدانیم شبیه سازی مشخصات بیومتریک فوق العاده سخت و تقریبا غیرممکن می باشد همین امر سبب میشود بدون چون و چرا این گونه احراز هویت را بپذیریم. در حالی که توکن و یا پسورد احتمال لو رفتن و یا دزده شدن را دارد.

استدلال هایی هم برای عدم استفاده از خصوصیات بیومتریک وجود دارد که نشان دادن و ثابت کردن این استدلال ها در بسیاری از حوزه ها بحث برانگیز می باشد. اولین و مهم ترین دلیل گران بودن پیاده سازی این نوع احراز هویت می باشد. وقتی بحث هزینه مطرح می شود بسیاری از سازمان از عهده این امر بر نمی آیند و عملا پروژه را مختومه اعلام می کنند.

هزینه خرید، نصب و پیاده سازی تجهیزات سخت افزاری و نرم افزاری بیومتریک بسیار گران و گزاف می باشد. همچنین در این نوع احراز هویت ما هزینه های پنهانی همچون یکپارچه سازی با سیستم های موجود خواهیم داشت.

با وجود تمام استدلال های موجود، سیستم های بیومتریک تنها برای شبکه های ساده مناسب می باشند. بعضی از تفکرات به منطق فکری همه یا هیچ اعتقاد دارند.

همه یا هیچ به این معنی می باشد که شما تجهیزات گران قیمت احراز هویت بیومتریک خود را روی هر کامپیوتری در شبکه نصب می کنید اما هیچ چیز حساب می شود! زیرا اگر کاربران از راه دور به این سیستم دسترسی داشته باشند پس عملا این هزینه برای سیستم بیومتریک به هیچ تبدیل می شود!! به عبارت ساده تر تجهیزات گران قیمت بیومتریک فقط برای دسترسی های فیزیکی و اینتراکتیو مناسب و بهینه می باشد.

استدلال دیگری که به مبارزه با سیستم های بیومتریک برخواسته است ذخیره سازی اطلاعات بیومتریک کاربران را تجاوز به حریم خصوصی آنها می داند. در سطوح بالاتر بحث بر سر آن است که اگر اطلاعات بیومتریک کاربر لو برود کل زندگی شخص را تحت الشعاع قرار می دهد و طیف وسیعی از فعالیت های غیرقانونی را شامل می شود.

در بیومتریک قابلیت به روزرسانی و تخریب خودش وجود ندارد. اگر اطلاعات شخصی بیومتریک مورد تهدید قرار بگیرد، یک موضوع ساده و پیش پا افتاده نیست و امکان صدور دیتای جدید وجود ندارد حداقل می توان گفت به راحتی و آسانی انجام نخواهد شد.

با توجه به تمام جنجال ها و تفسیرهای مثبت و منفی که حول و هوش استفاده از سیستم های بیومتریک صورت گرفته است مایکروسافت تصمیم نهایی خود برای این استفاده از این سیستم ها را گرفته است.

سادگی پاسخ قابلیت اطمینان آن است. عواقب داشتن یک سیستم کهنه که از متدهای قدیمی و منسوخ شده جهت محافظت دیتاها بکار برده می شود خیلی زیاد بوده و احتمال صدمه دیدن اطلاعات و دیتا بسیار زیاد

است. بسیاری از نرم افزارهایی که ما روزانه از آنها استفاده می نماییم از روش های قدیمی و کهنه جهت احراز هویت استفاده می نمایند.

تا آنجا که به مایکروسافت مربوط می شود، بوسیله ی احراز هویت های بیومتریکی که در ویندوز ۱۰ قرار داده شده است، شما می توانید تمام دسترسی های لازم را بر روی اکانت های خود و اپلیکشن ها داشته باشید- نیازی ندارید تا برای هر برنامه یک کلمه عبور به خاطر بسپارید .

ممکن است پسوردها مورد سرقت قرار بگیرند، اما اطلاعات بیومتریک چنین نخواهند بود. بعلاوه اطلاعات بیومتریک برای افراد جنبه های مثبتی دارند. مثلا یک کارت اعتباری بدون حضور شما نیزمورد استفاده قرار خواهد گرفت اما در مورد سیستم های بیومتریک چنین اتفاقی نخواهد افتاد و حضور شما الزامی می باشد.

ویندوز ۱۰ قابلیت های احراز هویت بیومتریک را به صورت کاملا مدرن برای شما پیاده سازی می نماید به طوری که کاربران به سادگی می توانند دستگاه را از حالت قفل Lock خارج نمایند. این روش بسیار ساده و مطمئن تر از وارد کردن کلمات عبور پیچیده می باشد. این قابلیت کاملا رایگان می باشد.

اینترنت مکانی نا امن بوده و بسیاری از کاربران خواهان برقراری امنیت در این شبکه بزرگ می باشند و این امنیت در شرایطی حاصل می شود که هویت سنجی ها مطلوب تر از حال حاضر صورت پذیرد و تجربیاتی از اطمینان بدست آید.

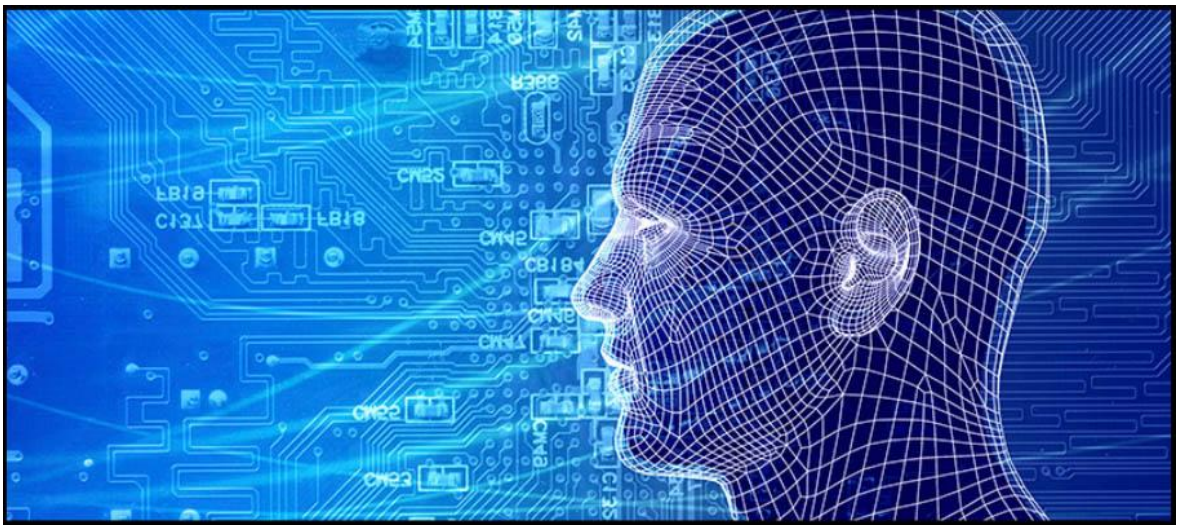
آنها خواهان سیستم امن هستند; یک سیستمی که کلمات عبور را به امان خدا نمی گذارد تا هرکسی هرکاری که دوست داشت انجام دهد! با ویندوز ۱۰ ما تجربه ای شیرین از اهدافی خواهیم داشت که مدت ها به دنبال آنها بودیم:

- هم مشتریان و هم کاربران خاص (یوزرهای پیشرفته) قادر هستند دستگاه های خود را باز کرده و پرداخت ها و محتوای کاری آنها امن باشد. تمام این موارد بدون استفاده از پسورد و در یک کانال امن اتفاق می افتد.
- راه حل های سخت افزاری توسعه داده شده که با حداقل تغییرات به وقوع پیوسته اند. انتظارات مشتریان این است که سخت افزارها قوی بوده و ساده سازی لازم جهت استفاده در آنها صورت پذیرفته باشد.
- ارائه دستگاه های جدید و خلاقانه بر اساس نیازها و توانایی های مشتری

ویندوز۱۰ برای رسیدن به این اهداف مدت ها است که در حال توسعه می باشد تا از یک دامنه ای گسترده از بیومتریک ها، اثرانگشت ها و ... که بنا به توانایی کاربر مناسب او می باشد مورد استفاده و بهره برداری قرار گیرد. برای احراز هویت بیومتریک سخت افزارهای ویژه مورد نیاز است که منفعت های ذیل را به همراه دارند:

- لاگین شدن بسیار آسان و راحت بوده و احراز هویت بسیار امن و مطمئن می باشد.
- سطوح امنیتی پیشرفته با دسترسی به منابع مورد نظر

در ضمن، ویندوز ۱۰ راهکار احراز هویت با چهره را پشتیبانی می نماید که این روش بدون استفاده از نرم افزارهای جانبی صورت میگیرد البته باید توجه داشته باشید که سخت افزار مورد نیاز باید وجود داشته باشد.



هویت سنجی با استفاده از صورت

ویندوز ۱۰ سطوح جدیدی از تشخیص چهره را به ارمغان آورده است. سیستمی که به راحتی هویت سنجی کرده و دستگاه ویندوزی را از حالت قفل خارج تا به آن دسترسی داشته باشیم.

تمام مراحل بالا بدون نیاز به استفاده از پسورد و یا هر گونه روش های احراز هویت قدیمی صورت می گیرد.

مزایا:

هویت سنجی با استفاده از تشخیص چهره در ویندوز ۱۰ مزایای زیر را به همراه دارد:

- یک اینترفیس کاملا جذاب و کاربرپسند، با قابلیت هایی برای فراهم نمودن SSO. هیچ نیازی برای استفاده از پسورد و یا هرگونه Authentication دیگری وجود ندارد.
- احراز هویت با درجه ی پیشرفته و کامل
- برطرف کردن مشکل حملات فیزیکی، در نظر داشته باشید که هیچکس توانایی لاگین کردن با سیستم شما را ندارد.
- استفاده از اشعه مادون قرمز که توانایی ایجاد تصویر واضح و مشخص را بوجود می آورد. این تکنولوژی سبب می شود در موقعیت های نوری متفاوت هم با تصاویر واضحی مواجه شویم. این سیستم با اضافه شدن و یا کم شدن موهای سر و یا تغییر در فریم عینک و آرایش صورت هیچ مشکلی نداشته و در تمامی شرایط شناسایی را به بهترین نحو انجام می دهد.

استفاده موردی

سه مورد استفاده اصلی برای شناسایی به وسیله صورت وجود دارد:

۱- در هنگام احراز هویت نیازمند لاگین شدن یا قفل شدن سیستم می باشیم.

به طور متوسط در کمتر از دو ثانیه سیستم صورت شما را می شناسد اگرچه ممکن است این فرآیند تا بیست ثانیه هم طول بکشد. اما می توانید مطمئن باشید که بیشتر از این زمان معطل نخواهید شد.

۲- احراز هویت برای خرید

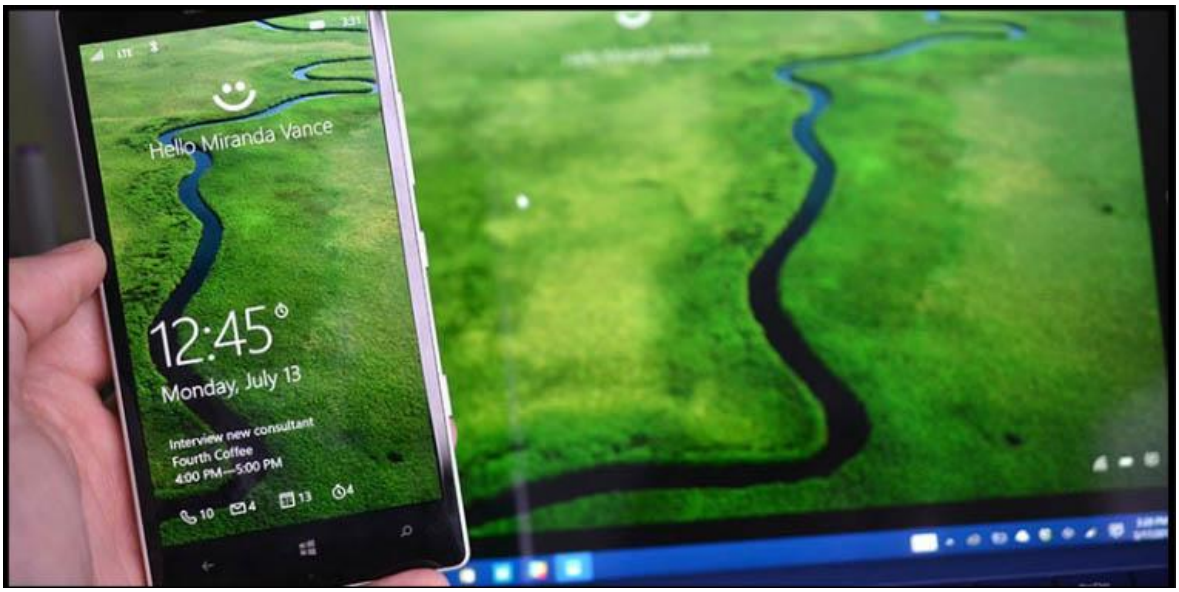
به طور متوسط در کمتر از دو ثانیه سیستم صورت شما را شناسایی می کند. اما ممکن است تا بیست ثانیه هم طول بکشد .این امر الزامی می باشد تا هر برنامه ای که نیاز به احراز هویت دارد کاربر مجدد اقدام به هویت سنجی نماید.

۳- حضور

مدت زمان شناسایی بین ۱,۵ تا ۳۰ ثانیه می باشد اگر چه ممکن است بیشتر طول بکشد. انتظار می رود با استفاده از API های جدید و برنامه هایی که در آینده از سنسورهای شناسایی استفاده خواهند کرد روند دفعات استفاده کاهش پیدا کند. اگر شخص حضور داشته باشد هویت سنجی خواهد شد در غیر اینصورت با کاربر میهمان و دسترسی های مشخص وارد خواهد شد.

حال وقت آن است که کمی در مورد تشخیص چهره مایکروسافت و مکانیزم های کارکرد آن صحبت کنیم.

ویندوز Hello



احراز هویت بیومتریک توسط Windows Hello صورت می گیرد و اجازه دسترسی بدون وقفه و سریع به تمام دستگاه هایی که ویندوز۱۰ بر روی آنها نصب شده را می دهد. به این نکته باید توجه داشت که نوع دستگاه فرقی نمیکند خواه دیسکتاپ باشد خواه موبایل.

تلاش های بیهوده و عبث برای به خاطر سپردن کلمات عبور طولانی و سخت را فراموش کنید با Windows Hello مایکروسافت شما کافی است به وب کم نگاه کرده و یا با استفاده از اثرانگشت به سرعت به هدف خود برسید و اجازه دسترسی را پیدا نمایید.

این روش بسیار راحت تر و امن تر از روش های قدیمی وارد کردن پسورد به صورت دستی می باشد.

ویندوز۱۰ سیستم جدیدی را معرفی کرده که اجازه ی دسترسی به محتویات سازمان یا شرکت شما را می دهد بدون اینکه پسوردی را ذخیره کرده باشید.

Windows Hello با شناسایی صورت، عنبیه و یا اثرانگشت شما کار می کند. (شما نیاز دارید یک وب کم متناسب با این تکنولوژی داشته باشید و یک سنسور اثرانگشت همین وبس). پس از اجرا، فقط شما قابلیت دسترسی به برنامه های ویندوز ۱۰، وب سایت ها و دیتاهای موجود را بدست می آورید. این قابلیت ها توسط یک سری از سنسورهای مدرن تعبیه شده در دستگاه اتفاق می افتد که با توجه به تنظیمات سفارشی شده این سنسورها فقط شخص شما را می شناسد.

اگر دستگاه شما سنسور Realsense با برند Intel دارد که سازگاری لازم با سنسورهای اثرانگشت و دوربین دارد. فقط کافی است دستگاه را به یکی از نسخه های ویندوز ۱۰ آپدیت کنید تا با دنیای زیبای Windows Hello آشنا شوید.

برای تشخیص چهره و شناسایی کاربر، Windows Hello از برنامه و سخت افزار خاصی استفاده می کند. برای مثال اگر شخصی عکسی از چهره ی شما را در مقابل این تکنولوژی قرار دهد کار نخواهد کرد.

Intel RealSense این توانایی را به دوربین ها میدهد تا از تکنولوژی مادون قرمز استفاده نموده و در نتیجه یک سری عکس خوب ۳D از چهره ی شما بدست می آید. این عکس ها فقط برای این که شما از دیدن چهره ی زیبای خود لذت ببرید نمی باشند!! باید کمی به عمق قضیه رجوع کنیم و یاد ضرب المثل معروف تو مو بینی و من پیچیش مو بیفتیم!

دوربین ها بسیار قابل اعتماد و پایدار طراحی شده اند و در بازه های مختلف نوری توانایی شناسایی چهره ها را دارند.

Windows Hello راهکاری می باشد که فقط توسط مصرف کنندگان مورد استفاده قرار نمیگیرد و در صنایع دفاعی، دولت ها، سازمان های سلامت، سازمان های مالی و قسمت ها و سازمان هایی که به امنیت اهمیت می دهند مورد استفاده قرار میگیرد.

قابلیت های جدید امنیتی در ویندزو ۱۰

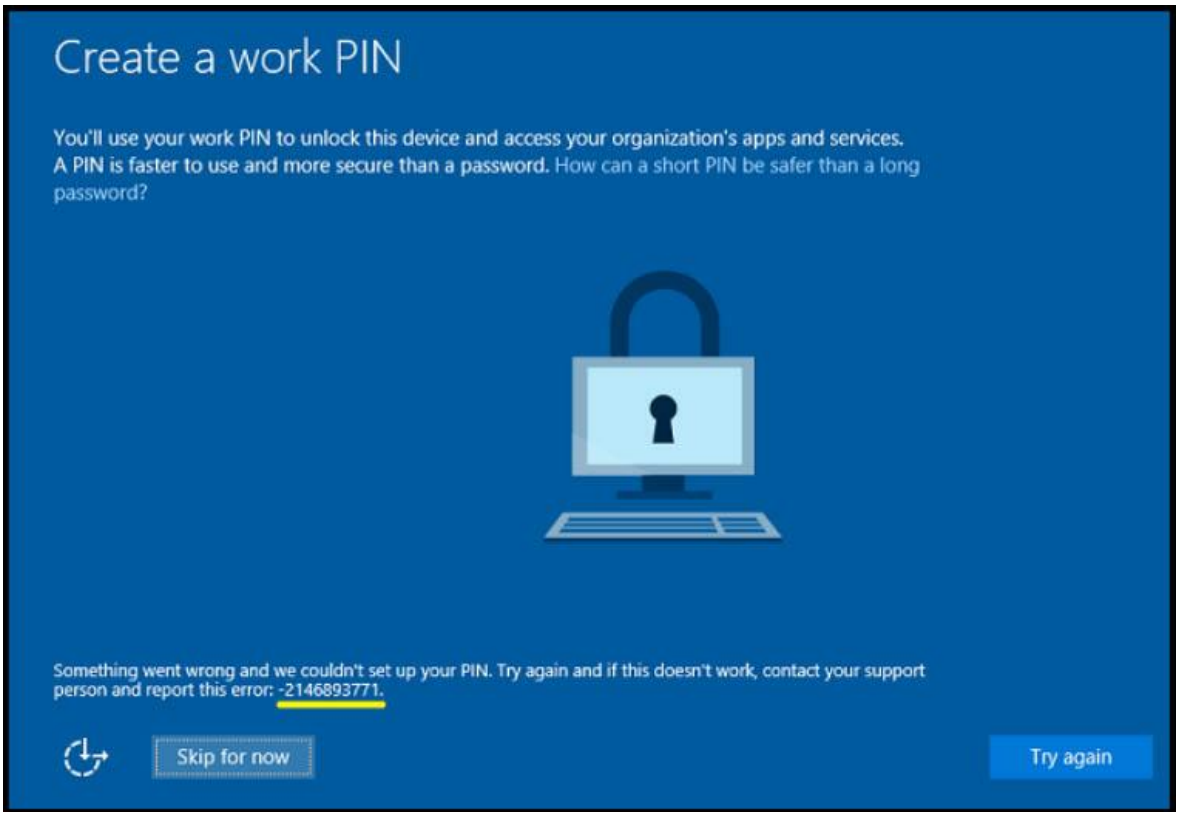
در ادامه بعضی از قابلیت های جدید و هیجان انگیز ویندوز ۱۰ را بیان خواهیم کرد.

Microsoft Passport

Windows Hello تمام داستان ما نیست. مایکروسافت قابلیت Microsoft Passport را نیز معرفی کرده است.

Passport برای دوری کردن (از بین بردن) کلمه عبور Password طراحی شده است. به مدیران IT، نویسندگان وب سایت ها و توسعه دهندگان وب اجازه می دهد راهکارهای امنیتی بیشتری جهت وارد شدن به برنامه ها و سایت هایشان داشته باشند.

به جای استفاده از روش های قدیمی و از رده خارج جهت وارد کردن پسورد ویندوز Passport طراحی شده است تا امنیت کاملا تضمین شود. احراز هویت و شناسایی شما در وب سایت ها، برنامه ها و شبکه بدون نیاز به ذخیره سازی پسوردها صورت می گیرد. و همین امر سبب می شود تهدیدات امنیتی و هک ها به حداقل مقدار خود برسد.



ویندوز ۱۰ پسورد سیستم را با یک کلید خصوصی یا PIN جایگیزین کرده است. این PIN به شما اجازه می دهد تا به دیتاهای شخصی یا سازمانی خود دسترسی داشته باشید. این PIN با دستگاه شما لینک شده و فقط با دستگاه شما کار میکند.و بدون این PIN دیوایس هیچ ارزشی ندارد!

اگر سعی کنید که با این PIN به یک دستگاه دیگر متصل شوید، از ورود شما جلوگیری خواهد شد. بدیهی است که جهت استفاده از منابع و اطلاعات یک دستگاه باید PIN جدیدی تولید شود. برای هر دستگاه باید یک PIN تولید شود.

چرا مایکروسافت استفاده از PIN را انتخاب کرده است؟ مسلما فقط به خاطر سوء استفاده از پسوردهای رایج قدیمی نمی باشد.

خیر.

یک PIN به صورت قابل ملاحظه ای سریعتر مورد استفاده قرار می گیرد و راهی است در جهت ایجاد امنیت بیشتر نسبت به ورود پسوردهای قدیمی و رایج می باشد.

حال سوالی که ایجاد می شود این است که چگونه یک PIN از یک پسورد پیچیده تر و امن تر است ؟!

جواب سوال ساده است زیرا الگوریتمی شبیه به آن وجود ندارد.

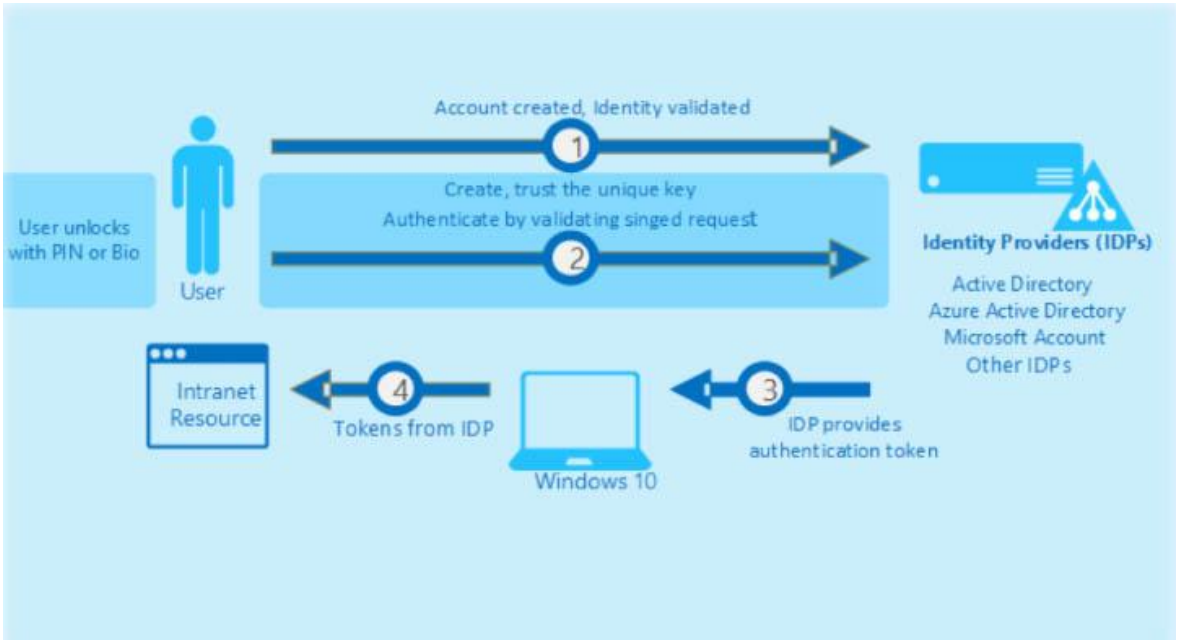
یک پسورد برای دسترسی به هر دستگاهی مورد استفاده قرار می گیرد اما PIN کاملا متفاوت است. PIN برای یک دستگاه خاص کاملا منحصر به فرد می باشد. یعنی اگر یک نفر PIN شما را به سرقت ببرد و برای دستیابی به دیتاهای شما تلاش کند خوشبختانه نمی تواند کاری از پیش ببرد مگر اینکه از دستگاهی استفاده شود که با PIN لینک شده است.

حتی پس از آن، هنوز نیاز به عبور از لاگین بیومتریک وجود دارد که این مرحله نیز فقط بوسیله ی خود شما امکان پذیر است. فکر می کنیم با ارائه این مثال اوج امنیت را حس کردید!

امکان دزدیدن PIN نامبر شما و استفاده از آن جهت دریافت پول وجود ندارد. PIN نامبر همراه با کارت می باشد و نمی توان آنرا به صورت مجزا استفاده کرد.

انتخاب با شماست. Windows Hello یا Microsoft Passport ؟ این نگرانی شما که احتمال دزدیده شدن اطلاعات بیومتریک وجود دارد کاملا قابل درک می باشد. به همین دلیل مایکروسافت اطلاعات بیومتریک را فقط در داخل دستگاه خودتان ذخیره سازی می کند و بر روی هیچ سرور خارجی وجود ندارد.

این روش بیشتر در مواردی استفاده می شود که نیاز به Unlock کردن دستگاه شما بوجود می آید. همچنین جهت هویت سنجی در یک شبکه معمولی مورد استفاده قرار می گیرد.



Passport2Go

Passport2GO یک قسمتی از سیستم Passport بوده که به شما اجازه می دهد مشخص نمایید دستگاهی که استفاده می کنید کاربری شخصی دارد یا برای شرکت است.

از طریق یک مثال به راحتی می توانیم کاربری Passport2Go را مشخص کنیم.

داستان خنده دار: اگر دقت کرده باشید مایکروسافت همیشه از یک کمپانی ساختگی به اسم Contoso در مثال ها و ارائه هایش استفاده میکند.

اروین بعنوان یک مشاور برای یک کمپانی کار می کند که سرویس هایی را برای Contoso فراهم میکنند. Contoso به شرکایش اکانت های cloud داده است. این اکانت ها در مواقع ضروری از طریق Azure Active Directory کار می کنند.

Azure Active Directory: آژور اکتیو دایرکتوری، فراهم کننده مدیریت تصدیق هویت و قابلیت های کنترل دسترسی برای برنامه های ابری می باشد. شما می توانید هویت های از پیش تعیین شده را هماهنگ کنید و برای ساده سازی کنترل کاربر به اپلیکیشن های cloud، ویژگی شناسایی یگانه یا Single Sign-On را فعال کنید.

اروین بعد از یک مدت طولانی نیاز به یک اکانت AAD دارد تا کارهای مربوط به Contoso را انجام دهد، با یک کمک هزینه مشخص، که به او اجازه داده می شود دستگاهی بخرد که فقط برای کمپانی Contoso استفاده نماید.

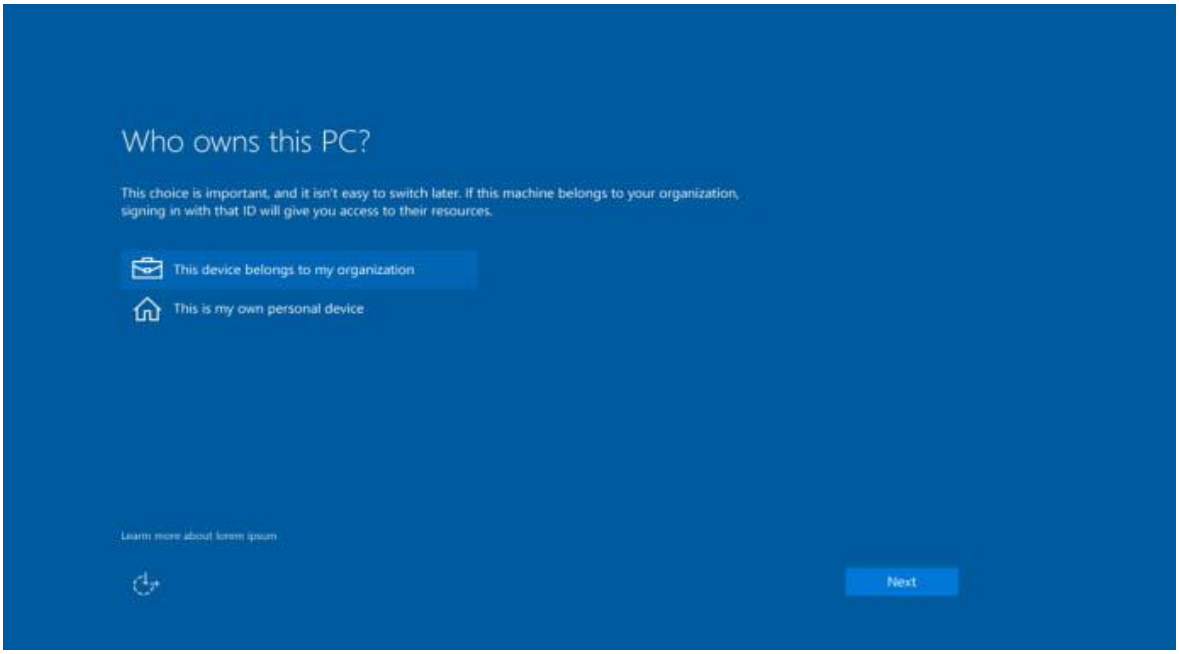
چگونه می توانیم کاری کنیم که او فقط از این دستگاه برای کارهای شرکت Contoso استفاده نماید ؟!

بوسیله ی فعال سازی قابلیت Passport2Go

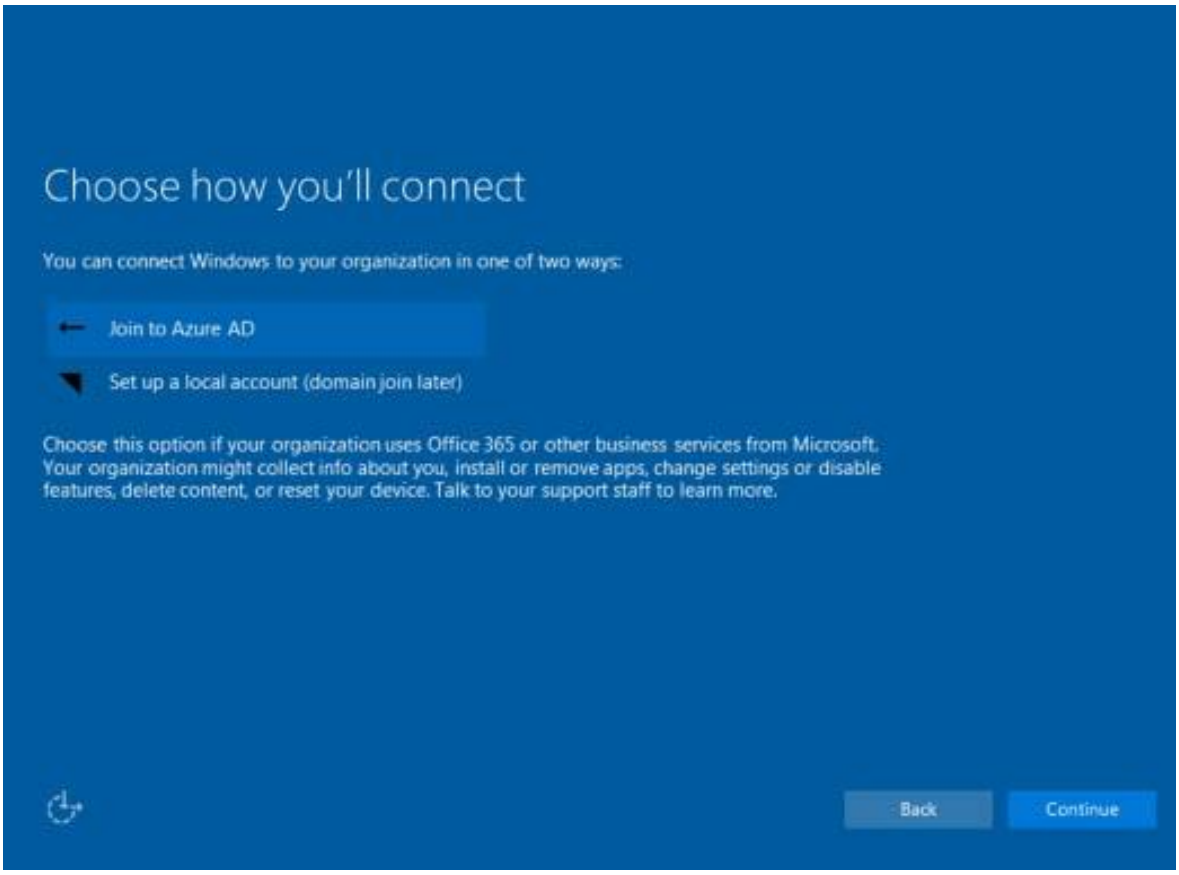
وقتی با Passport2Go لاگین می کنید، این شما هستید که مشخص خواهید کرد که دستگاه شما به صورت شخصی و یا شرکتی مورد استفاده قرار گیرد.

بریم سراغ مثال بعدی:

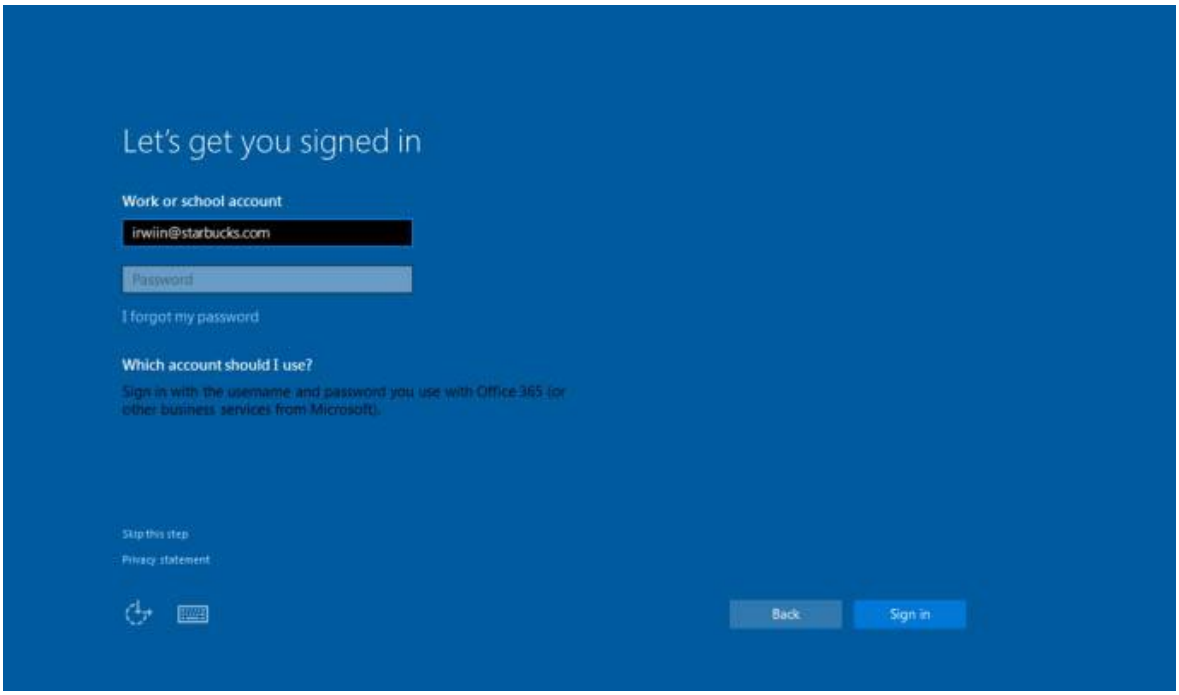
در مثال ما، سازمان تصمیم گرفته است دسترسی تمام منابعی که اروین برای انجام کارهایش نیاز دارد را به او بدهد.



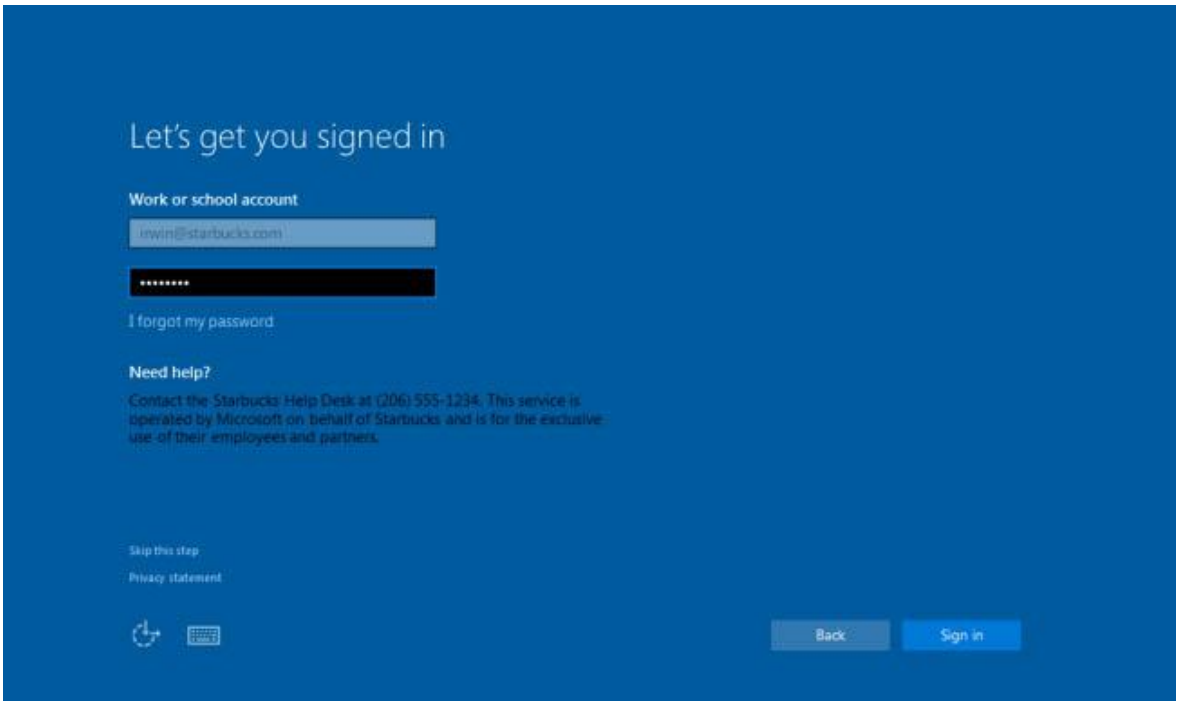
در مرحله بعدی اروین مشخص میکند که چطور وصل شود. Contoso برای او اکانت AAD را ایجاد کرده است. این امکان توسط او انتخاب می شود.



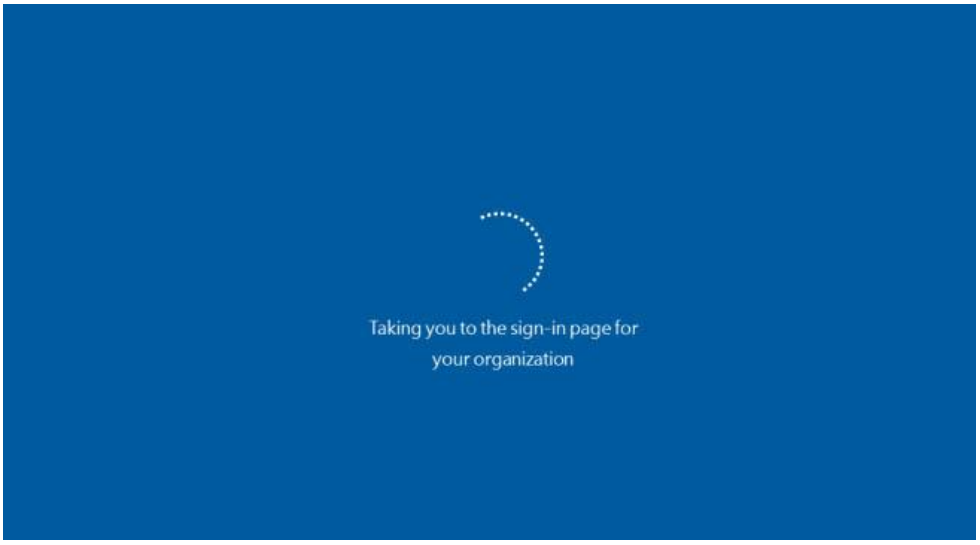
اروین وقتی با اکانت مربوط به AAD خود sign in می کند ابتدا اعتبارسنجی می شود و سپس امکاناتی مانند Office 365 و ایمیل هایش در اختیار او قرار می گیرد.



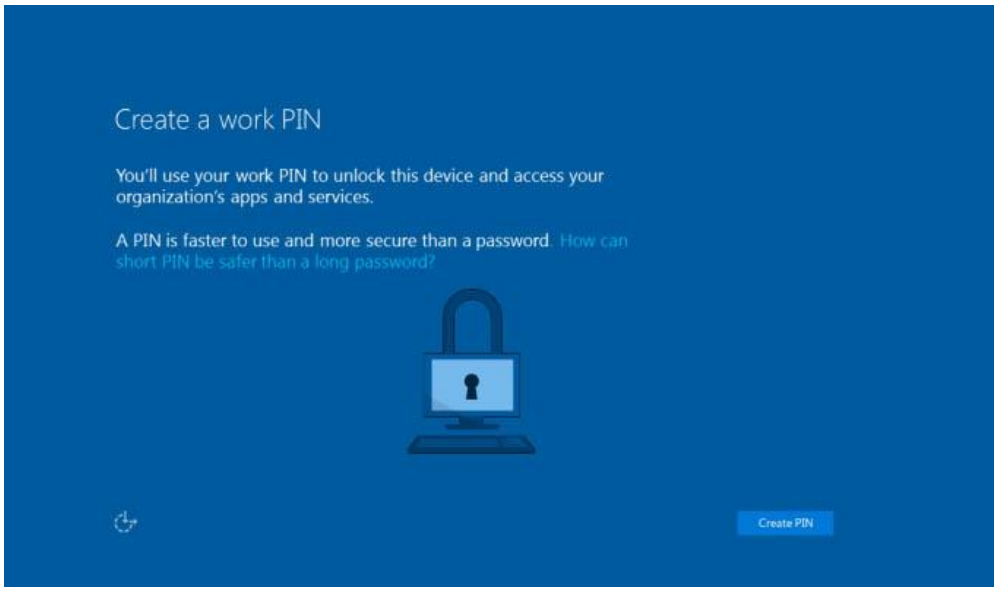
در این قسمت کلمه عبور وارد می شود ...



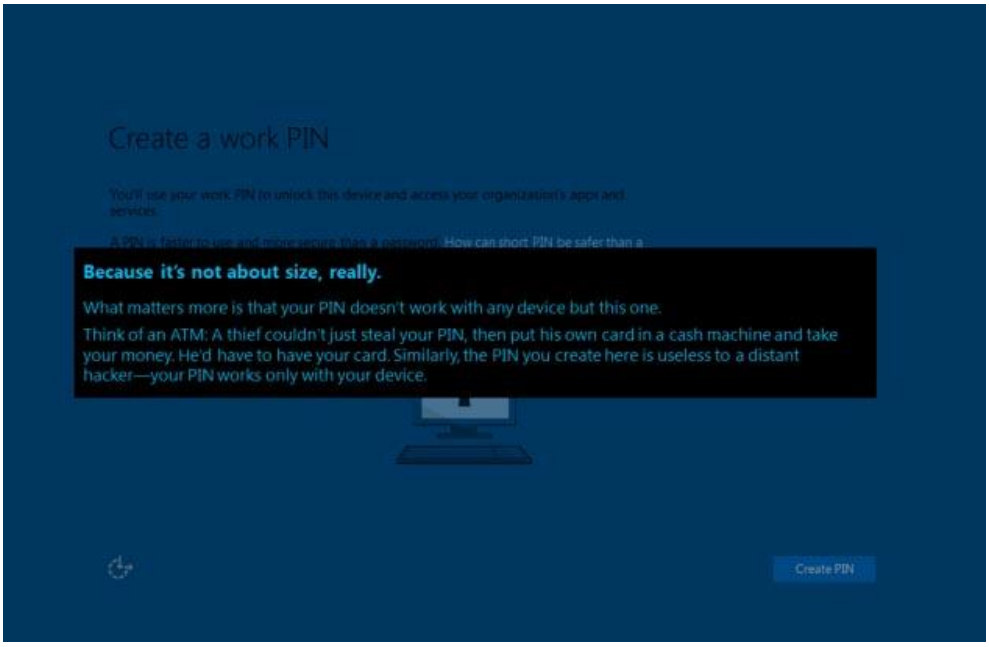
اروین سپس به صفحه Contoso هدایت می شود تا بر روی AAD مایکروسافت آژور Sign in نمایید.



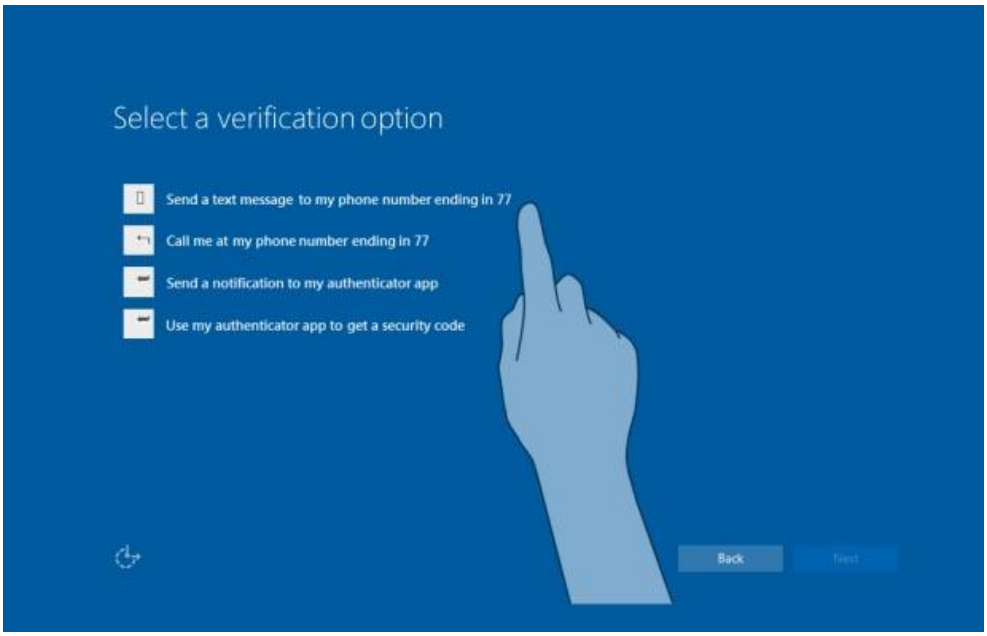
الان وقت آن است که اروین شماره PIN راSetup کند تا به او اجازه داده شود دستگاه را Unlock کرده و به تمام منابعی که جهت انجام کارهایش نیاز دارد دسترسی داشته باشد.



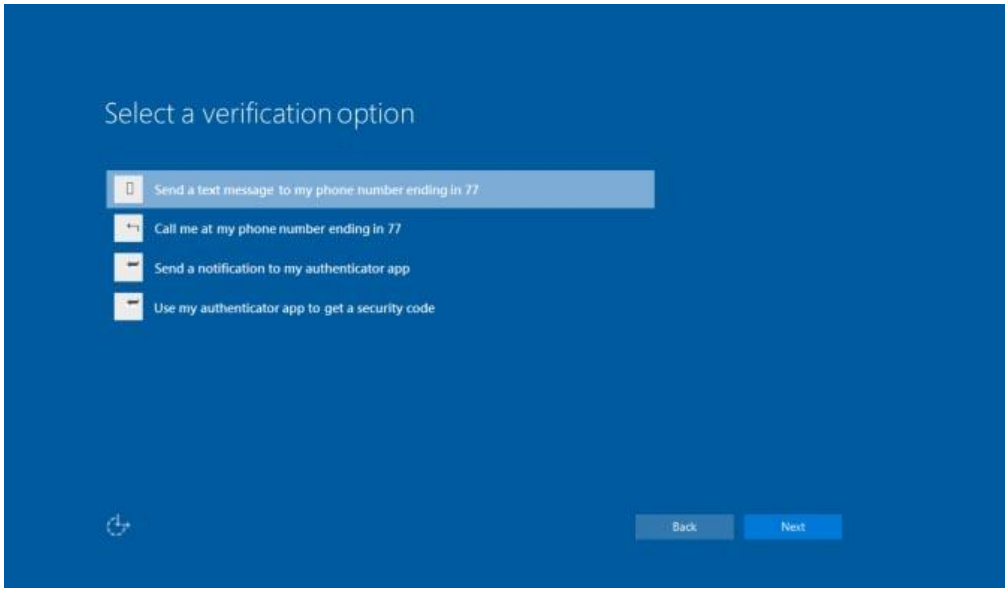
همان گونه که قبلا اشاره کردیم PIN نامبرها بسیار کوتاه تر و امن تر از کلمات عبور می باشند. ممکن است این سوال برای شما پیش بیاید که چطور PIN نامبرهای کوتاه می توانند امن تر از پسوردهای پیچیده و طولانی باشند ؟! مایکروسافت به زودی پاسخ سوال شما را می دهد.



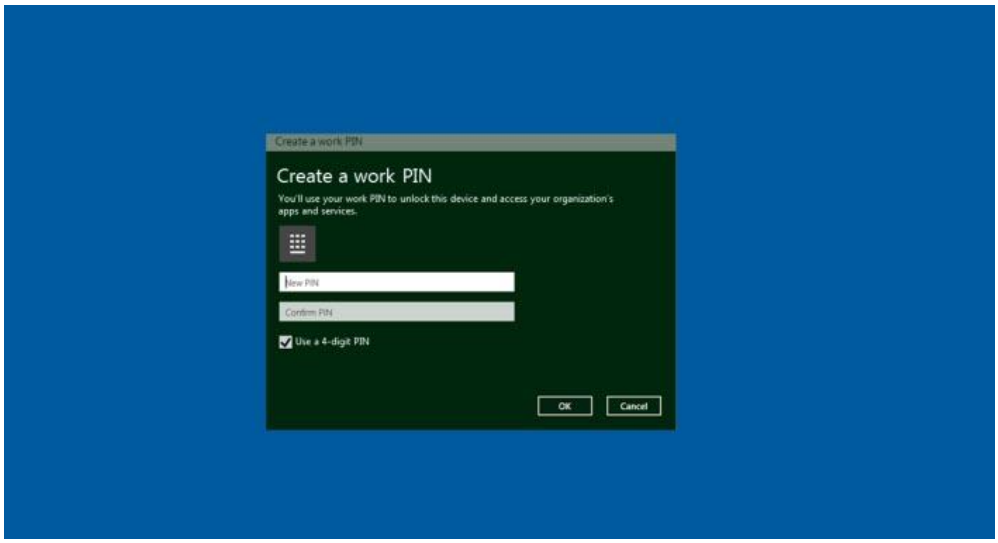
قدم بعدی برای اروین انتخاب این موضوع است که اکانتش چگونه اعتبارسنجی شود. او چهار انتخاب دارد: Text Message – Phone Call، یک اخطار که برای او ارسال می شود یا استفاده از برنامه ای که توسط کد امنیتی اعتبارسنجی میکند.



اروین پیام متنی را انتخاب میکند.



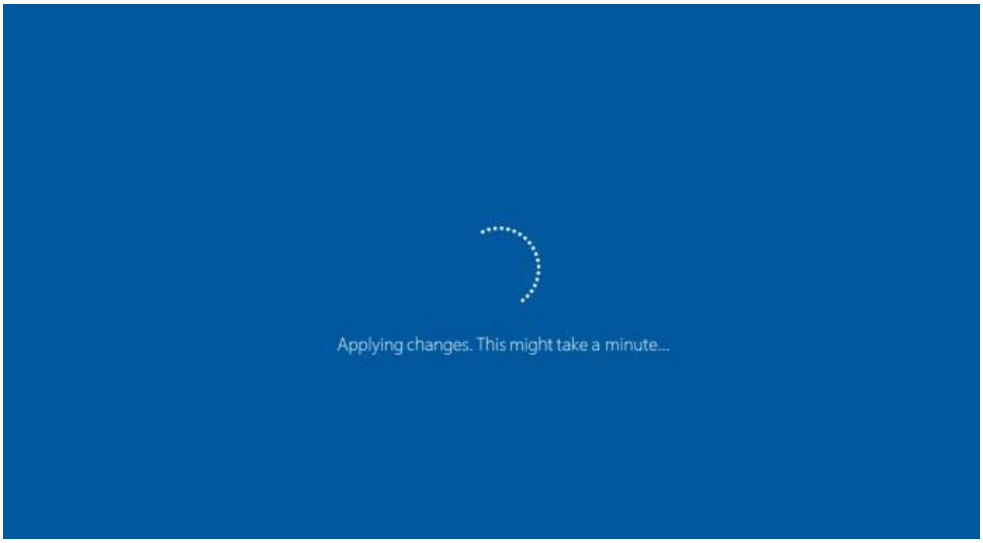
وقتی او برای اولین بار پیام تایید خود را دریافت می کند، اروین می تواند PIN برای خودش بسازد.



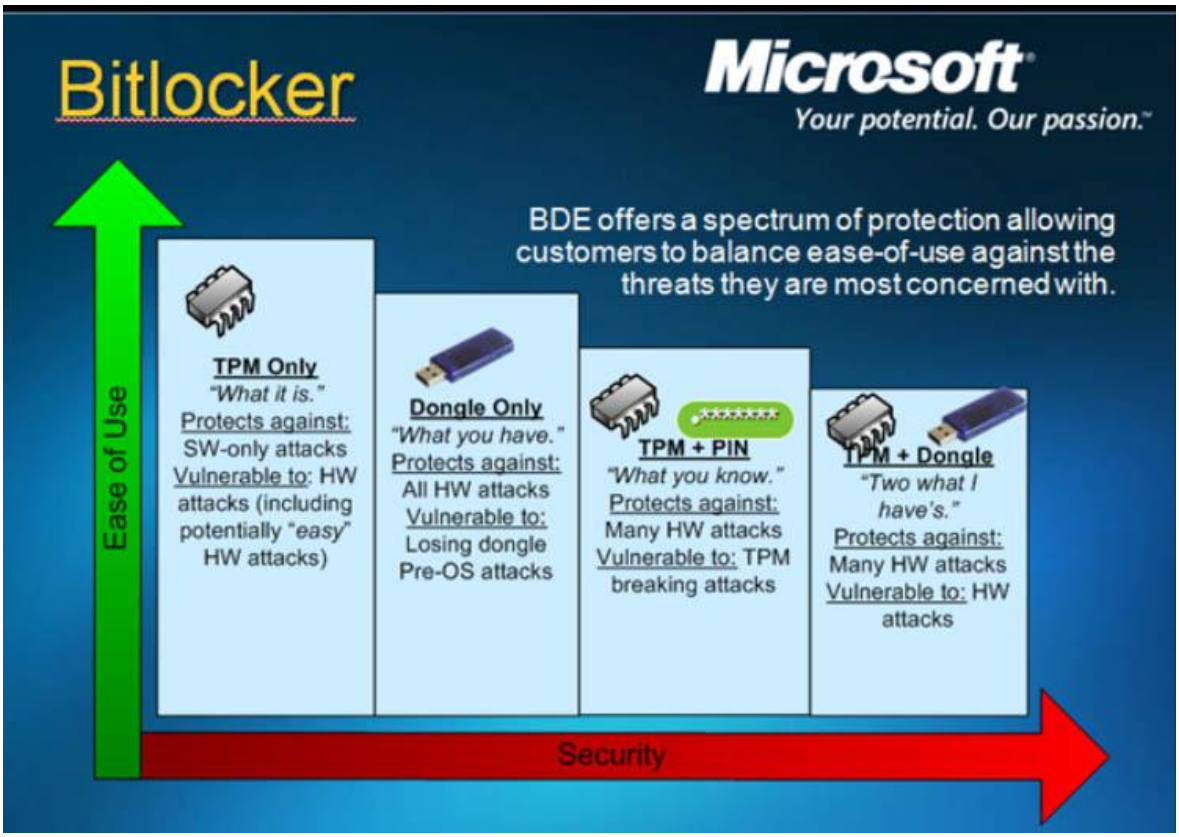
وقتی گزینه ی استفاده از کد ٤ رقمی تیک زده شود باید کد ٤ رقمی به همراه تکرار آن در فیلد مربوطه داده شود.

Contoso نیازمندی های خاصی را برای PIN های پیچیده درنظر گرفته و دستورالعمل ها به وضوح نشان می دهد که اروین چه کارهایی را باید انجام دهد تا PIN ساخته شده بر اساس خواسته های کمپانی باشد.

وقتی برای اولین بار اروین PIN خودش را به صورت صحیح وارد می نماید تغییرات اعمال می شود البته ممکن است مدت زمانی بین چند ثانیه تا چند دقیقه بطول بینجامد.



سرانجام، -NGC – Next Generation Credentials آماده سازی شد و اروین با خیالی آسوده می تواند دسترسی کاملی به تمام برنامه ها و سیستم داشته باشد. البته در نظر داشته باشید که این دسترسی ها بر اساس نیاز کاری او و با توجه به سیاست های سازمان چیده شده است.



BitLocker & TPM

Windows BitLocker Drive Encryption یک قابلیت جدید امنیتی در جهت محافظت موثرتر ازدیتا می باشد. این کار بر اساس رمزگذاری قطعات کوچک دیتا که در volume ها ذخیره شده اند صورت می پذیرد. پارتیشن های روی هارددیسک ها.

TPM – the Trusted Platform Module چیپی مخصوص که وظیفه ذخیره سازی کلید Pair شده که Endorsement key نامیده می شود را برعهده دارد. کلید Pair شده در داخل چیپ TPM ذخیره شده و توسط نرم افزارها قابل دستیابی نمی باشد.

وقتی یک کاربر و یا Admin مالکیت یک دستگاه را بدست می آورد، یک Root key قوی ساخته می شود. کلید Pair شده توسط TPM بر اساس کلید Endorsement ساخته شده و یک کلمه عبور مخصوص برای مالک سیستم ایجاد می شود.

کلید دیگر، که Attestation Identity Key (کلید گواهی هویت) نامیده می شود. این کلید جهت مخافظت از دستگاه ها در برابر تغییرات غیرمجاز بوسیله ی نرم افزار یا فریمویرها کار میکند. این کار می تواند بوسیله ی hash کردن قسمت های اصلی برنامه و فریم ورها قبل از اجرا باشد .

وقتی سیستم تلاش میکند تا به شبکه متصل شود، یک سرور وظیفه چک کردن تطابق بین متغییرها را دارد. اگرنسبت به آخرین اعتبارسنجی تغییری در Hashing ایجاد شود سیستم امکان ورود به شبکه را بدست نمی آورد.

Windows BitLocker از TPM جهت حفاظت از سیستم عامل و تمام دیتاهای آن استفاده میکند. همچنین به کاربران کمک می نماید تا از کامپیوترهایشان در برابر دستکاری و یا سوء استفاده محافظت نمایند.

گفته می شود، BitLocker بدون استفاده از TPM هم مورد استفاده قرار می گیرد اما، از سال ۲۰۱۶ مایکروسافت تدابیری اندیشه است که به کامپیوترهایی نیاز خواهد داشت که TPM نسخه ۲ را دارند.

اگر شما این کار را بدون استفاده از TPM انجام بدهید، باید پیکربندی BitLocker جوری انجام شود که کلیدهای رمزنگاری شده بر روی یک فلش قرار گیرد که بعد از آن هر وقت خواستید دیتاهای ذخیره شده را مورد استفاده قرار دهید از این فلش ممووری استفاده کنید.

پلتفرم ماژول مورد اعتماد یا TPM یک سری از سرویس های امنیتی جالب را برای شما فراهم میکند:

- نگهداری و امنیت مراحل بوت به صورت امن
- استخراج و ایزوله سازی کلیدها بر اساس ترتیب بوت مخصوص
- ایجاد root of trust بر روی بستر cloud
- محافظت از تمام پروسس ها در برابر malwareها و یا malicious ها

TPM 2.0 یک سری امکانات بیشتری نسبت به TPM 1.2 دارد که این امکانات بروزرسانی شده با قابلیت های بیشتر نسبت به نسخه ی قبلی می باشد:

- رمزنگاری قوی تر که جهت استانداردهای مدرن و مستحکم بروز رسانی شده است.
- انعطاف پذیر بیشتر بر روی الگوریتم های رمزنگاری شده تا پشتیبانی بهتری جهت مصارف عمومی داشته باشد
- انسجام مدیریتی بهتر در سراسر پیاده سازی

چگونگی کارکرد BitLocker جهت رمزگذاری درایوها:

مخلص کلام، با رمزنگاری همه دیتاها از سیستم شما محافظت بعمل می آید. اگر یک TPM از کلیدهای رمزنگاری برای قفل کردن سیستم استفاده نماید، این کلیدها تا زمانی که کامپیوتر اعتبار سنجی TPM را انجام ندهد نمی توانند مورد دسترسی قرار بگیرند.

اگر هر نشانه ای از سوء استفاده به چشم بخورد، TPM اجازه نخواهد داد تا کلیدها استفاده شوند.

با رمزنگاری محتوای ورودی Volumeها، شما از همه چیز محافظت می کنید. دیتاهای شخصی، سیستم عامل، temporary فایل ها، فایل های رجیستری ویندوز و ... .

چون کلیدها توسط TPM قفل شده اند، حتی اگر هارددیسک شما دزدیده شود و هارد آن بر روی دستگاه دیگری قرار گیرد سارق نمی تواند به دیتاهای شما دسترسی داشته باشد.

وقتی دستگاه را روشن می نمایید، TPM مقدارهای hash شده تنظیمات را با snapshotهای جدید مقایسه کرده و بعد از تایید پروسه ی استارت سیستم آغاز می شود.

اگر تمام موارد مورد تایید باشد TPM کلید را آزاد کرده و دیتای رمزنگاری شده می تواند Unlock شود. اگر Windows installation نشانه هایی از دستکاری را نشان دهد کلید آزاد نمی شود. همان طوری که گفته شد .

به صورت پیش فرض تنظیمات BitLocker طوری انجام شده که با TPM کار کند. شما می توانید PIN کد وارد شده ی کاربر یا کلید شروع دیگری را که در حافظه فلش ذخیره شده ترکیب نمایید. اگر شما یک TPM پیچیده ندارید این کلید یک نیاز می باشد.

BitLocker چیست ؟ به کاربران اجازه رمزگذاری درایوهای خود را با کلیدهای ۱۲۸ بیتی یا ۲۵٦ بیتی می دهد. از ویندوز vista نسخه های Ultimate و Enterprise ارائه شد. الگوریتم رمزگذاری AES در حالت CBC است.

CBC- Cipher Block Chaining: یک توالی از بیت ها کدگذاری می شود. همانند یک واحد یا بلاک که با یک کلید Cipher به کل بلاک اعمال می شود. اگر یک بیت اشتباه باشد کل بلاک ها تحت تاثیر قرار می گیرند.

در رابط جدید BitLocker علاوه بر رمزگذاری Volumeهای یک دیسک، USB ها هم اضافه شده اند.

TPM: یک چیپ بر روی مادربورد ها می باشد که حفظ اطلاعات رمزنگاری شده را برعهده دارد.

پروسه رمزنگاری:

۱- سیستم روشن می شود، بایوس اطلاعات موجود در TPM را بررسی می کند این اطلاعات با PCR ارتباط دارد.
۲- در صورتی که اطلاعات با ثبات ها هماهنگ باشند TMP از SRK برای رمزنگاری کلید اصلی استفاده خواهد کرد.
۳- Full Volume Encryption Key – FVEK: از داده های رمزنگاری شده آن Volume استخراج شده و توسط VMK رمزنگاری می شود. FVEK برای رمزنگاری کل دیتاها استفاده می شود.

خلاصه: ماژول توسط بایوس سیستم بررسی می شود، کلید SRK برای رمزنگاری VMK و کلید VMK برای رمزنگاری کلید اصلی FVEK و نهایتا کلید FVEK برای رمزنگاری کل داده ها استفاده می شود.

تایید اعتبار :

کاربر کدی را وارد می نماید تا داده ها رمزنگاری شود. این کد همان PIN Number می باشد.

۱- قبل از بوت شدن OS، PIN از کاربر درخواست می شود.
۲- کلید VMK توسط PIN وارد شده رمزنگاری می شود.

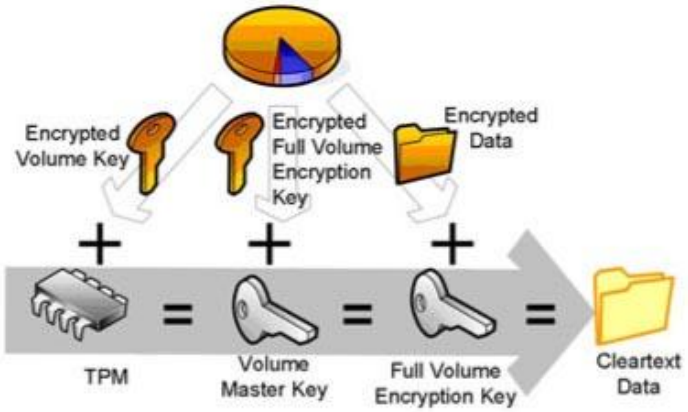
۳- کلید اصلی Volume از داده های رمزنگاری شده همان Volume استخراج شده و توسط VMK رمزنگاری می شود به این ترتیب FVEK رمزنگاری شده برای کل داده ها استفاده می شود.

دستگاه USB:

۱- هنگام بوت درخواست USB توسط OS داده می شود.
۲- پس از بررسی لازم، کلید VMK توسط کد موجود در حافظه USB رمزنگاری می شود.
۳- FVEK استخراج شده توسط VMK رمزنگاری می شود. FVEK برای رمزنگاری کل داده ها استفاده می شود.

TPM (Trusted Platform Module): یک میکروچیپ یا میکرو کنترلر است که قابلیت انجام برخی از فرآیندهای امنیتی سیستم را انجام می دهد. TPM بر روی مادربورد سیستم نصب می شود و با استفاده از یک BUS سخت افزاری با سایر قسمت های سیستم در تماس است. (تقریبا می توان گفت ماژولی برای احراز هویت است).

کلیدهای رمزنگاری در داخل TPM قرار می گیرد به این کار Wrapping کلیدها گفته می شود. هر TPM یک کلید ریشه دارد که به آن Storage Root گفته می شود. SRK درون TPM قرار می گیرد. قسمت خصوصی و محرمانه کلید که در درون TPM قرار گرفته است به هیچ عنوان برای شخص نرم افزاری در دسترس نخواهد بود. این نوع کلیدها فقط می توانند توسط معیارهای امنیتی همان Platform رمزگشایی شوند. در صورت تغییر مقادیر و برابر نبودن آنها با توجه به مقادر قبلی TPM، Platform احراز هویت نمی شود. عملیات رمزگشایی Unsealing گفته می شود. TPM روش رمزگذاری بر اساس سخت افزار می باشد.



BitLocker تغییرات شگرفی در ویندوز ۱۰ کرده است. این ابزار در جهت رمزگذاری فایل های مجزا می تواند مورد استفاده قرار گیرد. این امر در حالی صورت گرفته است که به صورت نرمال برای اطلاعات یک درایو مورد استفاده قرار می گرفت. اگر بخواهید فایل های خاصی را ایمیل کنید آنها باید در سطح فایل به فایل رمزگذاری شوند.

کاربران می توانند رمزنگاری فایل هایشان را از قسمت Save as انتخاب نمایند. در این مثال تمام چیزی که کاربر باید بداند راست کلیک بر روی فایل و انتخاب گزینه encryption option می باشد. تمام فایل ها رمزنگاری شده و سپس به رنگ سبز نمایش داده می شود. این امر سبب می شود کاربر با دیدن این رنگ متوجه شود که فایل ها محافظت شده است.

یکی از رایج ترین استفاده از BitLocker دانلود سندهای حساس از یک وب سایت می باشد. در این مثال، فایل های وب به صورت خودکار رمزنگاری شده اند، در این حالت تصور شما این است که اطلاعات کاملا رمزنگاری شده اند.

Device Guard

مایکروسافت دست بکار شده و از هویت و داده های شما محافظت می کند اما دستگاهی که شمااز آن استفاده میکنید چه خواهد شد؟

در ویندوز ۱۰ راهکارهای مختلفی جهت لاک کردن دستگاه وجود دارد. اضافه کردن محافظت های خاص و مقاومت در برابر تهدیدات بعضی از این راهکارها می باشند. کاربران سهوا فایل های آلوده ای را بر روی

سیستم خود دانلود می نمایند. بنابراین مایکروسافت سیستم جدیدی را معرفی نموده که فقط به اپلیکیشن های خاص اجازه اجرا می دهد.

برنامه های مورد اطمینان توسط مایکروسافت تایید شده اند. البته فراموش نکنیم که این پیکربندی از قبل به سیستم اعمال شده است. این قابلیت جدید Device Guard نامیده می شود.

Device Guard یک قسمت جدیدی از فریمور است که در سطح سخت افزار اجرا شده و قبل از پروسه بوت شدن اتفاق می افتد.

طراحی آن طوری می باشد که فقط به برنامه ها و اسکیریپ هایی اجازه اجرا می دهد که تایدیه لازم را دارا می باشند. این ویژگی محبوبیت زیادی بدست خواهد آورد.

Device Guard ترکیبی از قابلیت های سخت افزاری و نرم افزاری می باشد که جهت پیکربندی هر دو حالت سخت افزاری و نرم افزاری به یکدیگر نیاز دارند. وقتی این کار صورت گرفت دستگاه قفل شده و فقط برنامه های مورد اطمینان اجرا خواهند شد.

این قابلیت با استفاده از زیرساخت مجازی امنیتی که در ویندوز ۱۰ قرار دارد کار میکند یک سیستمی که کدهای بکار رفته در سرویس ها را از هسته ویندوز ایزوله کرده و بر اساس سیاست های مشخص تعیین می نماید که چه کسی دسترسی داشته و چه کسی دسترسی نداشته باشد.

وظیفه اصلی Device Guard این است که هر پروسه ای که جهت لود شدن آغاز به کار کرد تست نماید. در صورتی که پروسه ای با Signature های ما مطابقت نداشت از اجرا شدن آن جلوگیری می شود.

تکنولوژی مورد استفاده Device Guard در سطوح سخت افزار قرار دارد و این باعث می شود درصد خطاها کاهش پیدا کند. استفاده از این ویژگی در تکنولوژی مجازی سازی برای اتخاذ تصمیمات درست استفاده می شود. بدین صورت تصمیماتی اعمال می شود که به دستگاه در مورد پروسس هایی که باید اجرا شود و یا نباید اجرا شود دستورت لازم منتقل می شود.

این سطح از ایزوله کردن باعث می شود malware ها متوقف شده و اجازه داده نمی شود تا بر روی دستگاه لود شوند. این در شرایطی می باشد که مهاجمین دسترسی کاملی بر روی سیستم دارند اما امکان لود کردن malware بر روی رم را ندارند!

طبق گفته مایکروسافت امنیت در این روش نسبت به آنتی ویروس های قدیمی بالاتر بوده و حتی نسبت به تکنولوژی های کنترلی اپلیکشن ها شرایط بهتری پیدا کرده است.

نیازمندی های سخت افزاری و نرم افزاری برای Device Guard

شما برای استفاده از Device Guard به پیکربندی نرم افزارها و سخت افزارهای زیر نیاز دارید:

- ✓ Device Guard فقط با ویندوز ۱۰ کار میکند.
- ✓ UEFI Secure Boot – محافظت از دستگاه در سطح سخت افزاری
- ✓ Trusted Boot – جهت محافظت در برابر حملات سطح rootkitها طراحی شده است.
- ✓ Hyper V – Virtualization Based Security
- ✓ Package Inspector Tool به کاربران کمک میکند تا لیستی از فایل هایی که باید توسط برنامه های ویندوز sign شوند ساخته و ایجاد گردد.

چرا از Device Guard استفاده نماییم ؟

هر روزه صدها فایل مخرب جدید ساخه شده و ما با استفاده از روش های قدیمی و منسوخ به مبارزه با این فایل ها می رویم.

با Device Guard، کاربران نمی توانند malwareها را دانلود کنند به این خاطر که محتوای این فایل ها مورد اطمینان نمی باشد. از ویندوز ۸,۱ ببعد اپلیکیشن ها به صورت خودکار می توانند مورد Trust قرار گیرند مگر اینکه یک فایروال یا آنتی ویروس آن را بلاک نماید. با ویندوز ۱۰ یک اپلیکیشن اجرا نمی شود مگر اول مورد Trust قرار بگیرد.

Device Guard در برابر حملات Zero Day از سیستم ما محافظت خواهد کرد همچنین می تواند در اشکال مختلف و به صورت کامل از سیستم در برابر ویروس ها محافظت نماید.

در تنظیمات پیشرفته، سیاست های کدینگ مشخص میکند که کدام برنامه مورد اعتماد می باشد.

قبل از اینکه شما از Device Guard استفاده نمایید، باید امنیت را بر اساس ظرفیت های سیستم مجازی خودتان بسنجید و مطمئن شوید که کدها به درستی و بر اساس سیاست های مشخص سازمانی پیاده سازی شده باشند.

بعد از این موارد، Device Guard چیزی شبیه به این کار خواهد کرد:

۱- دستگاه با حالت Secure Boot بالا خواهد آمد. این کار سبب می شود rootkitها نتوانند خود را هنگام بوت شدن در استارت ویندوز قرار بدهند.

۲- اولین استارت امن و مطمئن خواهد بود، ویندوز ۱۰ با قابلیت هایی همچون Kernel Mode Integrity بر اساس سیستم مجازی سازی Hyper V استارت می شود. این امر سبب محافظت از Kernel ویندوز می شود.

۳- استفاده از UMCI، Device Guard سیستم را مورد بررسی قرار می دهد تا مطمئن شود که تمام موارد اجرا شده در سیستم مورد اطمینان– Trust – می باشند.

٤- وقتی ویندوز ۱۰ run می شود، TPM هم اجرا شده تا در جهت حفاظت از اطلاعات حساس نقش به سزایی را بازی کند همان گونه که در قبل توضیح داده شد این تکنولوژی کامپوننتی سخت افزاری می باشد که از گواهینامه ها و احراز هویت های مختلف کاربر در برابر حملات و سرقت محافظت می نماید.

EDP-Enterprise Data Protection

مایکروسافت یک سیستم جدید DLP جهت جلوگیری از نشر اطلاعات دارد.

در حالی از این سیستم استفاده می شود که هدف اصلی آن شرکت ها و سازمان های بزرگ می باشد و در مکان هایی که تعداد زیادی کارمند با دستگاه های مختلف وجود دارد مورد استفاده قرار می گیرد.

وجود تعداد زیادی دستگاه از انواع مختلف، ریسک سوء استفاده از دیتاها را بالا می برد، اساسا این اتفاق در شرایطی رخ می دهد که تعداد زیادی از برنامه های برون سازمانی و سرویس های خارج از شرکت توسط این دستگاه ها مورد استفاده قرار می گیرد.

اینها شامل ایمیل، مدیاهای اجتماعی و سرویس های ابری می باشند و تمام برنامه هایی که توسط ما بر روی موبایل ها هر روزه اجرا می شوند.

راه حل هایی مانند درخواست از کاربران و کارمندان جهت جلوگیری از نصب برنامه ها و اپلیکشن های مضر وجود دارد اما به وضوح روشن است که این روش ها زیاد موثر و کارا نبوده و کاربران توجه زیادی به این موارد نشان نمی دهند.

قابلیت جدید ویندوز ۱۰ با نام Enterprise Data Protection – EDP –که توسط مایکروسافت ارائه شده است تجربه ی کاربری دلنشینی را برای ما به ارمغان آورده است. همزمان به شما کمک می نماید تا فعالیت های سازمانی خود را از فعالیت های شخصی کاملا تفکیک نمایید.

EDP به سازمان ها کمک می نماید تا از برنامه ها و سرویس های خود در برابر سوء استفاده محافظت نمایند بدون اینکه از کاربر بخواهند تا تغییراتی را در سیستمی که با آن کار میکند اعمال نماید.

علاوه بر این، در ارتباط با EDP – Right Management Service – RMS از دیتاهای سازمانی شما بر اساس ساختار مشخصی محافظت می نماید، حتی وقتی که دیتاها به اشتراک گذاشته شده باشند.

EDP **چگونه کار میکند؟**

Enterprise Data Protection جهت ازبین بردن تمام چالش های زیر طراحی شده است:

- طریقه مواجه شدن با سرورهایی که با مشکل DLP مواجه هستند.
- نگهداری و محافظت از داده های خصوصی
- مدیریت اپلیکشن هایی که پالسی دریافت نمیکنند و به طور خاص بر روی موبایل ها نصب شده اند.
- برطرف کردن مشکل قفل نمودن دستگاه کاربری که به صورت بالقوه اجازه نشر دیتا به بیرون از سازمان را می دهد.

سطوح حفاظت

EDP قابلیت تنظیم در ٤ سطح متفاوت از حافظت را دارا می باشد:

- Block: قابلیتی که برای اشتراک گذاری دیتا بوده و با توجه به نوع کارکرد آن زیاد مناسب نبوده و نوع کار آن به این صورت می باشد که کاربران را از اشتراک گذاری منع کرده و آنها را بلاک می نماید.
- Override: به نظر میرسد این قابلیت برای هر نوع اشتراک گذاری دیتا کاربرد داشته ولی زیاد مناسب نمی باشد.
- EDP:Audit خیلی بی سر و صدا در پس زمینه اجرا شده و تمام لاگ های مربوط به اشتراک گذاری های دیتاها را دارد و آنهایی را که مشکل دارند فلگ میزند. هیچ چیزی بلاک نخواهد شد، فقط مانیتور و ثبت می شود.
- Off: EDP فعال نبوده و از دیتاهای سیستم شما محافظت نمیکند.

EDP **اجازه گردش کار بهتری را می دهد**

کارمندان جهت حفاظت از دیتاهای خود نیازی ندارند بین محیط ها و اپلیکیشن های مختلف سوئیچ نمایند، گردش کار بی وقفه بوده و بهره وری به صورت بالقوه و به طرز غیرقابل باوری افزایش پیدا خواهد کرد.

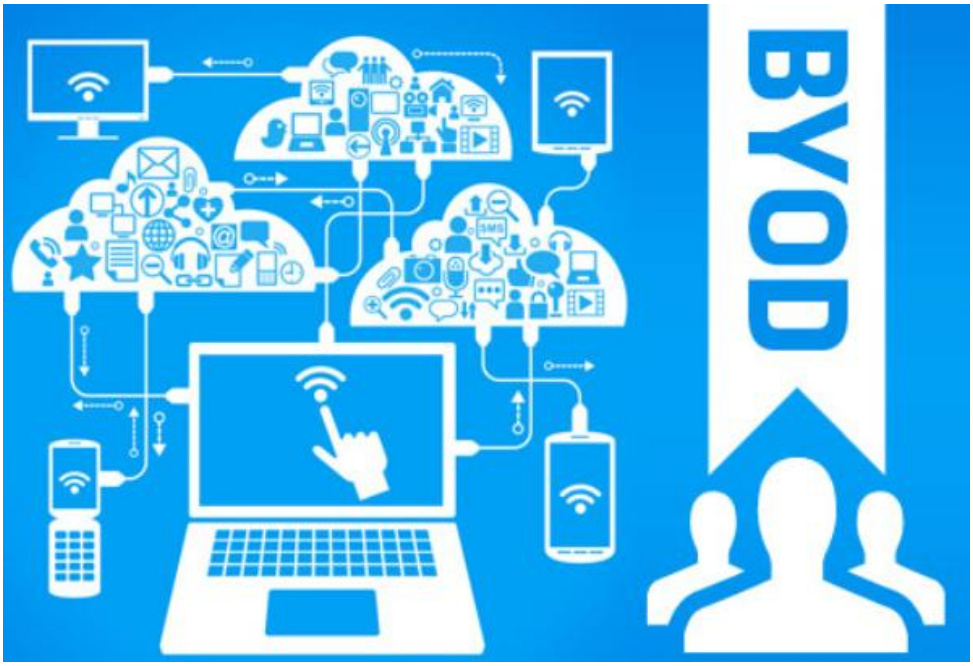
یک مثال عینی مانند این می باشد که یک کارمند در حال چک کردن ایمیل سازمانی خود می باشد و ناگهان یک ایمیل شخصی دریافت میکند. به جای اینکه از محیط مربوط به سازمان خود خارج شود، هر دو پیغام را در یک صفحه مشاهده خواهد کرد.

تغییرات سطوح امنیتی بر روی داکیومنت ها

کارمندان توانایی تغییرات سطوح محافظتی تنظیم شده براساس EDP را روی مستندات دارند.

در صورتی این امکان وجود دارد که داکیومنت شخصی بوده و یا به صورت نادرست توسط مدیر سیستم تنظیمات اعمال شده باشد. برای انجام آن، کارمندان باید اعمالی را انجام دهند که همین منجر به ایجاد لاگ شده و این لاگ ها جهت مشاهده برای مدیر سیستم ارسال می شود.

Enterprise Data Security



ادمین هر سیستمی باید محرمانگی و امنیت شبکه و دیتاهای خود را تضمین نماید. با EDP شما کاملا اطمینان خاطر دارید که دیتاهای موجود بر روی دستگاه های پرسنل به صورت کامل محافظت شده حتی زمانی که دستگاه در حال استفاده نمی باشد.

وقتی کارمندان فایل یا فولدری را بر روی دستگاه ایجاد میکنند، از آنها خواسته می شود که مشخص نمایند این دیتا شخصی می باشد یا شرکتی؟ اگر این دیتا شرکتی باشد به سرعت تحت محافظت دیتاهای داخلی شرکت قرار می گیرد.

Wipe Enterprise Data Remotely

EDP به مدیران سیستم پیشنهاد جالبی می دهد. این قابلیت مدیران را تشویق میکند تا از امکان پاک کردن دیتاهای شرکت از روی کامپیوتر پرسنل از طریق راه دور استفاده نمایند. این اتفاق در شرایطی رخ میدهد که دیتاهای سازمانی کاملا پاک شده ولی دیتاهای شخص بر روی دستگاه بدون هیچ گونه تغییری باقی می ماند. این مزیت وقتی خودش را نشان می دهد که دستگاه دزدیده می شود و یا کارمندان سازمان را ترک می کنند.

مستندات شرکتی به صورت لوکال بر روی دیوایس ها ذخیره سازی می شوند البته این فرآیند همراه با رمزگذاری دیتا صورت میگیرد.

وقتی شما قصد wipe کردن دیتا را دارید یک پروسه ی تایدیه در پیش دارید بعد از آن وقتی دستگاه به شبکه متصل شد دیتاها کاملا پاک می شود و کلیدهای رمزنگاری به صورت کامل غیرقابل بازگشت لغو شده و از بین می روند.

این اتفاقات فقط بر روی دستگاه مورد نظر (هدف) صورت می گیرد و بقیه دیوایس ها کاملا نرمال و بدون مشکل به کار خود ادامه می دهند.

کپی/دانلود کردن دیتاهای خاص:

وقتی دیتا از یک سورس شرکتی مثل SharePoint یا Office 365 دانلود می شود به صورت یک دیتای خاص و ویژه تعریف شده و قبل از دخیره بر روی هارد لوکال سیستم رمزگذاری می گردد.

مشابه همین اتفاق برای دیتاهای خاص دیگری می افتد که بر روی یک USB کپی می شود. دلیل این اتفاق ساده است وقتی شما دیتا را به صورت خاص و ویژه مارک می کنید سیستم به صورت خودکار آن را سازمانی تشخیص داده و بر اساس الگوریتم های کدگذاری مشخص شده آنها را رمزگذاری می نماید.

دسترسی به برنامه ها و محدودیت ها:

با EDP این شما هستید که مشخص می نماید چه برنامه ای می تواند به دیتاهای ویژه و سازمانی دسترسی داشته باشد یا نداشته باشد.

می توانید لیستی از برنامه ها جهت دسترسی به دیتاهای خاص را ایجاد نمایید. هر برنامه ای که در این لیست نباشد و بخواهد به اطلاعات دسترسی پیدا کند بلاک می شود.

دسترسی اپلیکیشن ها و دسترسی اشخاص متفاوت است. یک زمان کاربری تمایل دارد دیتا را کپی و Paste کند دسترسی برنامه این اجازه را به شخص می دهد اما دسترسی شخصی این اجازه را به او نمی دهد بنابراین شخص نمی تواند دیتا را کپی نماید.

یک شخص تلاش میکند تا دیتاهای سازمانی را داخل برنامه ای که دسترسی ندارد کپی نماید، در این هنگام پیامی با این شکل مشاهده می کند:

"محدودیت های موجود در این بخش اجازه تکمیل درخواست را به شما نمی دهد."

رمزگذاری پایدار دیتا Persistent Data Encryption

EDP به شما اجازه می دهد تا دیتاهای خود را حتی زمانی که دستگاه در حالت Roaming می باشد Safe نگهداری نمایید. برنامه هایی مانند OneNote و آفیس در ارتباط با EDP کار می کنند تا وقتی شما با هر سرویس و یا در هر مکانی بودید اطلاعات رمزنگاری شوند.

برای مثال، یک کارمند ایمیلی را توسط Outlook باز میکند که این محتوا با EDP رمزنگاری شده است، تغییراتی در این محتوا ایجاد میکند و سپس تلاش میکند که آنرا با اسم جدیدی ذخیره نماید تمام این تلاش ها در جهت خلاص شدن از رمزگذاری فایل صورت می گیرد!

اما زهی خیال باطل ! تمام این تلاش ها بیهوده است زیرا اوتلوک به صورت خودکار EDP را تایید کرده است و نسخه ی جدید از دیتای ایجاد شده مجددا رمزنگاری شده و به صورت مطمئن نگهداری می شود.

جلوگیری از به اشتراک رسانی تصادفی دیتا:

EDP نقش به سزایی در جلوگیری از به اشتراک گذاری دیتاهای سازمانی در فضای ابری دارد. برای مثال یک کارمند سندی را در یک فولدری به اسم DOCUMENTS قرار می دهد.

این فولدر به صورت خودکار با OneDrive سینک می شود، این در شرایطی است که این برنامه در لیست برنامه های مجاز می باشد. وقتی فولدر مذکور در سطح داخلی رمزنگاری می شود دیگر توانایی سینک شدن با سرویس های ابری کاربر را نداشته و با این کار از انتشار آن جلوگیری می کنیم.

در سیستم های قدیمی امکان داشت اتفاقات عجیبی برای دیتا رخ بدهد مثلا دیتا در سیستم دیگر منتشر شود (به سیستم دیگر منتقل شود) اطلاعاتی که نباید بین سیستم ها منتقل شود به راحتی بین سیستم ها جابجا گردد. برای مثال یک کارمند اطلاعات شرکت را روی فلش درایوی ذخیره می کند که آن فلش حاوی اطلاعات شخصی او نیز می باشد.

اطلاعات سازمانی تا زمانی که همراه با دیتای شخصی می باشد رمزگذاری می شود. تا زمانی رمزگذاری دیتا ادامه دارد که حتی اگر دیتا از یک دستگاهی به دستگاه دیگر منتقل شود هنوز به صورت رمزنگاری شده باقی می ماند.

مزایای EDP**:**

مزایای **EDP** شامل:

- ✓ محافظت دربرابر نشر اطلاعات سازمان، بدون کوچکترین تاثیر بر روی عملکرد کاری پرسنل
- ✓ جداسازی اطلاعات شخصی از اطلاعات سازمانی بدون نیاز به سوئیچینگ محیط و اپلیکیشن ها صورت می گیرد.
- ✓ محافظت از دیتاهای خاص موجود در سازمان بدون نیاز به بروزرسانی آنها
- ✓ قابلیت پاکسازی تمام اطلاعات سازمانی در شرایطی که کاربر از سازمان خارج می شود و دسترسی به او وجود ندارد.
- ✓ گزارش وضعیت جهت بررسی
- ✓ تجمیع کامل با سیستم مدیریتی حال حاضر یا سیستم مدیریت دستگاه موبایل جهت پیکربندی **EDP** برای شرکت یا سازمان، همچنین توسعه و مدیریت این دستگاه ها
- ✓ محافظت های ویژه از دیتاهایی که به اشتراک گذاشته شده است.

سناریوهای پیشرفته

- دیتاهای خاص می توانند بر روی هر دو حالت دستگاه سازمان یا دستگاه کارمندان رمزنگاری شوند.
- دیتاهای خاص از راه دور و بدون دخالت در دیتاهای شخصی کاربر می توانند پاک شوند.

- برنامه هایی به صورت ویژه انتخاب می شوند، که دسترسی برنامه نامیده می شود، تا وقتی که می تواند به دیتاهای خاص دسترسی داشته باشد. این برنامه ها توسط پرسنل کاملا شناخته شده هستند. برنامه هایی که اجازه دستیابی ندارند از دسترسی به دیتاهای خاصی محروم شده و بلاک می شوند.
- کارمندان نیازی به سوئیچ کردن بین اپلیکشین های سازمانی و شخصی ندارند، و همین باعث از بین رفتن وقفه های کاری می گردد.

Windows Defender

کاربران ویندوز ۱۰ هنوز به یک anti-malware جهت محافظت از malware ها نیاز دارند.

Device Guard فقط در برابر برنامه های malicious که درهنگام بوت سیستم باعث ایجاد اختلال می شوند سیستم را ایمن می نماید.

مایکروسافت Windows Defender را قرار داده است تا بحث حفاظت از سیستم را برعهده گیرد. این قابلیت از ویندوز ۸ ایجاد گردید. Windows Defender به صورت خودکار روی سیستم فعال شده و در پشت زمینه سیستم به آرامی اجرا میشود.

این اطمینان خاطر ایجاد می شود که خواه شما یک برنامه جانبی جهت محافظت از سیستم تان انتخاب کرده باشید یا خیر دست کم یک آنتی ویروس حداقلی بر روی سیستم شما وجود دارد. هرچند این برنامه محبوبتی در ویندوز ۷ نداشت، اما در ویندوز ۱۰ این محافظت برای شما الزامی بوده و به آرامی کار مربوط به خود را انجام می دهد.

وقتی می خواهید محافظت از سیستم را غیرفعال نمایید این عمل در Windows Defender بسیار ساده می باشد. وقتی برنامه جانبی حفاظتی بر روی سیستم وجود دارد و شما آنرا پاک می کنید به صورت خودکار Windows Defender فعال می شود، بدین ترتیب دستگاه شما هیچ وقت بدون نوعی از

anti-malware باقی نمی ماند.

قبلا با نام Microsoft Security Essentials می شناختیم. بی سر و صدا اجرا می گردد، تمام فایل ها را اسکن می کند قبل از آنکه شما بخواهید آن فایل را اجرا یا باز نمایید.

اگر فایلی را بعنوان malware یا هر چیزی که برای سیستم و یا فایل های شما یک تهدید محسوب شود پیدا نمایید به صورت خودکار آن را قرنطیه و یا پاک می نماید.

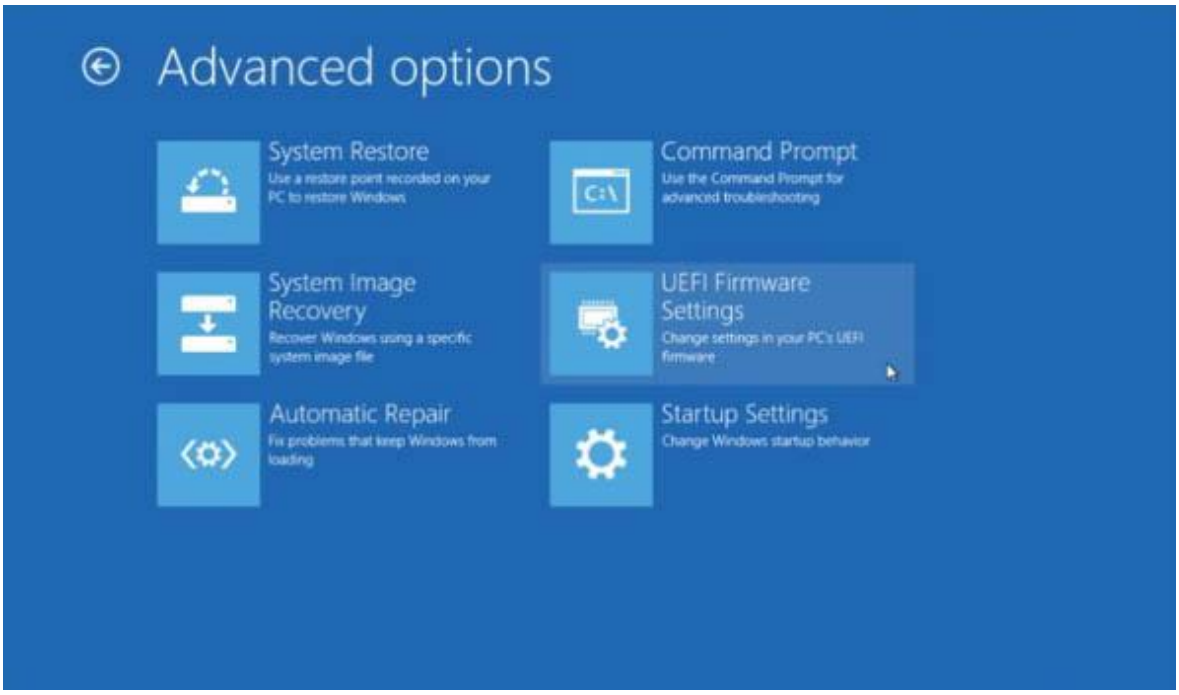
شما یک پیغامی دریافت می کنید مبنی بر اینکه Defender یک Malware شناسایی کرده است و حتما باید پاک شود. آنتی ویروس همراه با بروزرسانی های ویندوز آپدیت می شود و در این پروسه شما نیازی به ریستارت کردن سیستم ندارید.

پیکربندی و استثناها:

تنظیمات مرتبط با Windows Defender با ویندوز ۱۰ ترکیب شده است. دسترسی به تنظیمات از طریق منو استارت، در قسمت Update & Security امکان پذیر می باشد. به صورت پیش فرض و کاملا خودکار فعال شده و به صورت real time وظیفه محافظت از سیستم را برعهده دارد. اگر به هر دلیلی محافظت به صورت real time را غیرفعال نمایید Windows Defender به صورت اتوماتیک مجددا فعال شده تا شما را امن نگه دارد. در هر دو حالت ابری و محافظت با استفاده از نمونه های مشابه به Defender اجازه می دهد تا هر اطلاعاتی را که در حوزه امنیت پیدا کرد به اشتراک بگذارد. مایکروسافت پیشنهاد می کند به صورت کامل بروزرسانی ها انجام و اجازه دهید روند آپدیت و بهبود چرخه ی تولید این نرم افزار صورت بگیرد.

همچنین در این برنامه می توانید فایلهای خاص، فایل تایپ ها، فولدرها و بعضی از پروسس ها را استثنا قرار دهید.

برای مثال اگر در مواردی Defender باعث کاهش کارایی سیستم شما می شود به این دلیل است که اسکن کردن اپلیکیشن ها و فایل ها باعث مصرف منابع می شود، به همین منظور شما می توانید برای بعضی فایل ها و فولدرها استثنا قایل شوید.



Unified Extensible Firmware Interface یا UEFI Secure Boot، نسخه ی بروزرسانی شده ی BOIS می باشد. BIOS که به صورت سنتی و قدیمی جهت استارت شدن یک کامپیوتر دیده میشد.

Secure Boot طوری طراحی شده است تا malware ها در هنگام بوت توانایی ایجاد اختلال در سیستم را نداشته باشند. در گذشته، بعضی از فروشندگان گواهینامه هایی جهت ایجاد پروسه ی بوت امن برای سخت افزارهای خود تهیه میکردند.

سیستم هایی مثل لینوکس و ویندوز به کاربران اجازه می دهند تا پروسه ی بوت امن را خاموش نمایند. با انجام این کار شما درب ها را برای malware ها باز کرده و خوش آمدگویی گرمی با آنها خواهید داشت و باید آماده شوید تا هر نوع صدمه ای به سیستم شما وارد نمایند.

در ویندوز ۱۰، مایکروسافت به صورت شفاف اعلام میکند که قابلیت خاموش کردن این پروسه باید از بین برود و این قابلیت باید همیشه روشن باشد.

این تفکر که با نصب دو سیستم عامل و فراهم آوردن شرایطی جهت بوت دوگانه سیستم ما می توانیم ریسک نفوذ malware هایی را که در هنگام بوت شدن سیستم آنرا آلوده میکنند کاهش دهیم تفکری کاملا اشتباه می باشد و به همین دلیل مایکروسافت اعتقاد دارد که خاموش کردن قابلیت Secure boot غیرمنطقی و نادرست می باشد.

تجزیه و تحلیل تهدیدات امنیتی پیشرفته

امروزه حملات امنیتی بسیار مقاوم، تکرار پذیر و به شدت پیچیده شده اند. بدون در نظر گرفتن مدل دستگاهی که شما از آن استفاده می کنید، فرض کنیم شما مورد حمله قرار گرفته و در حال حاضر بعضی از تهدیدات در سیستم شما نفوذ کرده اند شما نمی توانید نسبت به این موارد چشمان خود را بسته و بی تفاوت از این موضوع عبور کنید.

ارقام زیر بیان کننده ی جدیت داستان امروز ماست :

- برای یک attacker رخنه کردن و باقی ماندن در سیستم شما برای بیشتر از ۲۰۰ روز تا زمان شناسایی امری عادی و معمول می باشد. کارهای زیر توسط آنها صورت می گیرد زیرا با استفاده از ایجاد دسترسی های غیرمجاز، استفاده از اکانت های کاربران و مخفی کردن خودشان درون شبکه این اتفاقات ناخوشایند رخ می دهد.
- تکنولوژی های پیشرفته سبب میشود پیدا کردن و متوقف نمودن این افراد با وقفه صورت پذیرد.
- بیش از ۷۵ درصد رسوخ به یک شبکه در نتیجه ی به خطر افتادن احراز هویت کاربران می باشد. (عدم دقت کاربران در حفظ و حراست از رمزهای عبور خودشان)
- بیش از ۵۰۰ میلیارد دلار برآوردی است از هزینه ی جرایم مجازی که با هدف های مختلفی صورت گرفته است.
- ۳,۵ میلیون دلار متوسط هزینه ای است که هر کمپانی بابت دیتاهای منتشر شده ی خود در اثر رخنه به آنها می پردازد!

در این آشفته بازار مایکروسافت با قابلیت جدیدی با نام Advanced Threat Analytics or Data وارد بازار شد. این ابزاری است جهت شناسایی تهدیدات و رفتارهای غیرطبیعی قبل از آنکه باعث هرگونه صدمه و یا خرابی در سیستم شوند.

چگونگی کارکرد این قابلیت را به شما نشان می دهیم. شما یک کارت اعتباری دارید و شرکت صادر کننده این کارت رفتار شما در هزینه ها را رصد می نماید.

در صورت مشاهده ی هرگونه رفتار مشکوک یا فعالیتی که خارج از رفتار نرمال است ارائه دهنده با شما تماس گرفته تا فعالیت های صورت گرفته را به تایید برساند. حتی این امکان وجود دارد که فعالیت های کارت شما متوقف شود تا زمانی که تایدیه توسط شما صادر گردد. این مفهمومی است که مایکروسافت در نظر دارد برای کاربران پیشرفته ترسیم نماید.

مزایای ATA :

- تهدیدات با آنالیز رفتارهای کاربران شناسایی می شوند. زمانی که تغییری در الگو مشکوک به نظر می رسد اخطاری صادر می شود.
- ATA دائما در حال تغییر است و پیوسته پروسه یادگیری در آن وجود دارد. از رفتارهای مختلف کاربران الگو برداشته و بنا به شرایط جدید خود را آداپته می نماید.
- ATA ریسک های مشخص و بارز را شناخته و پیغام هایی صادر می نماید. مثلا اعلام می کند که داشتن پسوردهای ضعیف، تراست نامطمئن، اعلام نقاط آسیب پذیر و ... ریسک های بسیار بالایی به همراه دارد.
- ATA سبب کاهش False Positive ها می شود.

چگونگی کارکرد:

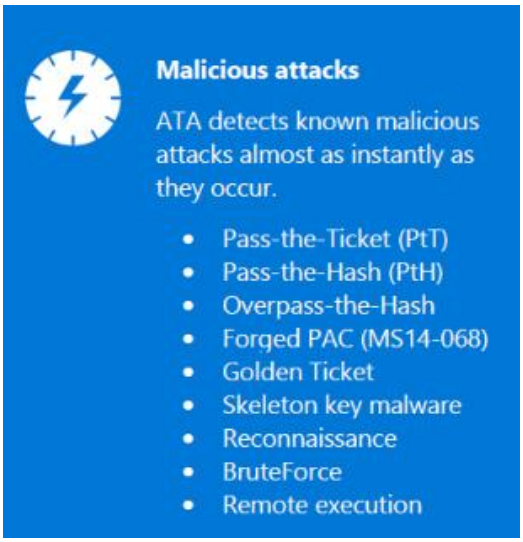
بعد از نصب ATA، تمام پیکربندی Port-mirroring و ترافیک های مرتبط با Active Directory بر روی ATA کپی خواهد شد. توجه داشته باشید که تمام این مراحل مخفیانه صورت می گیرد.

ATA دیتا و کارهایی که با SIEM- Security Information and Event Manager دارد را آنالیز خواهد کرد. تمام دیتاها به صورت لوکال ذخیره میشود.

موتور آموزشی ATA رفتارهای همه کاربران را بررسی کرده و از نوع رفتارهای آنها آموزش های لازم را بدست می آورد سپس از آنها استفاده های لازم را بعمل می آورد. با رفتارهای روزمره شما کاملا آشنا بوده و رفتارهای عجیب و غریب شما را شناسایی می کند.

اگر رفتارهای عجیبی از سمت کاربر اتفاق بیفتد، پرچم قرمز زده شده و تیم های امنیتی آلارم لازم را صادر می کنند، وقتی رفتارهای سابق شما با رفتارهای کنونی تطابق نداشته باشد و غیرطبیعی باشد فرض بر آن است که حملات امنیتی صورت گرفته است.

اینها سبب می شود شانس شناسایی های False Positive ها کاهش یافته و حملات malicious کاهش یابد همان گونه که در تصویر زیر مشاهده می نمایید:



مایکروسافتATA سیستمی است که بی سر و صدا در پس زمینه بدون اینکه آشکار شود کار میکند.

حالت امنیت مجازی Virtual Secure Mode

ویندوز ۱۰ از تعداد مختلفی کانتینر container ساخته شده است، یکی از آنها در سیستم عامل قرار دارد. با این حال توکن امنیتی برای اکتیودایرکتوری اجازه دسترسی به شبکه ی شرکت خودتان را میدهد و از طرفی احراز هویت LSA و سرویس های مرتبط با آن در کانتینرهای جداگانه قرار داشته که در بالای Hyper V اجرا می شوند.

اینها توکن های امنیتی هستند که هدفی برای حملات امنیتی می باشند.

دسترسی ادمین را دارند و برنامه ها را اجرا میکنند، دسترسی به گرفتن توکن ها امکان پذیر است. در شبکه هستند و بدون نیاز به پسورد به سرویس ها دسترسی دارند.

کانتینرها در اصل پدیده ای نو در صنعت تکنولوژی IT هستند. همانطور که می دانید کانتینرها محیط های کاملا ایزوله شده (Isolated)، قابل حمل (Portable) و منابع کنترل شده (Resource Controlled) هستند. در واقع کانتینر ها محل های کاملا ایزوله شده ای هستند که اپلیکیشن های مختلف در این محیط ها، بدون هیچ گونه تاثیر پذیری از سایر محیط های ایزوله شده و حتی اپلیکیشن های سیستم، راه اندازی می شوند.

به صورت خلاصه :

- Virtual Secure Mode پردازش های حساس را در داخل یک Hyper v کانتینر ایزوله میکند.
- VSM ویندوز کرنل را در داخل کانتینر اجرا میکند.
- VSM از کرنل محافظت میکند در زمانی که در معرض خطر می باشد بنابراین توکن ها همه سالم می مانند.

استراتژی امنیت مجازی مایکروسافت:

مجازی سازی در ده ساله گذشته یکی از بزرگترین مباحث مطرح شده در صنعت فناوری اطلاعات می باشد. دلیل این امر هم کاملا روشن و واضح می باشد مزایای حاصله از این امر بسیار زیاد است.

مجازی سازی توانایی استفاده از ظرفیت های سخت افزاری را به صورت بیشتر و بهتر در یک زمان به ارمغان می آورد. قابلیت هایی چون جابجایی ماشین ها بدون نیاز به down time و با آسودگی شما می توانید

ماشین مجازی خود را در چند ثانیه deploy نمایید.تمام این موارد گویا است که بار کاری واحد IT کاهش می یابد.

هدفی در ذهن مایکروسافت است چرا Hyper V را برای deploy سرورها و مدیریت آنها انتخاب کنیم ؟ آنها در نظر دارند تا تمام موارد را در سطح نرم افزاری انجام بدهند. آنها به کاربران این قابلیت را میدهند که توانایی خودکارسازی بسیاری از کارها را در دیتاسنتر داشته باشند و با انجام این موارد شاهد تاثیرگذاری زیادی خواهیم بود.

در نسخه های جدید ویندوز سرور، مایکروسافت مسیر مناسبی را طی کرده تا Hyper V را بهبود ببخشد و تولد دوباره ای برای آن ایجاد کند تا شاهد پشتیبانی تمام عیار از تکنولوژی با تعریف نرم افزار در دیتاسنترها باشیم.

در دو نسخه آخری از ویندوز سرور فضاهای ذخیره سازی، IP آدرس های قابل مدیریت و multi-tenant site to site vpn معرفی شده است.

سرور ۲۰۱۶ بر اساس قابلیت های بیان شده ریلیز خواهد شد همراه با قابلیت های بیشتری مثل storage Replica

بهبود بخشیدن امنیت

در طراحی ویندوز سرور ۲۰۱۶ ما شاهد نکات امنیتی بسیاری هستیم که در جهت محافظت بیشتر از VM ها در Hyper V طراحی شده اند. این نکات امنیتی در جهت جلوگیری از فعالیت Malware ها و حملات مخرب دیگر بوجود آمده اند.

مایکروسافت کاملا آگاه است که یکی از بزرگ ترین دلایلی که رایانش ابری هنوز همه گیر نشده است با توجه به پیش بینی هایی که کرده بود و هنوز شرکت های بزرگ به این سرویس اعتماد ندارند.

مایکروسافت تصمیم گرفته تا این سرویس را برای همه بهبود ببخشد هم برای شرکت ها هم برای مصرف کنندگان راهکار ابری می تواند پیشنهادی برای امنیت دیتاسنترها باشد تا کمترین خطر را آنها تجربه کنند.

ویندوز سرور ۲۰۱٦ پیشنهاد پشتیبانی از یک TPM مجازی که بر روی VM است را میدهد.

مزیت اصلی این قابلیت فعال سازی BitLocker برای همه ی ماشین های مجازی است، دسترسی غیرمجاز به هر فایل و یا درایوی را متوقف میکند.

در ویندوز سرور ۲۰۱٦ قابلیت امنیتی جدیدی ایجاد شده است که اجازه می دهد VM از هاست به صورت مجزا محافظت شود.

در این سناریو، مادامی که ادمین می تواند متوقف / شروع کند شیلد مربوط به ماشین مجازی را هیچ گونه تغییر در پیکربندی صورت نمی گیرد. اتفاقاتی که در سطح دیسک و پروسس ها صورت میگیرد فقط مانیتور می شود.

این یک راهکار جالبی است برای مشتریانی که تمایل ندارند کسی متوجه شود که روی VMها چه اتفاقاتی در حال رخ دادن می باشد.

در حال حاضرمدیریت هویت افراد در سازمان های بزرگ کار دشوار و سنگینی می باشد.

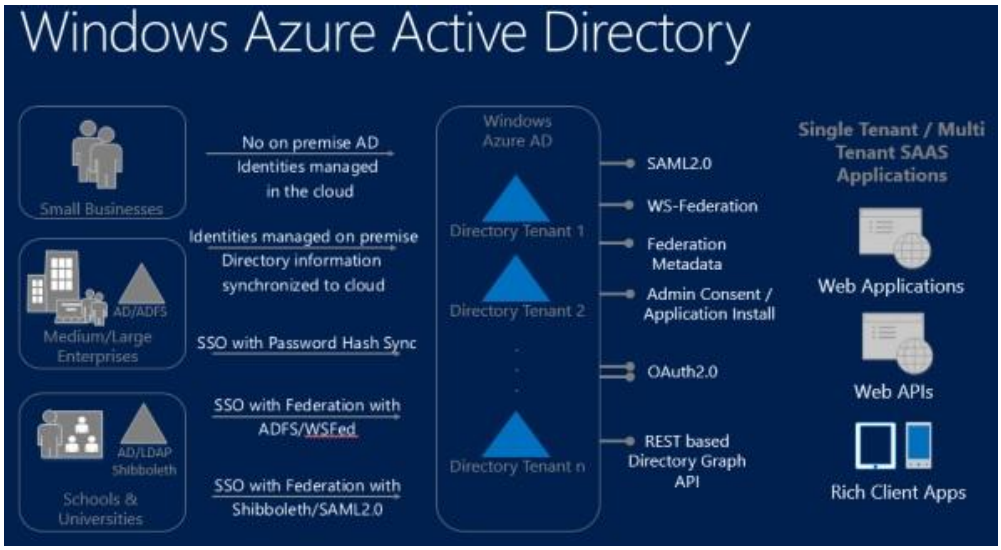
ویندوز ۱۰ به پیشواز تغییراتی در این زمینه رفته است و اجازه توانمند شدن موبیلیتی پیشرفته را می دهد. راهکارهایی که پیاده سازی میکند شامل: همه کاربران کمپانی تمایل دارند تا از هر دستگاهی به هرجایی و به هر چیزی دسترسی داشته باشند.

مدیران تمایل دارند همه چیز را کنترل کنند; مطمئن شوند که دیتا امن و محافظت شده است. که همین امر مشکل زا خواهد شد. زیرا کاربران برای ورود به هر سایتی از پسوردهای یکسان استفاده میکنند.

در حالی که ممکن است برای شروع همه چیز ساده باشد، وقتی تقاضای تغییر پسورد داده می شود همه چیز درهم ریخته می شود.... کاربر نهایی تمام پسوردهای متفاوت را به خاطر می سپارد.

ویندوز ۱۰ همه چیز را تغییر داد. در استراتژی موبیلیتی سازمانی هویت افراد نقش اصلی و اساسی را بازی می کند. در حال حاضر اغلب سازمان ها استراتژی هویت سنجی در همان محل سازمان را دارند، استفاده از اکتیو دایرکتوری و دیگر دایرکتوری ها و داشتن فایروالی که در خود سازمان نصب شده است.

دسترسی به اپلیکیشن های ابری در زیرساخت مجزا وجود دارد. ویندوز ۱۰ چیزی را با خود به ارمغان آورده است یک تغییر کوچک که در کل اتفاقات خوب بسیاری به همراه خواهد داشت.



این تغییر Azure Active Directory نامیده می شود و در کنار هم قرار دادن هویت سنجی در همان مکان و یا دسترسی از طریق کلود را به همراه دارد.

تمام چیزهایی که نیاز دارید در یک ارتباط ساده با هم متصل می شوند. در ویندوز ۱۰ تمام ابزارهایی که شما لازم دارید جهت اتصال فراهم می شود.

مواردی که Azure AD به شما می دهد شامل SSO تمام کاربران سازمانی می باشد که با این روش می توانند به تمام چیزهایی که نیاز دارند دسترسی داشته باشند. قبل از اینکه ما به سمت معرفی امکانات بیشتری برویم کمی در مورد Azure Active Directory وقت بگذاریم تا آشنایی بیشتری در مورد این قابلیت پیدا کنیم.

واقعا چیست ؟!

ADD راهکار شناسایی و دسترسی مدیریتی می باشد که:

- سرویس دایرکتوری
- اداره پیشرفته
- مدیریت دسترسی به برنامه
- پلتفرمی استاندارد که برای developer ها ایجاد گردیده است.

آژور AD به کاربران این امکان را می دهد که با SSO به چیزی در حدود ۱۰۰۰ برنامه دسترسی داشته باشند. از آن بهتر این امکان می باشد که به شما اجازه می دهد مشخص نمایید هر برنامه چه ویژگی هایی داشته باشد! (چه ویژگی هایی از برنامه فعال شود.)

:ADD

- **آسان برای استفاده** : با یک راه حل ساده و آسان مدیریت شناسایی و دسترسی ها به اپلیکیشن های سازمانی و سرویس ها رخ می دهد، هم برای کسانی که داخل سایت هستند هم برای کسانی که روی cloud هستند. در حال حاضر بیش از ۲۰۰۰ برنامه با پشتیبانی از SSO مجددا ادغام شده اند تا در جهت تجمیع آسان با برنامه های شما باشند.
- **طراحی جهت قدرتمند کردن کاربران:** بوسیله اجازه دادن به کاربران جهت وارد شدن با اکانت کاری یا اکانت شخصی برای دسترسی به برنامه های ابری یا برنامه های موجود در سازمان . با قابلیت سرویس های مشخص که به کاربر اجازه می دهد بسیاری از کارهایی که مربوط به Admin می باشد را خودش انجام داده و نیازی به حضور helpdesk نباشد.
- **طراحی کردن با ایجاد افزایش امنیت در ذهن:** کمپانی شما می تواند با دادن دسترسی های مناسب و درست کار محافظت از دیتاهای ابری یا دیتاهای موجود در سازمان را تضمین نماید. شما می توانید سیستم هایی که فعالیت های غیرمعمولی دارند را رصد نمایید و تهدیدات امنتیتی را شناسایی کنید.
- **ایجاد هویت های ترکیبی:** این خصوصیت به شما اجازه می دهد تا دایرکتوری های موجود در سازمان را ادغام کرده و کارمندان می توانند به منابع سازمانی به هر دو صورت امن و مداوم دسترسی داشته باشند. فقط با یک اکانت مشخص. ADD می تواند در زیرساخت حال حاضر، سرویس های شخصی، ابزارهای امنیتی و برنامه های اتصال مورد استفاده قرار گیرد.
- **راه اندازی جهت ایجاد کردن یک گزارش جامع تجزیه و تحلیل:** سیستمی که باعث افزایش امنیت می شود و اجازه مانیتور کردن میزان استفاده از کارهای سازمانی را می دهد.

شناسایی برنامه های ابری

Cloud app discovery اجازه مانیتور برنامه های ابری را می دهد. در حال حاضر، به طور میانگین، در حدود ۱۰ بار یا بیشتر برنامه های ابری توسط واحد فناوری اطلاعات استفاده می شوند.

Cloud App Discovery به شما نشان می دهد که کدام برنامه در حال استفاده بوده و چه کسی سرگرم استفاده از آن است همچنین زمان استفاده هم نشان داده می شود. شما می توانید از جزئیات گزارش به صورت مستقیم خروجی بگیرید.

مدیریت دایرکتوری در Cloud

قابلیت مفید دیگری که در ADD گنجانده شده است مدیریت شناسایی مایکروسافت Microsoft Identity Manager می باشد. این قابلیت به شما اجازه می دهد تا مدیریت هویت سنجی را در همان مکان انجام داده و به دایرکتوری آژور متصل شوید.

در حال حاضر بیش از ۲۴۰۰ برنامه ی SaaS وجود دارد که این برنامه ها می توانند با برنامه های دلخواه ما اضافه و یا ادغام شوند.ADD بعنوان یک واسط قرار گرفته و وظیفه ی هویت سنجی و میزان دسترسی از دستگاه های موبایل و کامپیوترها را بر عهده دارد.

ADD App Proxy شامل یک متصل کننده می باشد که به صورت خودکار به کلود متصل شده و اجازه همگام سازی با امنیت بالا را می دهد.

ADD شامل یک کنسول مدیریت جامع جهت فراهم سازی دسترسی مرکزی ادمین به تمام اپلیکشن ها می باشد که شامل ادغام سازی مجدد برنامه ها و بقیه ی اپلیکیشن های ابری می باشد.

زندگی کاربران بسیار راحت تر خواهد بود زیرا :

- ✓ کاربران در گروه های مختلفی قرار گرفته و این گروه ها به برنامه های متفاوتی دسترسی دارند.
- ✓ تنظیم اکانت های ویژه برای برنامه های خاص. این روش از بوجود آمدن اشتراک گذاری فایل ها جلوگیری میکند.
- ✓ ادمین سیستم کاربران را ایجاد و یا غیرفعال می کند. اگر کاربری از سازمان خارج شود از گروه خود بیرون می رود و به صورت خودکار غیرفعال می شود و این خروج باعث غیرفعال شدن تمام دسترسی ها به برنامه ها می شود.

بعضی دیگر از قابلیت های امنیتی که وجود دارد عبارت اند از :

- ✓ گزارش امنیتی که وظیفه مانیتور کردن و شناسایی دسترسی های متناقض با الگو های تعریف شده را برعهده دارد.
- ✓ فرصتی برای ادمین تا یک برنامه را با multi-factor هویت سنجی نماید. مثلا زمانی که به یک کاربرمشکوک می شوند که آیا خودش وصل شده است یا خیر می توانند به راحتی پروسه ای را اضافه نمایند. این قدم میتواند یک تماس تلفنی و یا یک پیغام نوشتاری باشد.

- ✓ پالس های دسترسی به موقعیت جغرافیایی کاربر، دستگاه و عضویت در گروه های مختلف بستگی دارد.

چگونه ویندوز ۱۰ مایکروسافت از شما محافظت خواهد کرد

محافظت کردن از شما، قسمتی است که مایکروسافت گام بلندی در آن برداشته است. آنها سخت کار میکنند تا با ایجاد راه حل های جدید از دیتا و اطلاعات شما محافظت نمایند.

دزدی دیتاها جدی ترین و سریالی ترین بخش برای مشتریان و سازمان ها می باشد. سیستم های امنیتی حال حاضر فقط از حدود نیمی از دیتای شما محافظت می کنند و امکان محافظت از دیتا به صورت کمال و تمام وجود ندارد.

هر زمانی که شما به وسیله ی موبایل و یا کامپیوترتان به اینترنت متصل می شوید و یا یک ایمیل را چک میکنید با ریسک های زیادی مواجه هستید و ممکن است یک هکر به شما صدمه بزند. مایکروسافت در تلاش است تا این ریسک ها را به حداقل برساند.

وقتی دیتا از سیستم پاک میشود مایکروسافت چیزی به اسم Azure rights Management and Information Rights Management دارد. این قابلیت به شما کمک شایانی در زمینه محافظت از دیتاها و مستندات پاک شده میکند .

وظایف مدیریتی Azure

کاربران بسیاری از وظایف مدیریتی خودش را با دیدن سایت http://myapps.microsoft.com می تواند انجام دهد و یا از طریق برنامه های اندروید و iOS این قابلیت ها وجود دارد. از طریق این امکانات کاربران می توانند با دستگاه های مختلف به برنامه های متعددی دسترسی داشته باشند.

Azure Active Directory در داخل ویندوز ۱۰ وجود دارد و چند گزینه بر اساس نیاز شما وجود دارد:

- Free
- Basic
- Premium

مایکروسافت زمان و هزینه ی زیادی را برای بهبود ADD صرف کرده است که نتایج زیر ماحصل این فرآیندها بوده :

- Admin Units – قابلیت جداسازی وظایف ادمین ها در گروه ها

- Business to Business – قابلیت جدیدی که در جهت به اشتراک گذاری منابع با پارتنرهای تجاری با استفاده از ADD ایجاد گردیده است.
- B2C –
- Conditional Access – قابلیت بلاک کردن دسترسی های خارجی
- مدیریت هویت سنجی – گزینه هایی که دسترسی ادمین به منابع دلخواه را ایجاد میکند
- ADD Join – کنترل ADD که به صورت کامل در ویندوز ۱۰ وجود دارد.

محافظت از دیتا در Azure

تمامی حملات سایبری در حال رشد می باشند و هزینه هایی که افراد در این رابطه متحمل می شوند به طور فزاینده ای در حال افزایش می باشد. تخمین زده می شود که ۱۵ الی ۲۰ درصد این جرایم در محیط اینترنت ایجاد می شود.

طبق گزارش های ثبت شده در دو سال گذشته فقط در کشور انگلستان بیش از ۸۰ درصد تجارت های بزرگ و ٦۰ درصد تجارت های کوچک مورد حملات سایبری قرار گرفته اند. که در سال ۲۰۱٤ به میزان ۳٤ درصد رشد داشته اند. تخمین زده می شود که هزینه ی حملات سایبری در حدود ۳ تریلیون دلار بوده است.

به این ترتیب و به منظور محافظت از دیتاهای کاربران و مشتریان مایکروسافت اقدامات امنیتی را در Azure AD درنظر گرفته است.به صورت پیش فرض ADD محافظت از مشتری ها را در اولویت قرار داده است و کاربران باید این قابلیت های امنیتی را فعال نمایند. ابتدا نیم نگاهی به وضعیت جابجایی دیتاها در این سرویس داشته باشیم :

وقتی دیتایی بین کاربر و این سرویس جابجا میشود کاملا از پروتکل https استفاده می شود و دیتا به صورت رمزنگاری شده منتقل می گردد.

تمام دیتاهای import وexport شده توسط BitLocker و با استفاده از ویندوز ۱۰ رمزگذاری می شود. همچنین دیتاهای مشتریان که بر روی تجهیزات ذخیره سازی و دیتاسنتر مایکروسافت قرار دارد با الگوریتم های پیشرفته رمزنگاری می شود.امکان انتخاب بین دو پروتکل http و https توسط مشتریان وجود دارد که توصیه مایکروسافت استفاده از https می باشد.

اگر یک مشتری ارسال دیتا را توسط وب کلاینت انتخاب نماید حتما باید TLS را پیاده سازی کرده باشد. TLS: Transport Layer Security پروتکلی است که به برنامه های جانبی اجازه نمی دهد که قابلیت رهگیری یا استراق سمع را روی دیتاهای رد و بدل شده را داشته باشند.

وقتی ما در مورد دیتا صحبت میکنیم، صحبت ما در مورد دیتایی است که بر روی یکی از کانتینرها قرار دارد. کانتینرهای مایکروسافت شرایط حفاظت شده ای را برای دیتا بوجود می آورند که بر اساس لیست زیر می باشد :

Virtual Machine – Windows / Linux

رمزگذاری دیسک Azure با استفاده از BitLocker برای ویندوز و DM-Crypt برای لینوکس. Virtual Hard Drive هم برای ویندوز و هم برای لینوکس رمزگذاری می شوند. مشتری این آپشن را دارد که رمزگذاری را در سطح بوت و volume ایجاد نماید. کلید رمزنگاری در key vault نگهداری می شود.

چطور کار میکند

- مشتری VHD رمزنگاری شده خود را در استورج اکانت Azure خود قرار میدهد.
- آماده سازی کلید رمزگذاری BitLocker یا passphrase لینوکس در VM key value.
- در این قسمت کدگذاری در سطح دیسک انجام می شود.
- سرویس مدیریتی آژور با استفاده از key value بروزرسانی می شود و تنظیمات رمزنگاری می گردد.
- آماده سازی پلتفرم رمزنگاری ماشین مجازی

Key Value Security

گردش تمام موارد در انتها به key Value می رسد. این کلید کجا ذخیره شده است ؟ کلیدهای رمزنگاری هستند که از دیتاهای شما محافظت می کنند. این کلیدها در شرایط ایزوله نگهداری می شوند بنابراین محل ذخیره این کلیدها همیشه در معرض تهدید می باشد ولی باید در نظر داشته باشید که امکان دزدیده شدن دیتا در حد و اندازه ی یک کپی بوده که بدرد هیچ دزدی نمیخورد زیرا فقط کلیدها می توانند دیتا را رمزگشایی کنند.

توجه به نکات زیر بسیار مهم می باشد:

- فقط مشتری دسترسی کنترلی به کلیدهایی که در value خصوصی اش موجود هستند را دارد .

- مشتری می تواند قابلیت مانیتورینگ را در اکانت خودش فعال کند تا تمام فعالیت ها لاگ شده و مانیتورینگ لازم صورت پذیرد. این امر سبب میشود که متوجه شویم چه کسی جهت دسترسی به vault تلاش کرده است.
- دیسک های رمزنگاری شده در فضای مربوط به اکانت مشتری ذخیره می شوند و فضای آژور به صورت خودکار آنها را replicate میکند. مشتری بر روی تعداد کپی ها کنترل کاملی دارد.
- آژور به صورت پیش فرض به Key Value ها دسترسی ندارد. مشتری باید دسترسی read / Write بدهد.
- آژور دسترسی به دیسک های رمزنگاری شده در Value ندارد.

ذخیره سازی آژور– Blobs, Tables, Queues

رمزنگاری سمت کلاینت این مزیت را دارد که کاربر قبل از بارگذاری دیتا آنها را رمزنگاری می نماید و سپس بر روی آژور خود قرار داده و اقدام به رمزگشایی می نماید. همین امر سبب امن ماندن کلیدها می شود از نکات مثبت دیگر این کار سرویس ذخیره سازی هیچ گاه کلیدها را مشاهده نمی کند و همین امر سبب می شود امکان رمزگشایی دیتاها کاملا از بین برود. برای دیتاهایی که در سرویس های ابری قرار میگیرند این روند بدین گونه می باشد که دیتا در محل رمزنگاری شده و یک نسخه پشتیبان هم در آژور نگهداری می شود.

SQL سرور و SQL دیتابیس

استفاده از TDE – Transport Data Encryption – تکنولوژی می باشد که محتوایی که قرار است وارد دیتابیس شود با استفاده از یک کلید رمزگذاری encrypt می نماید. این کلید از الگوریتم AES-256 استفاده میکند.

این کلید با یک سرویس مدیریت گواهینامه محافظت می شود که توسط SQL Database سرور محافظت می شود. certificate در یک چرخه ۹۰ روزه تنظیم شده است بعد از اینکه certificate جدید تولید شد قبلی از بین می رود و همین امر ریسک در معرض خطر قرار گرفتن دیتابیس را به حداقل مقدار خود می رساند.

HDInsight از فضای آژور استفاده کرده و SQL آژور دیتابیس شما را رمزنگاری میکند تا حفاظت از دیتاها را تضمین نماید همچنین نسخه های پشتیبان به صورت منظم و درست از دیتابیس های شما تهیه می شود تا دیتایی از بین نرود.

کنترل دسترسی و Auditing :

بنابراین، مایکروسافت Azure AD رمزنگاری و محافظت از تمام دیتاهای شما را انجام داده است و کلیدهای مربوط به رمزنگاری در مکانی امن ذخیره شده که فقط شما به آنها دسترسی دارید. هنوز تعداد زیادی از ریسک های مهم وجود دارند.

کاهش خطر حمله به حساب های کاربری:

مشکل اصلی و کلیدی در امنیت authenticationهای ضعیف می باشد. پسوردهای ضعیف، پسوردهایی هستند که نوشته می شوند و یا به اشتراک گذاشته می شوند و یا پسوردهای دزدیده شده بزرگ ترین راه حمله برای یک هکر می باشند. مایکروسافت به دنبال راهی جدید در تمام محصولات خود است تا کاربران پسوردها را کنار گذاشته و فاکتورهای جدیدی برای authentication داشته باشند.

تمام اکانت های کاربری با استفاده از Azure MFA می تواند امن شود، با استفاده کردن از سرویس های اکتیو دایرکتوری federation و Azure Active Directory همچنین استفاده از تماس و یا تکست مسیج راهی است برای احراز هویت ثانویه تا کاملا مطمئن و امن کار انجام شود. کاربران می توانند از PKI جهت محافظت از اکانت های خود و با استفاده از زیرساخت ADFS استفاده نمایند.

محدودیت Permission

یکی از سخت ترین مفاهیمی که از قدیم وجود داشته بدست آوردن بیشترها است اما بحث permission کم ترین ها را ایجاب می نماید. به طور مثال: دسترسی در صورتی داده می شود که یک رول مشخص و خاص ایجاد گردد. Azure RBAC- Role Based Access Control در حال حاضر شامل ۲۰ رول مختلف و متفاوت می باشد که به کاربران بر اساس owner ها و Contributor ها داده می شود.

Owner ها به دیتا دسترسی کامل دارند. مشارکت کنندگان می توانند به ownerها اضافه شوند با این تفاوت که امکان انجام کاری را ندارند.Reader ها امکان خواندن دیتا را دارند و هیچ تغییری را نمی توانند اعمال کنند.

Privilege Accounts:

کاربران ویژه Super USER ها شرایط مدیریت ویژه را دارا می باشند به این خاطر که آنها یکسری ویژگی های خاص را ایجاد می کنند. JIT-Just in Time را می توانند فعال نمایند. از بین بردن ریسک یک حمله از طریق ایجاد مجوز یا ایجاد دسترسی های مناسب.

JIT به یک کاربر دسترسی ادمین را می دهد این دسترسی در زمانی ایجاد می شود که آنها برای یک مدت کوتاهی به این وضعیت نیازمند هستند و فقط این دسترسی کارشان را راه می اندازد. مدیران تنظیم کردن بعضی قابلیت هایی مانند Azure AD PIM را دارند. Privilege Information – PIM Management.

این جایی است که آنها می توانند سیستم را مانیتور کرده، ببینند چه کسانی دسترسی دارند و چه کسانی تمایل به دسترسی دارند و سیاست هایی را اتخاذ کنند که امکان انتقال دسترسی دائمی به موقت وجود داشته باشد.

استفاده از Auditing و Logging، مدیریتی که فعالیت های مخرب را شناسایی میکند که این شامل : لاگ های نامنظم، Down شدن های سطح کاربر، که از طریق استفاده از ابزارهای شناسایی پیشرفته که به طور مداوم نظارت بر تمام حساب های کاربری دارد. در این روش تهدیدات شناسایی شده و جلوی آنها گرفته می شود قبل از اینکه آنها تبدیل به یک مسئله و مشکل شوند.

Operation Management Suite

یکی دیگر از قابلیت های بیشمار در ویندوز ۱۰ میباشد که در جهت ساده سازی مدیریت IT طراحی و توسعه پیدا کرده است.

یک سرویس مدیریتی چندگانه می باشد که از Azure AD ، AWS، VMware، OpenStack، Linux و ویندوز سرور پشتیبانی می نماید و نقش اتصال دیتاسنتر و سرویس های ابری را با محلی که کاربر در آنجا حاضر است را برعهده دارد. به مدیران IT یک پورتال داده که اجازه جمع آوری دیتا، آنالیز و جستجو در میان هزاران قسمت از دیتاها و رکوردهایی که به صورت جداگانه وجود داشته و شرایط کاری سرورها را می دهد.

این روزها اطلاعات زیادی وجود دارد، دیتای زیادی موجود می باشد و برنامه های زیادی که بر اساس زیرساخت های متفاوتی مثل سرویس های ابری منتشر شده است. مشکل بزرگ از آنجا شروع خواهد شد که سعی کنیم متوجه شویم که چگونه این سرویس های و دیتاها هندل می شوند؟

مدیران IT هنوز وظایفی در مورد مدیریت و امن سازی دیتاها دارند، بدون در نظر گرفتن این نکته که دیتاها کجا نگهداری می شوند. البته باید توجه داشت که OMS کارها را بسیار راحت می نماید.

مزایایی که OMS در اختیار ما میگذارد:

آنالیز لاگ ها: جمع آوری و جستجو در میان تعداد زیادی از ماشین هایی که سورس دیتاهای شناسایی بوده و وقتی که مشکلاتی در زمینه عملیات راست آزمایی ایجاد می شود.

در دسترسی پذیری: بدون در نظر گرفتن سرورها و اپلیکیشن هایی که وجود دارند OMS شامل ادغام تمام آنها برای ریکاوری می باشد که به صورت پیش فرض فعال شده است.

خودکارسازی: مجموعه ای از پیچیدگی ها و فعالیت های تکراری جهت فراهم شدن کارآمدی بیشتر و مقرون به صرفه شدن مدیریت سیستم ابری

امنیت: توانایی مانیتور کردن و شناسایی وضعیت Malwareها و پیدا کردن سیستم های از دست رفته و پیاده سازی آنها، جمع آوری رخدادهای مرتبط با امنیت برای تجزیه و تحلیل وضعیت

Extended System Center: OMS با سیستم سنتر حال حاضر شما ترکیب شده تا ظرفیت ها را گسترش پیدا کرده تا مدیریت سیستم ابری با هر دیتاسنتر دیگری به صورت کامل ترکیب شده و تحویل گردد.

Hybrid and Open: در حال حاضر بسیاری از سازمان های کوچک در یک دیتاسنتر قرار گرفته اند و OMS با استفاده از سرویس ابری مدیریت می شود، این سرویس بدون در نظر گرفتن توپولوژی یا تکنولوژی که در حال استفاده می باشید ترکیب شده و نتیجه خوبی را برای شما به ارمغان می آورد.

تمام این موارد سبب می شود که محافظت از دیتاهای شما انجام و جلوگیری از نقض دیتا آسان تر از قبل صورت پذیرد.

امنیت موبایل:

این روزها، ما نه تنها از دستگاه های خودمان برای کاربردهای شخصی استفاده می کنیم بلکه از آنها استفاده های تجاری و شرکتی هم داریم.

کارمندان شرکت ها برای کارهای مرتبط با شرکت از اسمارت فون ها و تبلت ها خیلی، خیلی استفاده می نمایند و ویندوز ۱۰ موبایل جهت جداسازی کاربردهای شخصی و کاری طراحی شده است به طوری که شما می توانید سطوح امنیتی و کنترلی را برای کاربردهای شخصی و کاری کاملا تفکیک نمایید.

دستگاه های موبایل هدف شماره یک جهت حملات سایبری می باشند و در حال حاضر حفظ و محافظت از آنها بسیار مشکل می باشد.

مایکروسافت لایه های امنیتی قابل توجه ای را به دستگاه های موبایلی تحت پلتفرم ویندوز اضافه کرده است. از هر تعدادی حملات malware و malicious تا اجازه دادن به کاربران مبتدی و پیشرفته تا کمی خیالشان راحت باشد و متوجه شوند که وضعیت امنیت سیستم آنها تحت کنترل بوده و شرایط خوب است.

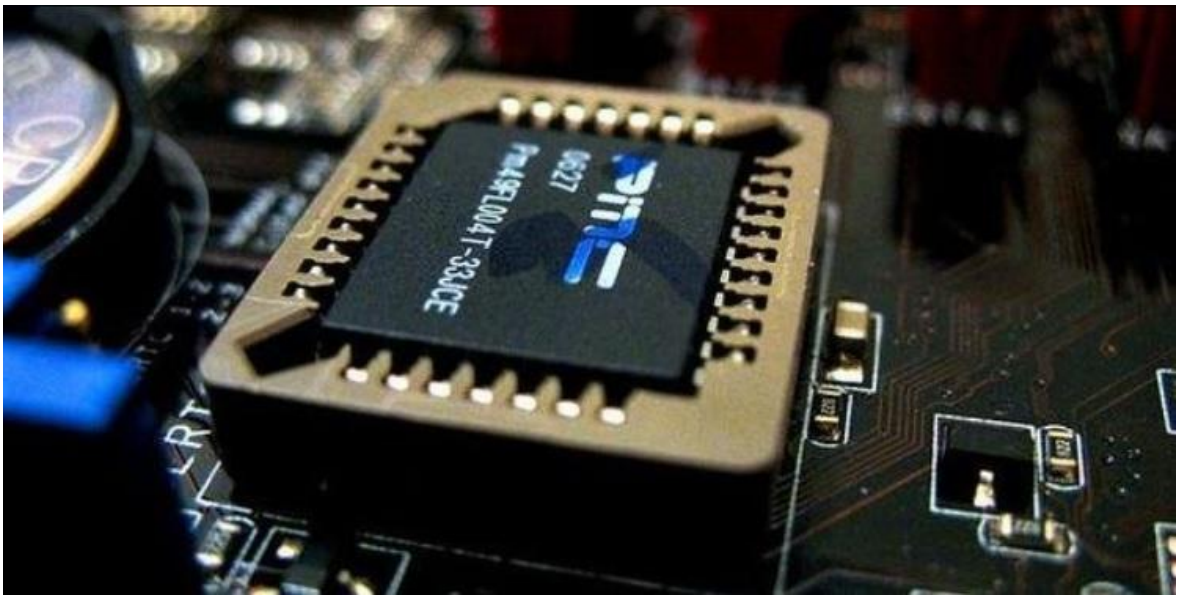
اولین خط دفاعی جهت حفظ امنیت سخت افزار می باشد. همه دستگاه های جدید ویندوزی به چیپ TPM نسخه ۲,۰ مجهز شده اند و قابلیت Secure Boot آنها فعال شده است. این یکی از الزامات ویندوز بوده و کسی نمی تواند آنرا Disable نماید.

UEFI Secure Boot System طوری طراحی شده که به محض روشن شدن سیستم TPM و فریمور سیستم را چک میکند و از صحت نرم افزارهای سیستم مطمئن می شود چک کردن نرم افزارها از طریق genuine بودن و sign بودن آنها صورت میگیرد.

اگر مراحل ذکر شده درست نباشد چیزی اجرا نمی شود به همین سادگی! یکبار که اعلام شود همه چیز برای آغاز بکار سالم است، UEFI در داخل Windows Boot Manager و سیستم عامل بوت خواهد شد.

تنها استثنایی که در این حالت وجود دارد برای زمانی است که سیستم نمی تواند از طریق ویندوز بوت شود و باید با استفاده از نرم افزارهای ریکاوری عمل بوت شدن صورت پذیرد، در این موارد، بوت منیجر از داخل فلش بوت خواهد شد.

چطور امنیت در UEFI وجود دارد؟ در طول فرآیند تولید، یک تعدادی از کلیدعمومی hash شده اند. این hash ها به پروسس هایی در داخل دستگاه لینک شده اند.



همه درایورها، لودرها، برنامه ها و فریمور در داخل UEFI باید signed شده و دیتابیس UEFI تمام کلیدها را لیست میکند، image hashes و CA مشخص می کنند که تراست هست یا خیر.

سیستم rollback امن یکبار UEFI سیستم را چک میکند و اعلام میکند که همه چیز امن بوده و همه چیز Genuine می باشد، rollback امن حالتی است که از بازگشت به هر نسخه ای از سیستم عامل که با حالت اولی فرق دارد جلوگیری میکند، به طور کاملا موثر malware ها را متوقف کرده و اجازه نمی دهد خودشان را مخفی کنند و هنگام بوت شدن با فایل های سیستم عامل لود شده و سیستم را آلوده نمایند.UEFI توسط آپدیت های ویندوز بروزرسانی می شود و تقریبا می توان اطمینان داشت که همیشه آپدیت است.

سایر موارد امنیتی در بحث سخت افزار شامل TPM می باشد که قبل تر در مورد آن سخن بسیار گفته شد و زمانی که کلیدها از سیستم عامل ایزوله شده اند. این بدین معنی می باشد که اگر سیستم به هر دلیلی مورد حمله قرار بگیرد آن کلید مورد دستبرد قرار نمیگیرد حتی سیستم عامل هم به کلیدها دسترسی ندارد.

لایه محافظتی سخت افزاری سلامت کامل را تضمین می نماید. تصمین صحت کارکرد و بهبود آن از نسخه ویندوز ۸,۱ ببعد بسیار بهبود یافته است.

قابلیت هایی که چک شده است شامل Secure Boot،BitLocker و سایر قابلیت های ضروری عملیاتی که باید به صورت صد در صد اوکی باشند تا ویندوز ۱۰ به صورت کامل اجرا شود.

لایه ی بعدی امنیتی ویندزو one Core می باشد. تست های اولیه بر روی پلتفرم اپلیکیشن ها بود. به این خاطر که کاربران چه عکس العمل هایی نشان می دهند وقتی ویندوز ۱۰ بر روی موبایل های آنها مورد استفاده قرار می گیرد.

ویندوز ۱۰ فقط از اپلیکیشن های جدید و یا RT که وابسته به سیستم می باشند پشتیبانی می نماید. لایه امنیتی جدید برای پلتفرم اپلیکیشن مدل چیزی شبیه به موارد زیر می باشد:

- سیستم عامل در TCB اجرا می شود –Trusted Computer Base–کسی به آن دسترسی نداشته و نمی تواند تغییری در آن ایجاد نماید.
- برنامه هایی که بوسیله ی استور یا shipped شدن با یک دستگاه دیگر install شده اند. وقتی برنامه در داخل یک Chamber قرار می گیرد به آن یک دسترسی بر اساس نیاز داده می شود. دسترسی ها توسط هر کاربری قابلیت تغییر ندارند و فقط با یک بروزرسانی تغییر در آنها صورت می گیرد.
- ویندوز ۱۰ برای موبایل همراه با تعدادی برنامه ی از قبل نصب شده ارائه خواهد شد که به شرح زیر می باشد:

تمام این برنامه ها جدید بوده و کاملا بروزرسانی می شوند با قابلیت های جدیدی که مایکروسافت در اختیار کاربران قرار داده است مثلا جهت بروزرسانی نیازی به اوپراتورهای موبایل نمی باشد آنها با استفاده از ویندوز آپدیت بروزرسانی می شوند. این قابلیت Windows As Service نامیده می شود.

دسترسی به برنامه ها و سرویس ها همیشه منجر به نگرانی هایی در حوزه های امنیتی می شود. مایکروسافت تعدادی از قابلیت های جدید را اجرا کرده که در هر دو حالت دیسکتاپ و موبایل امنیت را بسیار افزایش داده و دسترسی های کاربران را امن می نماید.

کاربران زیادی از کلمه عبور حال حاضر سیستم خودشان ناراضی می باشند. به این خاطر که باید کلمات عبور زیادی را به خاطر بسپارند. بیشتر افراد تمایل دارند تا پسوردهای مشابهی را در همه جا داشته باشند. مکان های زیادی وجود دارد که نیاز به ID های مختلف و متفاوتی دارند که شما باید یک دفترچه راهنما برای دسترسی های متفاوت با اشکال مختلف داشته باشید !!!

شرکت ها تمایل دارند کنترل بیشتری بر روی کاربران داشته باشند این امر مداخله در حریم خصوصی کارمندان نمی باشد بلکه تشخیص تهدیدات بالقوه و جلوگیری از درز اطلاعات می باشد. در اینجاست که مایکروسافت با ویندوز Hello وارد می شود.

همه ی ما مطلع هستیم که نسخه دیسکتاپ و موبایل شبیه یکدیگر می باشند، به صورت خلاصه:

- Windows Hello یک سیستم بایومتریک می باشد.
- مورد استفاده آن کم رنگ کردن شناسایی صورت یا اثرانگشت می باشد.
- نیاز به سخت افزارهای جدیدی برای تولید و تکمیل این تکنولوژی می باشد. امروزه موبایل ها قابلیت تشخیص صورت را نداشته و نمی توانند جزئیات را شناسایی کنند. بعضی از دستگاه ها قابلیت تشخیص اثرانگشت را دارند اما قابلیت Windows Hello نیاز به بروزرسانی داشته تا امکان دید D ۳ بوجود بیاید.
- مایکروسافت سخت در حال کار می باشد تا میزان اشتباهاتی را که سیستم ها با آن درگیر هستند به حداقل مقدار برساند.
- پسوردها یا PIN ها ممکن است هنوز استفاده شوند اما تفاوت در این مسئله توسط MDM پوشش داده می شود. به خصوص در حالتBYOD

Microsoft Passport سیستم دیگری است که در ویندوز ۱۰ وجود دارد که برای دیسکتاپ و موبایل به جای پسوردهای قدیمی سیستم به کار می رود. به جای یک پسورد کلیدی تولید می شود، یک کلید عمومی و یک کلید خصوصی که با یکدیگر pair می شوند. بعد از اینکه کاربر ساخته شد با IDP خودش تراست می شود.

کلید خصوصی با دستگاه Pair شده و هرگز از آن جدا نمی شود. کاربران تامین کننده خود را انتخاب کرده و این انتخاب می تواند هرکسی از اتحادیه FIDO باشد. که شامل Microsoft، Google، Facebook و ...

تفاوت بین کاربران تجاری و کاربران نهایی Passport اکانتی هست که برای آنها ساخته می شود. باید مشخص شود که آیا صاحب حساب اکانت را برای تجارت و کسب کار میخواهد یا استفاده شخصی میخواهد . وقتی یک کاربر تراست می شود IDP نیازمند به لایه ی دومی از احراز هویت میباشد مثل تماس تلفنی یا Text.

یکبار که تراست صورت می گیرد کلید تولید میشود و بعد Validate شده سپس یک توکن Authentication ارسال می شود توکن روی یک سری از منابع third-party که با این توکن ها تراست هستند مورد استفاده قرار میگیرد.

یک Access Token ساخته شده و کنترل را بوسیله MDM انجام می دهد. شما می توانید بر روی کاربری که دسترسی دارد بازه زمانی جهت محدودیت تنظیم نمایید. اگر این زمان تمام شود کاربر مجددا باید Authenticate شود تا بتواند دسترسی های قبلی را به دست آورد.

انتظارات سازمانی برای دسترسی ها " هر زمان، هرجایی، دسترسی امن و مطمئن" در شکل زیر نشان داده شده است.

در ویندوز ۱۰ ما شاهد این نکته هستیم که مایکروسافت قابلیت های VPN را توسعه داده است.

- IT این امکان را در اختیار دارد تا کسانی که بوسیله ی VPN متصل شده اند فقط دسترسی به سایت های خاص و تعریف شده را داشته باشند. این کاملا با Enterprise Data Protection ادغام شده است.
- قابلیت Always-On به این معنی می باشد که بوسیله ی VPN همیشه دسترسی امکان پذیر می باشد. این در اختیار IT است که تصمیم گیری کند که یک کاربر اجازه دسترسی را دارد یا باید غیرفعال شود.

BitLocker بر روی تمامی دستگاه ها وجود داشته و در جهت محافظت از دیتاهایی که بر روی دستگاه های موبایل قرار دارد طراحی شده است. وقتی دستگاه گم و یا دزده می شود این امکان بسیار کاربردی است. تمام دیتاهای مربوط به سازمانی که شما در آن کار می کنید رمزنگاری می شود. محافظت از دیتاها بوسیله ی جلوگیری از حملات Cold boot انجام می شود. به این منظور Secure Boot UEFI باید فعال باشد، که به صورت استاندارد بر روی ویندوز ۱۰ موبایل موجود دارد.

Enterprise Data Protection بر روی دستگاه های موبایل شبیه به دیسکتاپ ها می باشد و توکن مربوط به احراز هویت صادر می شود.

IT می تواند پالسی های کلیدی جهت حافظت از دستگاه های شخصی را تنظیم نماید. این پالسی های شامل کلیدها، تنظیم اپلیکیشن ها و محافظت از کاربران شبکه و امکانات ذخیره سازی سازمان و کنترل برنامه هایی که ممکن است به سیستم آسیب برسانند می شود.

برنامه هایی هم وجود دارند که وضعیت آنها کامل روشن و واضح می باشد مثل مایکروسافت آفیس. برای مثال، اگر شما یک فایل ورد و یا یک template اکسل را باز کنید، پیغامی ظاهر می شود که از شما می خواهد مشخص نمایید استفاده از برنامه شخصی است یا برای شرکت قصد استفاده دارید.

مستنداتی که جنبه شخصی دارند رمزنگاری نمی شود در حالی که این اتفاق برای مستندات سازمانی / شرکت می افتد و تمام آنها رمزنگاری می شوند.

IT برای اکشن هایی مانند copy/paste دسترسی میگذارد. برای مثال شما یک قسمتی از دیتای سازمان را که از یک سند و یا وب سایت است می خواهید برای خودتان کپی / paste نمایید. IT دسترسی های زیر را صادر میکند:

- Block altogether
- Allow
- Or Allow the user to decide

اگر کاربری Paste کردن دیتا را انتخاب نمایید به اوهشدار داده می شود که این اطلاعات مربوط به سازمان است و سپس اکشن کاربر audit می شود.

در انتها این نکته قابل ذکر است که IT می تواند دسترسی افرادی را که از سازمان خارج می شوند یا به مناطق دیگر اعزام می شوند پاک نماید. این بدین معنا است که دیگر دسترسی جهت اتصال و استفاده از برنامه ها وجود ندارد.

MDM – Mobile Device Management and Business Store

امروزه مشاغل نیازهای در حال تغییر سریعی دارند و به همین دلیل مایکروسافت پیشنهاد مدیریت پیشرفته را در ویندوز ۱۰ می دهد زیرا با نیازهای آنها سازگاری دارد. کارمندانی که تمام طول هفته پشت میز خود نشسته اند و در حال کار می باشند.

کامپیوترهای آنها متصل به شبکه می باشد، کامپیوترهایی که توسط سازمان تامین و مدیریت شده است. آنها فقط از یک دستگاه استفاده می کنند که همین دستگاه دارای سیستم عامل توسعه یافته می باشد.

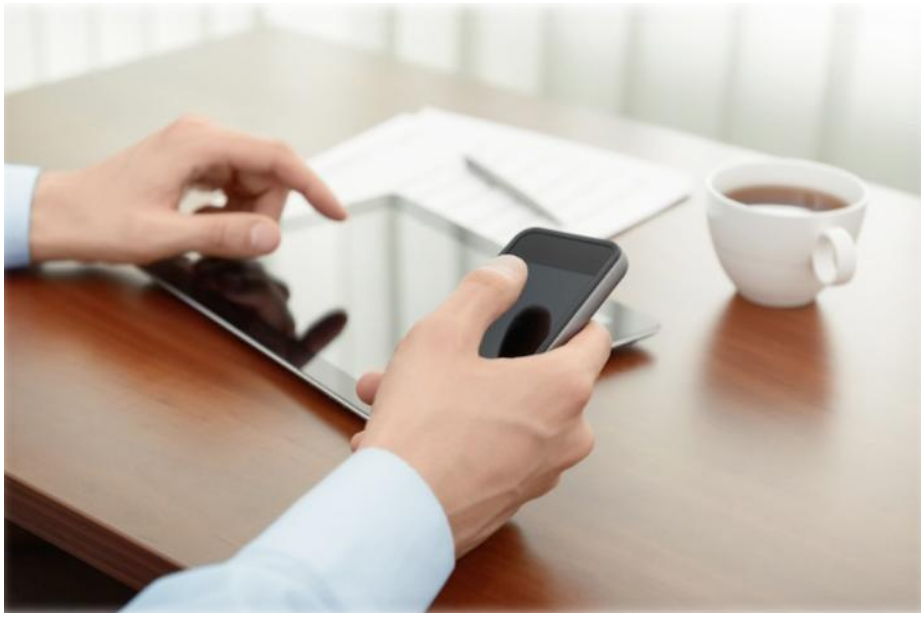
در این سناریو، دستگاه ها باید دارای عمر طولانی باشند به این دلیل دائما آپدیت میگیرند و در حال کار مداوم می باشند. کاربران در جایی که حضور دارند فایل ها و فولدرهایشان را به اشتراک میگذارند و دسترسی آنها به برنامه ها تمام سازمان کنترل می شود.

مدیریت عمیقا در زمینه کنترل سیاست ها و تنظیمات برنامه ها و بدافزارهایی که سیستم را با چالش مواجه می کنند ریز می شود. Network Perimeter همانند یک سیستم دفاعی خوب عمل می نماید.

چه چیزی تغییر کرده است؟ آمدن دستگاه های موبایل همه چیز را تغییر داده است. افراد زیادی هستند که از موبایل برای انجام کار استفاده می نمایند و مدیران ارشد باید تغییرات را در محیط های جدید در نظر بگیرند. البته این بدین معنی می باشد که این دستگاه ها به صور۷*۲٤ هم برای کار و هم برای شخص استفاده می شود.

به جای کار کردن بر روی دیسکتاپی که متصل شده به یک شبکه LAN، ما کارهای خود را بر روی موبایلمان انجام می دهیم که همین موبایل ممکن است به هر شبکه ای متصل شده باشد. نه تنها از برنامه های شخصی بلکه از برنامه های سازمانی هم استفاده می کنیم و تمام این اتفاقات بر روی یک دستگاه رخ میدهد.

ما می توانیم از هر تعداد سیستم استفاده نماییم که شامل اندروید،iOS و کروم و همچنین ویندوز می باشد. دستگاه های ما پایداری لازم را ندارد زیرا از لحاظ سخت افزاری و مشخصات شبیه به دیسکتاپ ها نمی باشند.



به جای استفاده از برنامه های پیش فرض و اپلیکیشن هایی که در همان مکان فقط قابلیت اجرا را دارند ما می توانیم از SaaS استفاده نماییم و یا از قابلیت file-sharing apps استفاده نماییم. به این معنی که کنترل دسترسی سخت تر شده زیرا به جای اینکه به سازمان محدود شود انتشار بر اساس کاربران و دستگاه ها صورت میگیرد.

مدیریت cloud base به این معنی می باشد که کنترل بیشتری وجود داشته و نرم افزارهای مخرب بعنوان یک سلاح مورد استفاده برای جاسوسی دیده می شوند. ما در حال حاضر باید طوری عمل نماییم که دستگاه ها مشکل پیدا کرده اند و اگردر برخی از نقاط نباشند چه اتفاقی خواهد افتاد؟

با سازمان های بیشتر و کارمندانی که به BYOD عادت کرده اند، چالش های امنیتی سخت تر می شوند. گوناگونی دستگاه ها، اپلیکیشن ها و شبکه ها خیلی زیاد شده و از دست رفتن محیط دفاعی آنها احتمال حملات را بشدت بالا برده است.

به این جریان با تامل بیشتری دقت کنید، در پایان سال ۲۰۱۸ بیش از ۵۰درصد کاربران بیشتر فعالیت های جاری خود را از طریق موبایل انجام خواهند داد. و این در حالی اتفاق می افتد که کاملا بی نیاز از دیسکتاپ ها خواهند بود. در پایان سال ۲۰۱٦ بیش از ٤۰درصد از جمعیت جهان صاحب تلفن هوشمند و یا تبلت

خواهند بود. اضافه شدن بیش از ٦,٥ بیلیون کانکشن وایرلس که در حال استفاده می باشد!! اینها ابعاد فاجعه را برای ملموس تر می سازند.

شدت حملات افزایش پیدا کرده و سازمان یافته تر شده است. حملات تداوم بیشتر و اهداف مشخص تری دارند. تنها در چند سال اخیر تعدد حملات بر روی خورده فروشانی مانند Sony و EBay شناخته شده است و این حملات افزایش فزاینده ای داشته است.

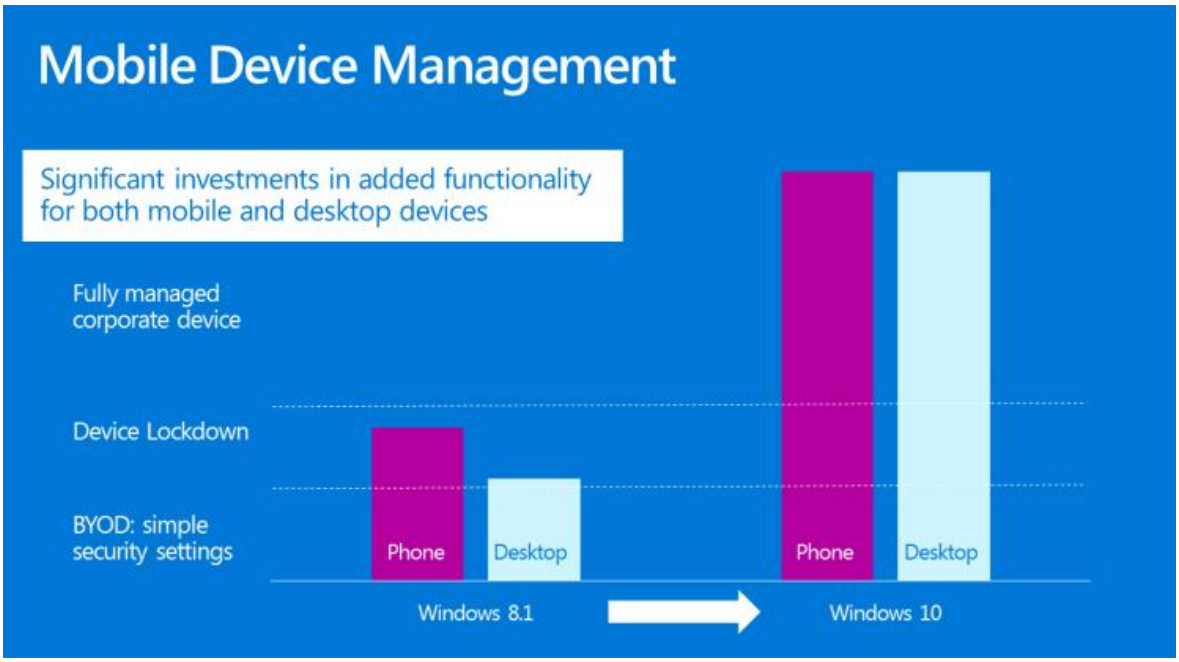
آخرین لایه امنیتی که مایکروسافت شامل آن می شود امنیت برنامه می باشد. تا کنون کنترلی بر روی برنامه هایی که کاربر از هر جایی دانلود و نصب می نماید نبوده است. با ویندوز ۱۰ لایه های ویژه ای برای این مورد اضافه شده است. کاربران می توانند برنامه های شخصی خود را خریداری و دانلود نموده و از LIVE ID خودشان استفاده کنند.

هرچند، در حال حاضر فروشگاه تجاری برای کاربران جهت خرید لایسنس برنامه ها وجود دارد. در داخل پرتال شرکت ، یک فروشگاه جدا وجود دارد و مجوز دسترسی هایی به افرادی که نیاز به برنامه ها دارند داده می شود. تولید برنامه بدین صورت باعث می شود توسعه آن راحت تر شده و از لحاظ امنیت شرایط مطلوب تری برای سازمان حاصل شود.

ویندوز ۱۰ انتخاب شگفت انگیزی برای مدیران می باشد. Group Policy، System Center و تمام کامپوننت های مرتبط در داخل MDM وجود دارد. زمان آغاز بهبود های جدی از ویندوز ۸ آغاز گردید و قابلیت ها در ویندوز ۱۰ توسعه یافت.

با ویندوز ۸,۱ و ویندوز فون ۸,۱ دستگاه ها جهت دسترسی به اطلاعات شرکت/سازمان نیازهای امنیتی پیشرفته ای را باید برآورده سازند. ویندوز فون ۸,۱ کمی به سمت فعال سازی قابلیت های امنیتی حرکت کرد. به این معنی که دستگاه می توانست جهت اجرای بعضی از برنامه ها پیکربندی بشود.

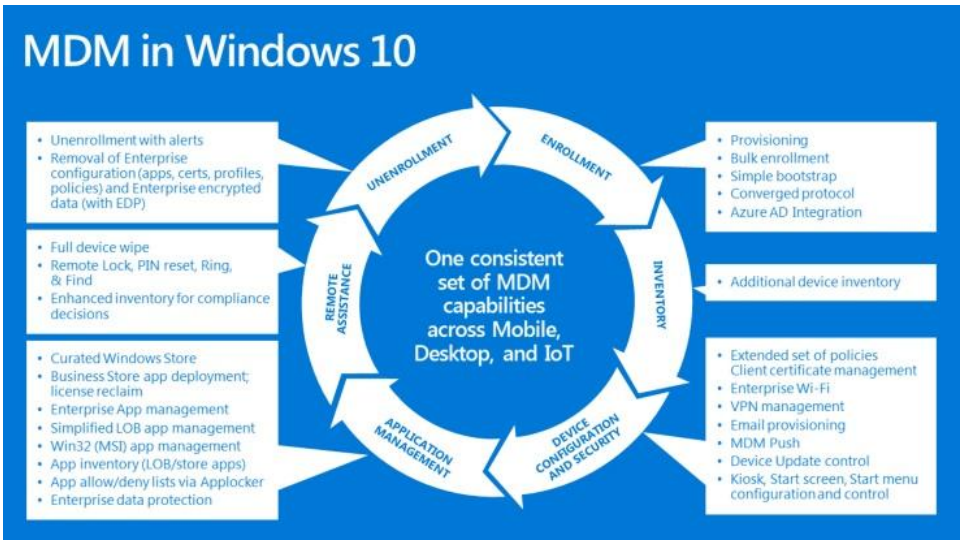
بنابراین، همان گونه که در عکس مشاهده می فرمایید، دستگاه هایی که از پلتفرم ویندوز ۱۰ استفاده میکنند به صورت کامل می توانید توسعه دهید.



در ویندوز ۱۰، مایکروسافت فازهای MDM **را جهت آماده سازی افزایش داده است که شامل:**

- ثبت نام ساده برای دستگاه های خاص جهت خودکار سازی استفاده از MDM همانند یک قسمت ازپروسه AAD
- پیکربندی جدید و مدیریت ابزارهای start menu
- کنترل های جدید بروزرسانی ویندوز، به شما این توانایی را می دهد که تنظیمات را جوری قرار دهید که بروزرسانی های خاصی از MDM به دستگاه اعمال می شوند.
- پیکربندی جدید برای اعمال بر روی Enterprise Data Protection and AppLocker
- ادغام عالی با ویندوز استور و بیزینس استور برای مدیریت خودکار اپلیکیشن ها
- قابلیت های کامل جهت پاک کردن دستگاه ها

تمام این قابلیت ها و شاید هم بیشتر از چیزهایی که نام برده شد به صورت تمام و کمال بر روی تمام دستگاه ها پیشتیبانی می شود، تمام ویندوز فون ها، تبلت ها و دستگاه هایی که متصل به اینترنت هستند همانند شکل زیر:



امروزه Active Directory تقریبا توسط تمام شرکت ها مورد استفاده قرار می گیرد تا امنیت و سرویس های شناسایی و احراز هویت را به صورت کامل و مطمئن انجام دهند. تمام قابلیت های AD توسط ویندوز ۱۰ پشتیبانی می شود. اما بزرگترین تغییری که در ویندوز ۱۰ اضافه شده است پشتیبانی کامل از AAD یا آژور اکتیو دایرکتوری می باشد.

این بدین معنی می باشد که ویندوز ۱۰ طوری طراحی شده که تمام دایرکتوری ها و اکانت ها در AAD از روش های مختلفی می توانند مورد استفاده قرار بگیرند.

اولین چیزی که به ذهن خطور میکند این نکته است که باید بین اکتیو دایرکتوری و آژور اکتیو دایرکتوری یکی را انتخاب نمایید. اگر انتخاب شما AD است شما به صورت خودکار قادر خواهید بود از AAD هم استفاده نمایید.که این قابلیت باعث می شود مزیت های ویژه ای برای شما حاصل شود.

ویندوز ۱۰ میتواند از مدیریت BYOD پشتیبانی نماید ، وقتی ما در مورد احراز هویت صحبت می کنیم دستگاه های سازمان سالم خواهند ماند. یک دستگاهی که برای سازمان بوده می تواند به اکتیو دایرکتوری join شده تا ارتباط آن تراست شود و بعد با اکانت AAD ساخته شده signed شود.

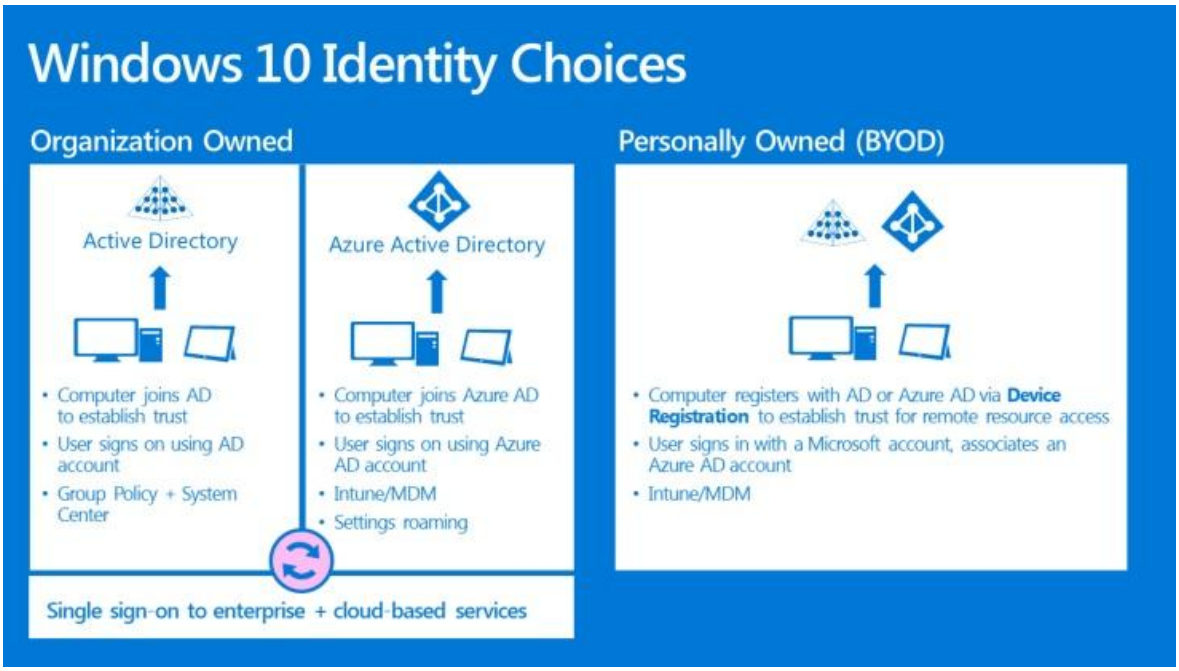
انتخاب شما می تواند ملحق شدن به AAD همانند یک مستجر باشد سپس با اکانت AAD خود لاگین شوید استورج آژور این قابلیت را کاملا پشتیبانی می نماید.

ارزش واقعی زمانی مشخص می شود که دستگاه با هر دو حالت ترکیب شود. بعد از اینکه AD دامین با AAD سینک شد، مزیت های ویژه ای در single sign on ایجاد می شود. ویندوز ۱۰ به صورت خودکار اکانت های ارتباطی بین اکانت ها را به رسمیت می شناسد، بدین معنی که AD یوزرها توانایی دسترسی به

سرویس ابری خود را دارند بدون اینکه نیازی به ورود مجدد داشته باشند. و برعکس این موضوع که کاربران AAD به صورت پیش فرض دسترسی داشته و نیازی به احراز هویت های قدیمی نمی باشد.

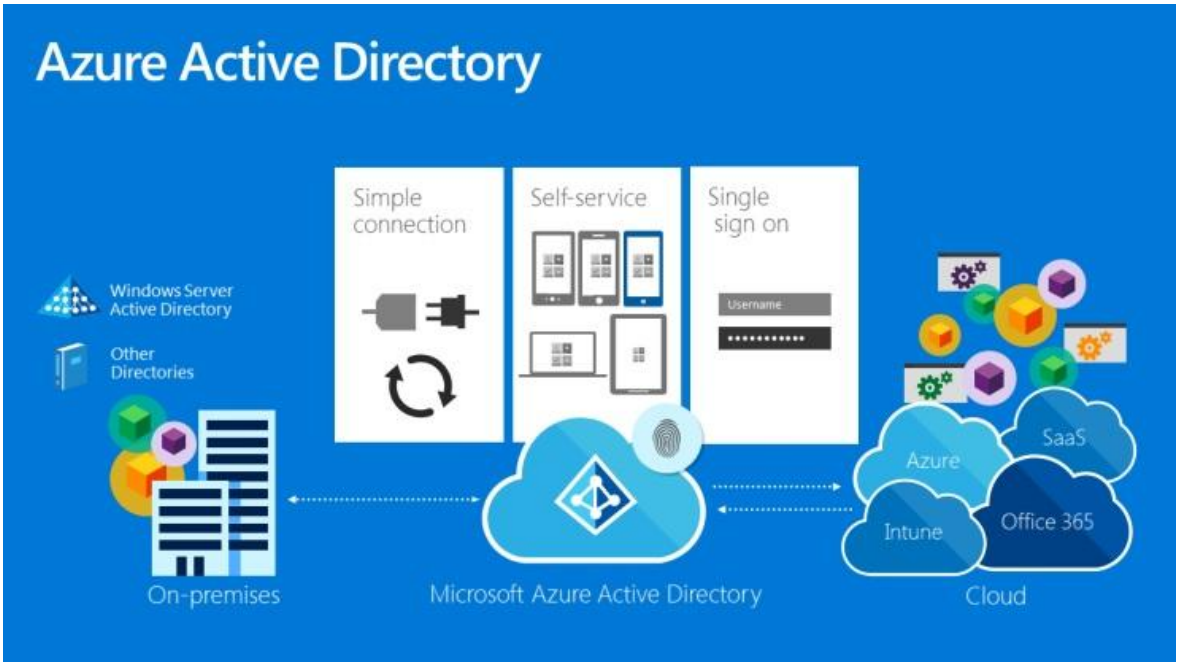
در اینجا فقط در مورد مایکروسافت کلود صحبت نمی شود; صحبت من در مورد داشتن single sign on برای صدها تامین کننده ی SaaS مختلف می باشد. Software as a Service به سادگی ارتباط بین AAD و سرویس هایی که شما نیاز دارید تعریف می شود و برای تمام مجموعه شامل single sign on وجود دارد.

برای BYOD، ویندوز ۱۰ تمام دستگاه های ثبت شده شخصی را پشتیبانی می کند. یکبار که رجیستر می شود، همانند شکل زیر، یک سطح اضافی جهت تراست ایجاد می شود ، به این معنی که اجاز می دهد به تمام سرویس ها و برنامه ها که بر روی دستگاهی که رجیستر نشده است اجرا نشوند.



یک AAD اجاره شده در راستای اهداف سازمان تنظیم میشود . بعد از آن همسان سازی بین AD اتفاق می افتد. این همگاه سازی در فواصل معین زمانی رخ می دهد تا مطمئن شویم AAD به صورت کامل بروزرسانی شده است.

تمام دستگاه ها می توانند به AAD جوین شوند یا آنها فقط اکانتی داشته باشند. در هر صورت، دسترسی single sign in را در سرویس های ابری بدست می آورند. همچنین گرفتن تنظیمات برنامه های roaming و دیتا برای یک رنج وسیعی از دستگاه ها امکان پذیر می شود.



امنیت مرورگر

بر روی ویندوز ۱۰ دستگاه های موبایل، فقط یک مرورگر به نام edge وجود خواهد داشت. جایگزینی مناسب برای Internet Explorer خواهد بود.

البته، با یک مرورگر جدید چالش های امنیتی جدیدی ایجاد خواهد شد همان گونه که قبلا بیان شد با توجه به استفاده بسیار زیاد کاربران از موبایل ها جهت انجام کارهای شخصی و شرکتی مثلا این چالش ها بسیار زیاد خواهد بود. Edge توسط MDM مدیریت می شود.

مایکروسافت پالسی های جدیدی را برای edge معرفی کرده است. پالسی های MDM هم در Group Policy وجود داشته و نام تجاری جدیدی را در ویندوز ۱۰ ایجاد کرده اند.

پالسی های MDM راهی برای مدیریت پلتفرم های مختلف دستگاه ها می باشد که از زبان های توسعه پذیر یا XML برای تبادل دیتاها استفاده می نماید. XML قوانینی برای رمزنگاری دیتا تعریف می نماید این در شرایطی انجام می شود که هم برای کاربر و هم برای دیوایس قابل خواندن است.

MDM به صورت کامل توسط سازندگان اصلی موبایل حمایت شده و تمام چرخه دستگاه را تحت پوشش قرار می دهد که شامل:

- ثبت دستگاه
- پیکربندی

- مدیریت برنامه
- راهنمایی از راه دور و موجودی
- کنار گذاشتن دستگاه

مایکروسافت edge سناریوهای روبه جلویی هستند، این بدین معنا است که آنها به طور کلی وابسته به استفاده ی دسترسی های فردی و دستگاه می باشند.

آنها شامل تمام دستگاه ها می شوند، بدون درنظر گرفتن اینکه آنها چه هستند و شامل موارد زیر می شوند:

- Enterprise site list configuration
- Sending the Intranet to IE
- Allowing the browser on a mobile
- Default browser
- Allowing pop-ups
- Configuring cookies
- Allowing SmartScreen
- Allowing Active Scripting
- Configuring the home page
- Allowing Do Not Track
- Allowing Autofill
- Configuring Password Manager
- Disable search suggestions in the address bar

کلیه این طراحی ها به شرکت ها کمک می نمایند تا دیتاهای خود را به صورت مطمئن نگهداری کرده و با مانیتور کردن مواردی چون : چه کاربرانی نمی توانند دسترسی داشته باشند ؟ و چه کاربرانی دسترسی بیش از اندازه گرفته اند بر مشکلات خود فائق آیند.

این موارد باعث کاهش ریسک malware ها یا هر تهدید ناخوشایندی می شود و از دسترسی های غیرمجاز و به خطر افتادن دستگاه های موبایل جلوگیری میکند.

Enterprise Mobility Suite

EMS پاسخ دادن مایکروسافت به کنترل دسترسی امنیتی می باشد. در حال حاضر بیشتر شرکت ها و سازمان ها دیتاهای خود را در مکانی که حضور دارند ذخیره می نمایند. مانند اطلاعاتی همچون Active Directory و از طریق اینترنت و بوسیله ی مرورگرهای تحت موبایل و پی سی به این اطلاعات دسترسی پیدا میکنند.

به صورت خلاصه، اینجاست که کنترل امری مهمی می شود چه کسی از کجا و چه وقتی دسترسی دارد؟ ضعیف ترین نقطه در سیستم DMZ می باشد زیرا راه های متعددی برای دسترسی وجود دارد و حفظ نمودن کنترل این منطقه بسیار دست و پا گیر و مشکل می باشد.

راهکار مایکروسافت برای ساخت دسترسی های کنترلی به تمام اپلیکیشن ها، در جایی که نصب شده اند و یا سرویس های ابری، بعنوان یک راهی که شامل تمام داده ها می شود و از نشست اطلاعات جلوگیری میکند.

در لایه بیس از EMS، بر روی دستگاه موبایل Mobile Device Management – MDM وجود دارد. این تقریبا استانداردی بر روی اکثر دستگاه های شرکتی بوده و اجازه دسترسی به سرویس های مختلف را فراهم میکند.

در لایه ترکیبی بعدی، آفیس ۳٦۵ محصولات موبایلی وجود دارد و این شامل همه برنامه های آفیس می باشد مانند Word، Excel، OneDrive.

روند توسعه به برنامه های تجاری اجازه می دهد که قابلیت یکپارچه شدن با برنامه های آفیس در موبایل ها ایجاد شود.

اولین و مهم ترین قسمت از EMS شرایط دسترسی کنترلی می باشد، Azure AD از بخش های زیر تشکیل شده است:

- User attributes: کاربر باید هویت سنجی شود که چه کسی است و عضو چه گروهی می باشد و به چه برنامه هایی دسترسی دارد. همچنین باید مشخص شود که به MultiFactor برای احراز هویت نیاز دارد.
- Device authentication: در ویندوز ۱۰ رابطه کاربر با دستگاه تشکیل دهنده ی ایده امنیتی می باشد. نه تنها کاربر باید ثابت کند که صاحب اصلی دستگاه می باشد بلکه سازگاری دستگاه با این نوع احراز هویت هم بسیار حائز اهمیت است.
- Application: این بخش بر اساس حساسیت های شرکت تنظیم می شود و کاربران تنها به برنامه های مورد نیازشان دسترسی دارند. با توجه به تنظیماتی که IT اعمال میکند دسترسی های مشخص میگردد.

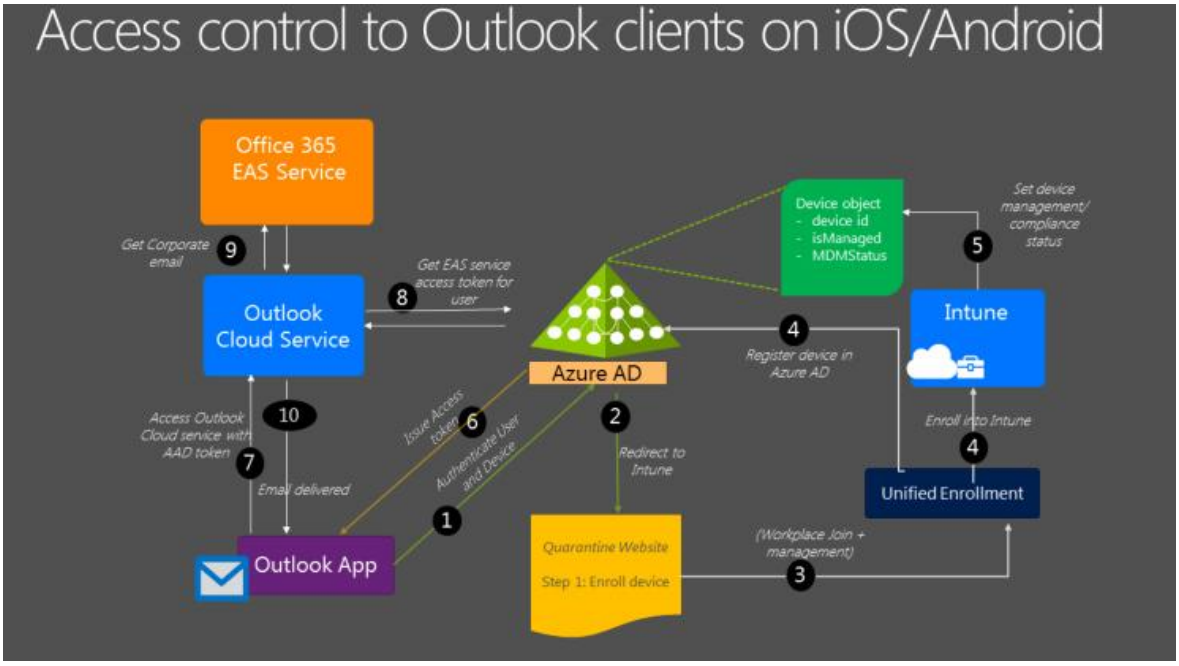
- Network: EMS مشخص می نماید که چه کاربرانی به شبکه دسترسی دارند و داخل یا بیرون بودن کاربران از شبکه مشخص می شود.

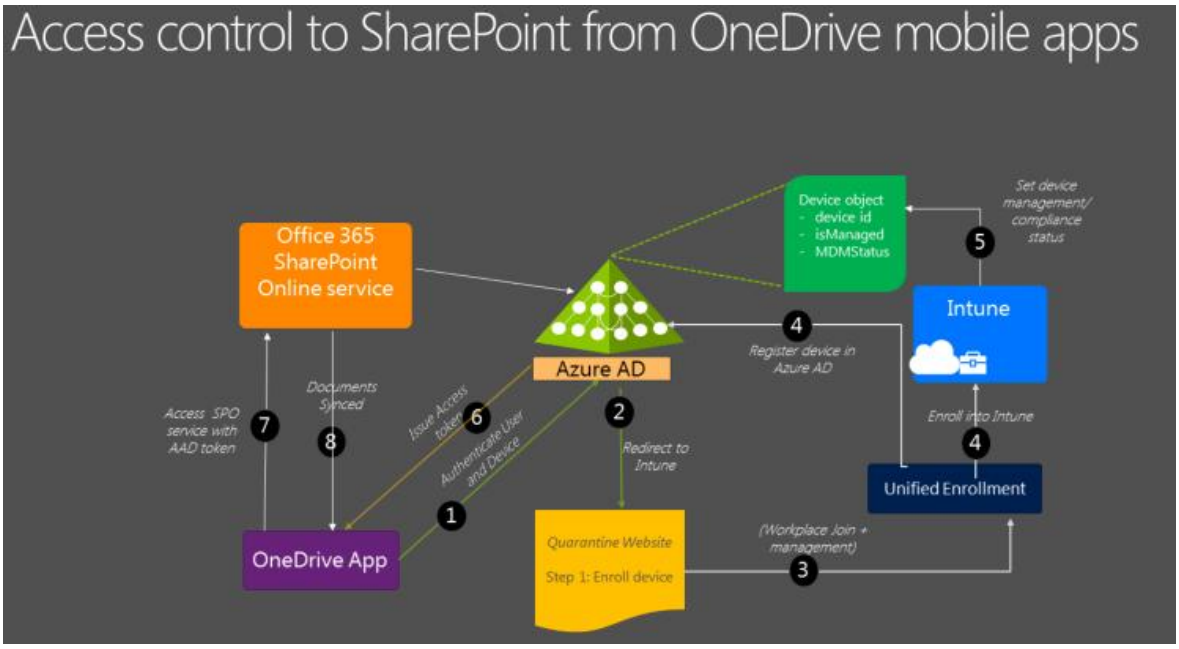
Office 365

بر اساس شرایط کنترلی مشخص شده، کاربران جهت استفاده از ابزارهای آفیس با محدودیت مواجه هستند مگر اینکه در MDM تعریف شده و یا با پالسی های سازمانی سازگاری داشته باشند.

بعد از احراز هویت کاربر دسترسی مربوطه ایجاد می شود. تمام دیتاهای مربوط به برنامه های سازمانی رمزگذاری می شود و بحث اشتراک گذاری محدود دیتاهای سازمانی اعمال می گردد. کارمندانی که سازمان را ترک میکنند دسترسی های آنها گرفته می شود و تمام اطلاعات wipe می شود.

دو شکل زیر نشان دهنده ی دسترسی کنترل مشابه برای استفاده از اوتلوک بر روی iOS و اندروید از OneDrive موبایل می باشد.





دسترسی مشروط برنامه های متصل شده به Azure AD

Azure AD با بیش از ۲ هزار برنامه از قبل پیکربندی شده که می توان بر اساس MFA به آنها دسترسی داشت. مثلا می توانیم مشخص کنیم امکان دسترسی به برنامه از طریق Extranet وجود نداشته باشد. این برنامه ها بر اساس SaaS کار میکنند و IT مشخص میکند که یک گروه خاص یا اشخاص به برنامه های مشخصی دسترسی داشته و یا فقط یک گروه خاص یا شخصی جهت دسترسی به برنامه بلاک شوند. این توضیحات به این معنی می باشد که کاربران فقط چیزهایی را میبینند که به آنها نیاز دارند و همین باعث می شود از سردرگمی آنها کاسته شود.

دسترسی مشروط به دستگاه

دسترسی محدود شده فقط به دستگاه هایی که با سیستم سازگار بوده و توسط کارشناسان مدیریت می شود. در Auto-workplace کامپیوترها به صورت خودکار join شده و در مرحله بعدی پالسی ها به سیستم ها اعمال می شود. هر دستگاهی که ویژگی های تغییرات را داشته باشد دسترسی خود را لغو نموده و ممکن است کاربر درخواست تنظیم اعتبار جدید را صادر نماید.

پشتیبانی برای یک تعدادی ازتامین کنندگان عمده SSL VPN مانند juniper, Cisco, Checkpoint, SonicWALL, SFS ساخته شده است. استانداردهای VPN مانند PPTP، L2TP و IKWv2 پشتیبانی می شود.

Windows as a Service – More Security via secure updates

همه آگاهی داریم که تغییرات زیادی در پیرامون ما در حال انجام است و با هر تغییری که اتفاق می افتد مشکلات و چالش های جدیدی ایجاد می شود.

کاربران نهایی و فروشندگان نگرانی های زیادی را در مورد ویندوز ۱۰ ابزار نموده اند و بعضی از مسایل مشترک مطرح شده عبارت اند از :

- نگرانی از ارتقا به ویندوز ۱۰ و Crash کردن برنامه ها
- فروشندگان قفل های نرم افزاری نگران هستند که زمان لازم برای آزمایش کلیدهای خود نداشته باشند و همین امر سبب شود نتوانند پشتیبانی لازم را به مشتریان خود ارائه دهند.
- مردم حس میکنند زمان بیشتری برای برنامه ریزی جهت آپدیت به ویندوز ۱۰ نیاز دارند.
- وابستگی بیش از اندازه بین نسخه های مختلف و محصولات مایکروسافت وجود دارد.
- استقرار و توسعه بیش از حد وقت گیر بوده و بسیار گران است.
- نگرانی از تهدیدات امنیتی
- مردمی که اعتقاد دارند برای پیاده سازی این سیستم جدید نیاز به کمک و راهنمایی متخصصین دارند.

بنابراین در موارد بیان شده بالا، مایکروسافت کاملا توجه کرده و مواردی را که کاربران نهایی و کاربران تجاری نیاز دارند احساس کرده است:

چابکی:

- دسترسی به تکنولوژی جدید
- مایکروسافت نیاز به پیاده سازی بازخوردهای سریع دارد
- شفافیت
- انعطاف پذیری برای ادغام محیط های مختلف

کنترل

- ثبات بیشتر
- ارتقا کمتر
- چرخه عمر طولانی جهت پشتیبانی
- زمان بیشتر برای تست و اخذ گواهینامه

- قابلیت پیش بینی
- اظهارات ISV برای پشتیبانی

Windows as a Service یک تجربه بی نظیری را برای مصرف کنندگان فراهم میکند. برای استفاده کنندگان بروزرسانی ها بسیار وسیع شده اند. بروزرسانی بر اساس اهداف مشخص صورت می گیرد. دستگاه های BYOD به صورت کامل آپدیت و امن باقی می مانند و در هر لحظه میلیون ها دستگاه بروزرسانی می شوند.

روی دیگر سکه قسمتی است که ما سیستم های خاصی داریم. مانند سیستم های کنترل هوایی، سیستم های پزشکی و سیستم های بانکی. همه ی این سامانه ها حیاتی بوده و به احتمال زیاد دائما نیازی به آپدیت ندارند اما بروزرسانی های معمول امنیتی را انجام می دهند.

این وسط کاربری تجاری وجود دارد. کاربر تجاری یک مصرف کننده نمی باشد و در تمام مدت و در لحظات حساس نیازی به بسیاری از آپدیت ها ندارد .

حال سوال اینجاست که با کاربران تجاری چگونه برخورد کنیم ؟ بروزرسانی های سیستم برای این کاربران قطعا مفید خواهد بود و سبب بهبود روند کاری آنها می شود. بعد از اینکه نوع فعالیت این کاربران مشخص شد به توصیه مایکروسافت می توانیم آپدیت ها را برای آنها اعمال نماییم.

این بروزرسانی آنها ابتدا باید مورد آزمون قرار بگیرند سپس در مدت زمان مشخص بر روی سیستم ها توسعه پیدا کنند.

بروزرسانی ویندوز برای Business

آپدیت ویندوز برای بخش تجاری یک قابلیت جدید ارائه شده توسط مایکروسافت می باشد که در جهت کمک به متخصصان IT در سراسر دنیا عرضه شده است. این قابلیت طراحی شده تا موارد زیر را پوشش دهد:

Roll out Rings: متخصصان IT می توانند مشخص نمایند که چه دستگاهی و در چه زمانی بروزرسانی شده است. بنابراین قبل از اینکه اتفاق ناخوشایندی رخ دهد تمام گیر و گورهای سیستم مشخص می گردد.

Maintenance Windows: متخصصان IT زمان هایی که بروزرسانی باید یا نباید انجام شود را مشخص کرده و زمان های بحرانی برای سیستم ها را تعیین می نمایند.

Peer-to-Peer Devilry: it آپدیت ها را برای شعبه های مختلف با پهنای باند محدود شده ارسال می نماید.

Integration with Existing: ابزارهای یکپارچه سازی که کاملا با مدیریت سیستم هماهنگ و یکپارچه می باشند.

بروزرسانی ویندوز برای بخش تجاری در جهت کاهش مدیریت هزینه ها طراحی شده است و کنترل بیشتری بر روی توسعه آپدیت ها دارد.

در گذشته دو برنامه جهت بروزرسانی وجود داشت – ویندوز آپدیت ، همان چیزی که در حال حاضر ما از آن استفاده میکنیم و هدف آن دستگاه های BYOD می باشند، دستگاه های مصرفی و ماشین های تستی و سرویس بروزرسانی ویندوزWSUS ، که در آن سیستم های خاص آپدیت های امنیتی را دریافت می نمایند.

حالا ما بروزرسانی ویندوز برای کسب و کار را داریم (WUB). WUB به مدیران قابلیت اضافه کردن دستگاه جهت دریافت بروزرسانی دلخواه را می دهد. به جای اینکه درگیر راه های دیگر بشوند.

شما تصمیم گیری میکنید که دستگاه چه زمانی آپدیت ها را دریافت نماید و آپدیت های امنیتی حیاتی به صورت منظم برای شما ارسال می شود.

ویندوز و اینترنت اشیاء

اینترنت اشیا چیست ؟ اینترنت اشیا آینده ی اینترنت می باشد، قابلیتی برای اتصال اشیا و دستگاه ها.

یک فرصت بزرگ در حالی که بسیار ناشناخته باقی مانده است. ایده های بزرگ و چیزهایی که به ذهن می رسد:

- در سال ۲۰۲۰، تخمین زده می شود چیزی در حدود ۲۸ بیلیون شی با هم متصل باشند. به ازا هر شخص روی کره ی خاکی چهار دستگاه.
- در سال ۲۰۱۷، فرصت ها و موقعیت ها در اختیار ابزارهای پوشیدنی می باشد که ارزشی در حدود بیست بیلوین دلار دارند.
- در سال ۲۰۱۷، فرصتی برای خانه های هوشمند ایجاد می شود که ارزشی در حدود ۱۲ بیلیون دلار دارند.

اما، با وجود تمام فرصت هایی که بوجود خواهد آمد چالش های بزرگی هم ایجاد خواهد شد مثل :

- سخت افزارهای اختصاصی و پروتکل های پیچیده ای که ایجاد خواهد شد.
- اداره، پیکربندی و شناسایی
- امنیت

چالش ها باید به دو حوزه اصلی تقسیم شوند – مصرف کننده و شرکتی. در قسمت مصرف کننده، گرایش عمده ما به سمت دستگاه های خانگی است برای خودکارسازی، امنیت، تفریح و مدیریت انرژی.

در قسمت شرکتی تعاریف کمی کمتر بوده و ناشناختگی بیشتر می باشد. در این قسمت پیچیدگی اینترنت اشیا بیشتر است– هزاران اتصال در خارج وجود دارد اما هیچ قابلیت همکاری داخلی دیده نمی شود.

ارزش واقعی اینترنت اشیا آن قسمتی می باشد که تمام دستگاه ها باید بتوانند در تمام مارکت ها و در تمام گروه ها به یکدیگر متصل شوند.

AllSeen and AllJoyn

AllJoyn: یک اسم برای تکنولوژی اوپن سورس می باشد، یک شبکه ارتباطی که به دستگاه ها اجازه ی صحبت با یکدیگر را داده و بالاترین حالت جهت همکاری را ایجاد می نماید.

AllSeen: اتحادی که برای نظارت بر روی AllJoyn ایجاد شده و قابلیت فعال سازی اینترنت اشیا را برای کار بوجود می آورد همچنین قسمتی از پروژه ی اوپن سورس لینوکس می باشد.

AllJoyn طراحی شده تا به دستگاه ها اجازه:

- شناسایی دستگاه های دوستانشان که در نزدیک آنها
- شناسایی سرویس هایی که در سایر دستگاه ها اجرا شده اند.
- انطباق با دستگاه هایی که در حال گردش می باشند. مانند اینکه اگر دو دستگاه یکبار با یکدیگر pair شده باشند و سپس قطع شوند، اگر دوباره Pair شوند، آنها Pair قبلی را داشته و به راحتی دوباره با یکدیگر Pair می شوند.
- مدیریت جابجایی دو طرفه
- همکاری بین تمامی سیستم عامل ها
- تبادل اطلاعات، یک دستگاه را قادر می سازد تا نسبت به دیگری قوی تر شود بوسیله دانستن اینکه چه سرویس هایی بر روی دستگاه اجرا شده است.