باسمه تعالی

عنوان مستند

مکانیزم Device Guard ویندوز ۱۰

فهرست مطالب

۱ مقدمه

با هزاران فایل جدید مخربی که هر روزه تولید می شوند، استفاده از راه های قدیمی مانند استفاده از آنتی ویروس ها راه دفاعی کافی در برابر حملات جدید محسوب نخواهد شد. Device Guard در ویندوز ۱۰ نسخه سازمانی[۱]، رویه سیستم عامل را از حالتی که در آن برنامه ها قابل اعتماد هستند (مگر اینکه توسط یک آنتی ویروس یا برنامه ی امنیتی دیگر جلوی کار آنها گرفته شود)، به حالتی که در آن سیستم عامل فقط به برنامه هایی اعتماد می کند که توسط خود شرکت مجاز شده باشند تغییر داده است. این برنامه ها با ایجاد سیاست های درستی کد، به عنوان برنامه های قابل اعتماد مشخص می شوند.

مکانیزم صحت کد دو قسمت دارد: حالت درستی کد در مد هسته و حالت درستی کد در مد کاربر. حالت هسته ی درستی کد در نسخه های قبلی ویندوز وجود داشته و هسته ی سیستم عامل را در برابر اجرا شدن درایور های شناخته نشده محافظت می کرد. در ویندوز ۱۰ و ویندوز سرور ۲۰۱۶ علاوه بر حالت هسته، حالت کاربر درستی کد هم برای محافظت در برابر ویروس ها و بد افزار ها اضافه شده است.

برای بیشتر کردن میزان امنیتی که سیاست های درستی کد ایجاد می کند، Device guard می تواند از قابلیت های پیشرفته ی سخت افزار ها برای محافظت بیشتر آنها استفاده کند. این قابلیت ها شامل شبیه سازی CPU (Intel VT و AMD-V) و ترجمه سطح دوم آدرس (SLAT) می شود. علاوه بر این سخت افزار هایی که دارای واحد های مدیریت ورودی و خروجی حافظه هستند، محافظت بیشتری را شامل می شوند. وقتی که قابلیت های پیشرفته سخت افزار را فعال سازی می کنید، سرویس درستی کد می تواند در کنار هسته ی ویندوز در یک حالت محافظتی اجرا شود.

[۱] Windows 10 Enterprise

۲ قابلیت های محافظتی Device Guard

جدولی زیر اطلاعات بیشتری راجع به نحوه ی کمک Device Guard و قابلیت های پیشرفته ای که به منظور محافظت بیشتر در اختیار کاربران قرار می دهد را ارائه می دهد.

تهدید امنیتی	چگونه Device Guard به محافظت در برابر تهدید کمک میکند
برخورد با بدافزار جدید	سیاست درستی کد: می توان به جای به روز رسانی کردن جدول امضای بدافزار ها، یک لیست سفید از نرم افزار های قابل اعتماد تهیه کرد. این روش از مدل "به هیچ چیز اعتماد نکن" در سیستم عامل موبایل ها استفاده می کند. تنها کدی که امضای آن به عنوان امضای قابل اعتماد در درستی کد ذخیره شده است قابلیت اجرا پیدا می کند. این امر باعث ایجاد کنترل کامل، روی کد های اجازه داده شده هم در حالت کاربر و هم در حالت هسته می شود. قابلیت پیشرفته سخت افزار: این روش نیاز به داشتن قابلیت های پیشرفته در سخت افزار نمی باشد.
برخورد با کد ثبت نشده	سیاست درستی کد: از آنجایی اکثر بدافزار ها دارای کد امضا نشده هستند، استفاده از یک سیاست درستی کد میتواند باعث محافظت در برابر تعداد زیادی از تهدید ها شود. با این حال، بسیاری از سازمان ها از برنامه های LOB[۲] امضا نشده استفاده می کنند که عملیات امضا کردن را سخت می کند. در ویندوز ۱۰ این موضوع تغییرکرده است. به این صورت که می توانید از ابزاری تحت عنوان package inspector برای درست کردن کاتالوگی از تمام باینری فایل های اجرا و بارگزاری شده استفاده کنید. بعد از ثبت کاتالوگ درستی کد با این

[۲] Line-of-Business

	بسته دقیقا مانند سایر برنامه هایی که امضای آنها ثبت شده برخورد می کند. با این روش می توان برنامه ی نامشخص را راحت تر بلاک کرد. قابلیت پیشرفته سخت افزار: این روش نیاز به داشتن قابلیت های پیشرفته در سخت افزار نمی باشد.
بد افزار هایی که دسترسی به هسته ی سیستم عامل دارند	امنیت مجازی: این لایه امنیتی از hypervisor برای محافظت از هسته و سایر قسمت های سیستم عامل استفاده می کند. وقتی این حالت فعال است حالت هسته ی درستی کد یا آن نسخه از درستی کد که آن را پیاده سازی کرده اید را قوی تر می کند. با استفاده از VBS[۳] حتی اگر بدافزار به هستهی سیستم عامل دسترسی پیدا کند آثار مخرب کمی از خود به جای خواهد گذاشت به این دلیل که VBS به ویروس اجازه ی اجرا کدهایش را نمی دهد. Hypervisor محدود ترین بخش نرم افزار سیستم محدودیت های R/W/X را روی تمام حافظه پیاده می کند. بررسی های درستی کد در محیطی امن که در برابر حملات در حالت هسته مصون است انجام می شوند و همچنین دسترسی های صفحات حالت هسته توسط hypervisor تعیین و تنظیم می شوند. حتی اگر این موارد در برابر حملاتی که باعث تغییر در حافظه آسیب پذیر باشند (برای مثال سرریز حافظه) حافظه ی تغییر داده شده نمی تواند اجرا شود. قابلیت پیشرفته سخت افزار: VBS نیاز به افزونه های مجازی سازی CPU و SLAT دارد.
حملات DMA[۴]	امنیت مجازی با استفاده از IOMMU ها: در این نوع امنیت از VBS وقتی حملات DMA درخواست حافظه می دهند واحد های مدیریت

[۳] Virtualization-based security

[۴] Direct memory access

	ورودی و خروجی حافظه (IMMOU) درخواست را بررسی کرده و آن را رد می کنند. قابلیت پیشرفته سخت افزار: IMMOU ها یک قابلیت پیشرفته‌ی سخت افزاری هستند که از hypervisor پشتیبانی می کنند و زمانی که سخت افزاری که دارای آن ها است را انتخاب کنید می‌توانند در برابر حملاتی که نیاز به دسترسی به حافظه دارند محافظت کنند.
قرار گرفتن در معرض بوت کیت یا حمله کننده ی فیزیکی حاضر در هنگام بوت شدن	بوت امن UEFI: بوت امن و متد های مرتبط با آن عملیات بوت شدن و سفت افزار را در برابر دستکاری محافظت می کند. این دستکاری می تواند از سوی یک حمله کننده ی فیزیکی حاضر یا از طرف بدافزاری که در مراحل اولیه بوت شدن کار خود را آغاز می کند یا در هسته بعد از آغاز کار سیستم رخ دهد. در این نوع ایمن سازی UEFI قفل می شود و تنظیمات آن قابل تعویض نیستند. قابلیت پیشرفته سخت افزار: نیاز های این روش ایمن سازی، همان نیاز های سفت افزار هستند.

۳ ابزار های مورد استفاده برای مدیریت Device Guard

کاربران می توانند قابلیت های Device Guard را با استفاده از ابزار های آشنایی که متخصصان IT هرروزه استفاده می کنند به راحتی مدیریت کنند:

۳-۱ Group Policy

ویندوز ۱۰ یک قالب مدیریتی برای دستکاری و پیاده سازی درستی کد برای سازمان ها آماده کرده است. این قالب همچنان مشخص می کند کاربر کدام یک از قابلیت های سخت افزاری را برای محافظت پیاده سازی کرده است. می توان این قابلیت ها را در کنار GPO[۵] مدیریت کرد که باعث راحت تر شدن پیاده سازی آن می شود. علاوه بر این ها کاربران می توانند از Group Policy برای مدیریت فایل های کاتالوگ استفاده کنند.

۳-۲ Microsoft System Center Configuration Manager

از Microsoft System Center Configuration Manager برای راحت تر کردن پیاده سازی و مدیریت فایل های کاتالوگ، سیاست های درستی کد و قابلیت های امنیتی وابسته به سخت افزار و همچنین کنترل ورژن استفاده می شود.

۳-۳ Microsoft Intune

در نسخه های بعدی Microsoft Intune، ماکروسافت در نظر دارد قابلیت هایی که از پیاده سازی و مدیریت درستی کد پشتیبانی می کند را به آن اضافه کند.

۳-۴ Windows PowerShell

برای درست کردن و تغییر در سیاست های درستی کد از Windows PowerShell استفاده می شود.

[۵] Group Policy Object

۴ سایر قابلیت های مرتبط با Device Guard

۴-۱ Device Guard همراه با AppLocker

با اینکه Applocker به عنوان یکی از قابلیت های جدید Device Guard به حساب نمی آید ولی می تواند امنیت سیستم را در مواقعی که درستی کد به طور کامل پیاده سازی نشده یا تمام سناریو های موجود را پشتیبانی نمی کند بالاتر ببرد. سناریو های فراوانی هستند که در آنها محدودیت های درستی کد در کنار قوانین AppLockr به کار می روند. در اکثر مواقع باید محدودیت های درستی کد را به بالاترین میزان ممکن برای سازمان برد و با استفاده از قوانین AppLocker، سطح دسترسی ها را پایین تر آورد.

AppLocker و Device Guard باید در کنار هم اجرا شوند که باعث ایجاد بهترین قابلیت و حد امنیت در دستگاه های مختلف شوند. علاوه بر این موارد پیشنهاد داشتن یک آنتی ویروس برای مقابله با ویروس های سنتی نیز داده می شود.

۴-۲ Device Guard همراه با Credential Guard

یکی دیگر از قابلیت های ویندوز ۱۰ که از VBS استفاده می کند Credential Guard است. Credential Guard محافظت بیشتری برای فعال سازی کاربران دامنه ی دایرکتوری با ذخیره سازی مجوز های دامنه با یک نوع از VBS که میزبان درستی کد هستند، ایجاد می کند. با جدا کردن این مجوز دامنه ها از حالت هسته و حالت کاربر، آنها احتمال کمتری دارد که در معرض سرقت قرار بگیرند.

۵ ابزار ها و راهنمایی های برنامه پیاده سازی Device Guard

۵-۱ سخت افزار، سفت افزار و نرم افزار مورد نیاز برای Device Guard

برای پیاده سازی Device Guard به صورتی که بتوان از همه ی قابلیت های امنیت مجازی اش استفاده کرد، کامپیوتری که از آن استفاده می کند باید سخت افزار، نرم افزار و سفت افزار مناسب را داشته باشد با این حال کامپیوتر هایی که سخت افزار یا سفت افزار مناسب را نداشته باشند، از قسمتی از محافظت در هنگامی که شما سیاست های درستی کد را پیاده سازی می کنید، بهره می برند. تفاوت اینجاست که این کامپیوتر ها در برابر تهدیدات هدف سختی برای نفوذگران تلقی نمی شوند.

برای مثال کامپیوتر هایی که دارای افزونه ی مجازی سازی CPU یا SLAT هستند برای بدافزار هایی که درخواست دسترسی به هسته را دارند هدف سختی به شمار می آیند. ولی بدون داشتن گزینه های محافظت

از BIOS مانند "بوت شدن فقط از روی هارد دیسک داخلی"، کامپیوتر می تواند به وسیله ی یک مدیای قابل بوت شدن، به یک سیستم عامل بوت شود.

می توان Device Guard را در فاز های مختلف پیاده سازی کرد و این فاز ها را با توجه به برنامه ی کاربر برای به روز رسانی سخت افزار سیستم خود برنامه ریزی کرد.

جدول هایی که در ادامه آمده است، اطلاعات درباره ی سخت افزار، سفت افزار و نرم افزار مورد نیاز برای قابلیت های مختلف Device Gaurd در اختیارتان می گذارد. جدول محافظت های اولیه و محافظت هایی برای امنیت بیشتر که با سخت افزار و سفت افزار های مورد استفاده در سال ۲۰۱۵، ۲۰۱۶ و آنهایی که به عنوان انتخاب در سال ۲۰۱۷ وجود دارند، به کار می رود، را توضیح می دهد.

۵–۲ نیاز های Device Guard برای محافظت اولیه

نیاز های محافظت اولیه	تعریف
CPU ۶۴ بیتی	این سخت افزار برای فعال سازی VBS توسط hypervisor ویندوز مورد نیاز است.
افزونه ی مجازی سازی CPU و صفحات اضافه شده ی جدول ها	**نیازها:** این سخت افزار ها برای VBS مورد نیاز می باشند. یکی از افزونه های مجازی سازی زیر: - (intel) VT-x یا - AMD-V و: - صفحات اضافه شده ی جدول ها که آدرس دهی مرحله ی ۲ هم نامیده می شوند. **سود های امنیتی:** VBS می تواند باعث تامین امنیت هسته جدا از سیستم عامل نرمال شود. آسیب پذیری های Zero-day به دلیل این جدایی نمی توانند وارد کار شوند.
سفت افزار UEFI ورژن 2.3.1.c یا بالا تر به همراه بوت ایمن UEFI	**نیازها:** برای دیدن نیاز ها از این لینک استفاده کنید: https://msdn.microsoft.com/library/windows/hardware/dn932805.aspx#system-fundamentals-firmware-uefisecureboot

	سود های امنیتی: این سخت افزار کمک می کند تا مطمئن باشیم که فقط کد هایی که اجازه دارند روی سیستم بوت می شوند. این قابلیت مانع نصب بوت کیت ها و روت کیت ها شده و از ریبوت جلوگیری می کند.
پروسه ی به روز رسانی سفت افزار ایمن	**نیاز ها:** سفت افزار UEFI باید از به روز رسانی ایمن سفت افزار که در لینک زیر وجود دارد، پشتیبانی کند https://msdn.microsoft.com/library/windows/hardware/dn932805.aspx#system-fundamentals-firmware-uefisecureboot **سود های امنیتی:** سفت افزار UEFI دقیقا مانند هر نرم افزار دیگری ممکن است دارای آسیب پذیری هایی باشد که وقتی کشف می شوند، باید تحت به روز رسانی هایی رفع شوند. به روز رسانی مانع از نصب شدن روت کیت می شود.
درایور های مناسب HVCI[۶]	**نیاز ها:** برای دیدن نیاز ها از این لینک استفاده کنید: https://msdn.microsoft.com/library/windows/hardware/mt589732(v=vs.85).aspx **سود های امنیتی:** درایور های مناسب HVCI کمک می کند تا مطمئن باشیم VBS می تواند اجازه ی دسترسی مناسب حافظه را صادر کند. این موضوع باعث افزایش مقاومت در برابر دورزدن درایور های هسته ی آسیب پذیر می شود و کمک می کند تا درباره اینکه بدافزار ها نتوانند در حالت هسته اجرا شوند، اطمینان پیدا کنیم. تنها کد هایی که توسط درستی کد اجازه گرفته اند می توانند در حالت هسته اجرا شوند.
سیستم عامل ویندوز	**نیازها:** نسخه های آموزشی و صنعتی ویندوز ۱۰، ویندوز سرور ۲۰۱۶ یا ویندوز IoT صنعتی **سود های امنیتی:** از VBS و قابلیت های امنیتی پشتیبانی می کند که باعث می شود تنظیم Device Guard ساده تر شود.

[۶] Hypervisor Code Integrity

۵-۳ نیاز های Device Guard برای امنیت پیشرفته

جدول هایی که در ادامه آمده است، نیاز های اضافی سفت افزار و سخت افزار و امنیت اضافی در ازای آن نیاز ها را شرح می دهند.

۵-۳-۱ نیاز های اضافی برای Device Guard در سال ۲۰۱۵

سفت افزار: **ایمن سازی تنظیمات و مدیریت بوت**	**نیاز ها:** - رمز عبور BIOS یا اجازه دسترسی قوی تر. - در تنظیمات BIOS، تعیین دسترسی به BIOS باید فعال شده باشد. - باید از قابلیت "گزینه های BIOS ایمن" پشتیبانی وجود داشته باشد تا لیست دستگاه های ایمن قابل بوت قابلیت تنظیم داشته باشد و ترتیب بوت دستگاه ها، تنظیمات BOOTORDER که توسط سیستم عامل نوشته شده است را دوباره نویسی کند. - در تنظیمات BIOS، گزینه های BIOS مرتبط با ایمنی و گزینه های بوت باید ایمن سازی شده باشند تا مانع از اجرای سایر سیستم عامل ها و دستکاری تنظیمات BIOS شوند. **سود های امنیتی:** - رمز عبور BIOS سیستم های امنیتی پیشرفته تر کمک میکند مطمئن باشیم تنها مدیران دارای صلاحیت پلتفرم BIOS بتوانند تنظیمات BIOS را تغییر دهند. این موضوع کمک می کند در برابر کاربر دارای حضور فیزیکی امنیت BIOS وجود داشته باشد.

۵-۳-۲ نیاز های اضافی برای Device Guard در سال ۲۰۱۶

سفت افزار: سخت افزار پلتفرم بوت ایمن مورد اطمینان روت شده	**نیاز ها:** یکپارچگی بوت باید پشتیبانی شده باشد. رابط تست امنیت سخت افزار باید پیاده سازی شده باشد. **سود های امنیتی:** - یکپارچگی بوت از زمان روشن شدن باعث محافظت در برابر مهاجمانی که حضور فیزیکی دارند می شود و در برابر بدافزار ها دفاع عمیقی دارد. - HSTI[۷] اطمینان بیشتری برای ایمن بودن پلتفرم به ما می دهد.
سفت افزار: به روز رسانی سفت افزار از طریق به روز رسانی ویندوز	**نیاز ها:** سفت افزار باید به روز رسانی های فیلد از طریق به روز رسانی ویندوز و به روز رسانی UEFI encapsulation را پشتیبانی کند. **سود های امنیتی:** کمک می کند تا از سریع، ایمن و قابل اطمینان بودن به روز رسانی سفت افزار اطمینان حاصل کنیم.
سفت افزار: ایمن سازی تنظیمات و مدیریت بوت	**نیاز ها:** - نیازهای قابلیت های BIOS: قابلیت OEM[۸] برای اضافه کردن ISV[۹]، OEM یا گواهی نامه صنعتی در حالت Boot DB ایمن در هنگام ساخت.

[۷] Hardware Security Testability Specification
[۸] Original equipment manufacturer
[۹] Independent Software Vendor

	- نیاز های تنظیمات: UEFI CA[۱۰] ماکروسافت باید از Boot DB[۱۱] پاک شود. پشتیبانی از ماژول های ثالث UEFI ایرادی ندارد. **سود های امنیتی:** - سرمایه گذار می تواند به درایور ها و برنامه های اختصاصی EFI[۱۲] اجازه ی اجرا دهد. - حذف کردن UEFI CA ماکروسافت از حالت ایمن Boot DB به سرمایه گذاران کنترل کامل روی نرم افزار هایی که قبل از بوت شدن سیستم عامل اجرا می شوند را می دهد.

[۱۰] UEFI Certification Authority
[۱۱] Boot Database
[۱۲] Extensible Firmware Interface

۵-۳-۳ نیاز های اضافی برای Device Guard در سال ۲۰۱۷

سفت افزار: محافظت از UEFI NX[۱۳]	نیازها: - تمام حافظه ی UEFI که به عنوان ناحیه قابل اجرا مشخص شده اند باید فقط قابلیت خواندن داشته باشند. حافظه هایی که قابلیت نوشتن دارند نباید قابل اجرا شدن باشند. سرویس های هنگام اجرای UEFI: - باید UEFI 2.6 EFI_MEMORY_ATTRIBUTES_TABLE را پیاده سازی کنند. تمام حالت اجرای UEFI باید توسط این جدول توضیح داده شده باشد. - تمام ورودی ها باید ویژگی های EFI_MEMORY_RO, EFI_MEMORY_XP یا هر دو را داشته باشند. - هیچ ورودی ای نباید بدون یکی از ویژگی های بالا وجود داشته باشد. چرا که نشان دهنده ی این است که حافظه هم قابل خواندن است و هم قابل اجرا. حافظه باید فقط قابل خواندن و اجرا کردن یا فقط قابل نوشتن و اجرا نکردن باشد. **سود های امنیتی:** - در برابر آسیب پذیری های احتمالی در هنگام اجرای UEFI در توابع مانند Update Capsule، تنظیم متغیر ها و... محافظت می کند به طوری که آنها نمی توانند برای VBS تهدیدی باشند.

[۱۳] Not exucutable

	- حملات به VBS از طریق سفت افزار سیستم را کاهش می دهد.
سفت افزار: سفت افزاری که از محافظت SMM[۱۴] پشتیبانی می کند	**نیازها:** Windows SMM Security Mitigations Table (WSMT) specification شامل جزئیات یک جدول پیشرفته ی تنظیمات و رابط قدرت می شود که برای استفاده ی ویندوز به وجود آمده است و از قابلیت های VBS پشتیبانی میکند. **سود های امنیتی:** - در برابر آسیب پذیری های احتمالی در هنگام اجرای UEFI در توابع مانند Update Capsule، تنظیم متغیر ها و... محافظت می کند به طوری که آنها نمی توانند برای VBS تهدیدی باشند. - حملات به VBS از طریق سفت افزار سیستم را کاهش می دهد. - حملات امنیتی اضافی در برابر SMM را دفع می کند.

[۱۴] System Management Mode

۴-۵ پیاده سازی Device Guard در سناریو های مختلف: دستگاه های متفاوت

پیاده سازی Device Guard در فاز های متفاوت انجام می شود. انتخاب و ترتیب فاز ها بستگی به دستگاه مورد استفاده و درجه ی متخصص IT که آنها را مدیریت میکند، دارد. جدولی که در ادامه آمده است می تواند برای برنامه ریزی برای پیاده سازی Device Guard در سازمان ها کمک کند.

نوع دستگاه	چگونگی ارتباط Device Guard با این نوع دستگاه	اجزای Device Guard که میتوان برای محافظت از این نوع دستگاه از آنها استفاده کرد
دستگاه های Fixed-Workload: یک کار تکراری را هر روز انجام می دهند. لیست برنامه های قابل قبول به ندرت تغییر می کند.	Device Guard می تواند به صورت کامل پیاده سازی شود و پیاده سازی و مدیریت آن ساده است. بعد از پیاده سازی Device Guard تنها برنامه های قبول شده می توانند اجرا شوند. این به این دلیل است که محافظ توسط سرویس HVCI[۱۵] ارائه می شود.	- محافظت VBS فعال - درستی کد در حالت اجرا و UMCI[۱۶] فعال
دستگاه هایی که به صورت کامل مدیریت شده اند: نرم افزار اجازه داده شده توسط بخش IT محدود شده است کاربران می توانند نرم افزار های اضافه را درخواست دهند یا آن ها را از میان نرم افزار های در لیست آماده	اصول اولیه ی سیاست درستی کد می تواند ایجاد و اجرا شود. هنگامی که بخش IT برنامه ی اضافی را تایید کرد، سیاست درستی کد و کاتالوگ را به روز رسانی میکند. سیاست های	- محافظت VBS فعال - درستی کد در حالت اجرا و UMCI فعال

[۱۵] Hypervisor Code Integrity

[۱۶] user mode code integrity

شده از طرف بخش IT نصب کنند.	درستی کد توسط سرویس HVCI پشتیبانی می شوند.	
دستگاه های مدیریت شده ی سبک: این دستگاه ها متعلق به شرکت می باشند ولی کاربر می تواند آزادانه برنامه ها را روی آن نصب کند. دستگاه ها لازم است که برنامه های مدیریت کاربر و آنتی ویروس سازمان را اجرا داشته باشند.	Device Guard میتواند برای محافظت هسته و نظارت بر برنامه ها (برای تشخیص وقوع مشکل احتمالی) به جای محدود کردن آنها درباره ی اجرا شدن مورد استفاده قرار بگیرد.	- محافظت VBS فعال در هنگام اجرا بودن به همراه سیاست درستی کد در حالت بازرسی، hypervisor VBS را مجبور به کمک کردن به اجرای سیاست کد در حالت هسته می کند که باعث محافظت در برابر درایور ها و سیستم فایل های ناشناخته می شود. - درستی کد در حالت اجرا و UMCI فعال، ولی تنها در حالت بازرسی. این به این معنا است که برنامه ها بلاک نیستند. این سیاست تنها یک لاگ از برنامه هایی که خارج از سیاست اجرا می شوند نگه می دارد.
دستگاه شخصی: کارکنان اجازه ی آوردن دستگاه های خودشان به محل کار را دارند و همچنین اجازه ی استفاده از آن ها را در بیرون از محل کار نیز دارند.	Device Guard در این زمینه پیاده سازی نمی شود. در عوض شما می توانید سایر قابلیت های امنیتی و سخت گیرانه ی بر پایه ی راه حل های دسترسی شرطی مانند MDM[۱۷] Microsoft Intune را جستجو کنید.	وجود ندارد.

[۱۷] Mobile Device Management

۵-۵ دوره کردن برنامه ها: ثبت برنامه ها و کاتالوگ فایل ها

در حالت کلی، سیاست های درستی کد برای استفاده از گواهی ثبت برنامه ها در کنار هر چیز دیگری که باعث اعتماد به برنامه ها شود، به وجود آمده اند. این به این معنی است که برنامه یا باید دارای امضای درونی باشد (طوری که امضا قسمتی از کد باینری برنامه است) یا باید از ثبت کاتالوگ استفاده کند. در این روش یک فایل کاتالوگ از برنامه ها درست کرده، آن را ثبت می کنیم و به وسیله ی آن سیاست درستی کد را طوری تنظیم می کنیم که برنامه های در کاتالوگ فایل را به عنوان برنامه ی قابل اعتماد بشناسد.

کاتالوگ فایل ها می توانند برای برنامه های ثبت نشده LOB[۱۸] که می توانند به راحتی دارای یک امضای درونی شوند، بسیار مفید باشند با این حال کاتالوگ فایل باید هربار که برنامه ای به روز رسانی می شود، بروزرسانی شود. در عوض با داشتن امضای درونی با به روز رسانی شدن برنامه نیازی نیست که سیاست های درستی کد به روز رسانی شوند. در نتیجه اگر اضافه کردن امضای برنامه در مراحل توسعه قابل انجام است، می تواند مدیریت سیاست های درستی کد را آسان تر کند.

برای ثبت کردن برنامه ها یا به دست آوردن امضای درونی برای برنامه ها می توان یکی از راه های زیر را انتخاب کرد:

- استفاده از پروسه ی انتشار فروشگاه ویندوز. تمام برنامه هایی که از طریق فروشگاه ویندوز عرضه می شوند دارای گواهی درون فروشگاهی یا گواهی خود برنامه هستند.
- استفاده از گواهی دیجیتال (به عنوان توسعه دهنده در هنگام توسعه ی یک نرم افزار) یا زیر ساخت کلید عمومی.ISV[۱۹] ها و سرمایه گذاران می توانند برنامه های قدیمی ویندوزشان را خودشان ثبت کنند و خودشان را به لیست ثبت کنندگان مورد اعتماد اضافه کنند.
- استفاده از سیستم ثبتی به جز ماکروسافت. ISV ها و سرمایه گذاران از یک سیستم ثبت قابل اعتماد به جز ماکروسافت برای ثبت برنامه های کلاسیک خودشان استفاده کنند.

برای استفاده از ثبت کاتالوگ، می توان از یکی از گزینه های زیر استفاده کرد:

- استفاده از پورتال ثبت Device Guard که برای تجارت در ویندوز ۱۰ است. این پورتال یک سرویس بر پایه ی وب ماکروسافت است که می تواند برای ثبت برنامه های کلاسیک ویندوز از آن استفاده کرد.

---

[۱۸] Line-Of-Bussiness

[۱۹] Independent Software Vendor

- ایجاد کاتالوگ فایل ها

۵-۶ کاتالوگ فایل ها

کاتالوگ فایل ها شامل اطلاعاتی درباره ی تمام باینری فایل های پیاده سازی شده و در حال اجرا مرتبط با برنامه های قابل اعتماد ولی ثبت نشده ی کاربر هستند. کاربر هنگامی که کاتالوگ فایل ها را می سازد، می تواند برنامه های ثبت شده را هم درون آن ها قرار دهد. به این منظور که نمی خواهد به ثبت کننده برنامه به جز در آن برنامه ی خاص اعتماد کرد. بعد از درست کردن یک کاتالوگ، باید آن را به وسیله ی کلید عمومی زیرساخت، یا یک کد ثبت خریداری شده ثبت کرد. بعد از آن می توان آن کاتالوگ را توزیع کرد و برنامه های مورد اعتماد کاربر می توانند مانند برنامه های ثبت شده توسط سیاست های درستی کد، به رسمیت شناخته شوند.

فایل های کاتالوگ لیست هش شده ی باینری های یافت شده هستند. باینری های هش شده ی هر برنامه با به روز رسانی آن برنامه، به روز رسانی می شوند که باعث به روز رسانی فایل کاتالوگ هم می شود.

بعد از اینکه کاربر فایل کاتالوگ خود را درست کرده و آن را ثبت کرد، می تواند سیاست های درستی کد خود را طوری تنظیم کند که به ثبت کننده اعتماد کند یا گواهی آن فایل ها را ثبت کند.

۵-۷ نحوه ی سیاست های درستی کد و ثبت کردن

زمانی که کاربر یک سیاست درستی کد ایجاد می کند، در حال درست کردن یک فایل باینری-کد شده ی XML می باشد که شامل تنظیمات حالت هسته و حالت کاربر ویندوز ۱۰، به همراه محدودیت های میزبان های اسکریپت ویندوز ۱۰ است. می توان فایل اصلی XML را توسط یک ویرایشگر متن باز و آن را مشاهده کرد.

پیشنهاد می شود فایل اصلی XML را برای زمانی که می خواهید سیاست درستی کد را با سیاست دیگری ترکیب کنید یا قوانین آن را به روز رسانی کنید، نگه دارید. برای پیاده سازی، فایل، تبدیل به فرمت باینری می شود، که می تواند توسط Windows Power Shell هم انجام شود.

وقتی سیاست درستی کد پیاده سازی شد، برنامه هایی که می توانند روی یک سیستم اجر شوند را محدود می کند. فایل XML می تواند ثبت شود، که این کار کمک به اضافه کردن امنیت بیشتر در برابر کاربران مدیری که سعی در تغییر یا حذف سیاست ها دارند می کند.

۶ راه اندازی Device Guard در ویندوز ۱۰

۶-۱ مدیریت Device Guard با استفاده از Configuration Manager

برای راه اندازی و مدیریت Device Guard و اپلیکیشن های قابل پشتیبانی از آن می توان از Configuration Manager استفاده نمود. Configuration Manager برای انجام سناریو های زیر کاربرد خواهد داشت:

- تعیین اینکه چه کلاینتی پیش نیاز های استفاده از Device Guard را دارد
- فعال سازی تنظیمات Device Guard
- پیاده سازی قوانین Device Guard
- فعال سازی اپلیکشن هایی که از Device Guard پشتیبانی می کنند

در ادامه هر کدام را بیشتر توضیح خواهیم داد.

Configuration Manager و دیگر ابزارهای وابسته به آن در مجموعه Windows Assessment and Deployment Kit یا همان Windows ADK وجود دارد. به همین منظور برای دسترسی به این ابزار باید Windows ADK را نصب نمود.

۶-۲ تعیین سیستم های قابل اعمال

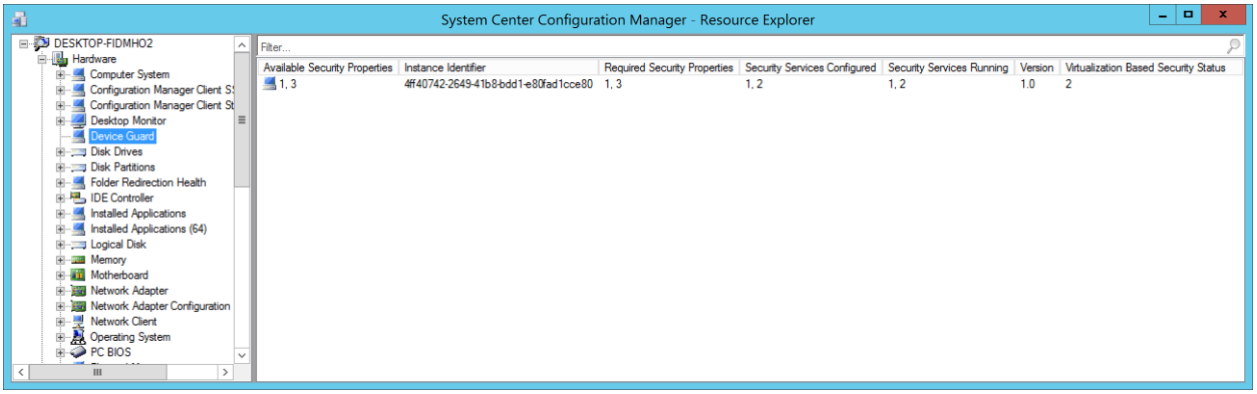
کامپیوتر های مبتنی بر ویندوز ۱۰ باید دارای پیش نیاز های مشخصی برای فعال سازی Device Guard باشند. برای تعیین اینکه یک کامپیوتر این قابلیت را دارد یا خیر مراحل زیر را باید طی کرد:

- کنسول Configuration Manager را باز کرده و به فضای کاری Administrator تغییر حالت می دهیم. سپس Client Settings را انتخاب می کنیم.
- گروه Hardware Inventory را انتخاب نموده و سپس Set Classes را انتخاب می کنیم.
- Device Guard شامل یک کلاس WMI[۲۰] به منظور گرفتن پرس و جوی تنظیمات و حالت های مدیریتی خود می باشد. این کلاس می تواند به عنوان یک کلاس فهرست سخت افزاری اضافه شود. بدین منظور بر روی Add کلیک کنید.

[۲۰] Windows Management Instrumentation

- بر روی Connect کلیک کنید. در صورتی که این کار را بر روی ویندوز ۱۰ انجام می دهید نام محلی کامپیوتر را تغییر ندهید. در صورتی که از ویندوز سرور استفاده می کنید، نام سیستم ویندوز ۱۰ از راه دور را وارد کنید. در هر دو حالت فضای نام WMI را rootMicrosoftWindowsDeviceGuard قرار دهید.
- کلاس Win32_DeviceGuard را انتخاب کنید.
- بر روی OK کلیک کنید تا تنظیمات ذخیره شود.

در این صورت، به محض اینکه کامپیوتر مورد نظر سیکل hardware inventory را اجرا نمود، یک گزارش در کلاس Device Guard برگشت داده خواهد شد که می توان آن را در Resource Explorer مشاهده نمود:



توسط این داده فهرست، می تواند گزارش های سفارشی و یا مجموعه هایی را ایجاد نمود.

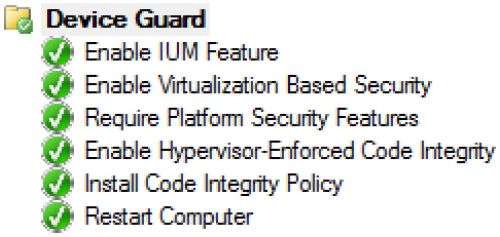
۳-۶ انجام تنظیمات Device Guard

تنظیمات Device guard برای یک دستگاه می تواند در مرحله اولیه استقرار ویندوز ۱۰ انجام گیرد و یا اینکه برای ویندوز ۱۰ ایی که قبلا عملیاتی شده پیکربندی شود. دو راه اصلی برای اینکار وجود دارد: راه اول، نوشتن یک اسکریپت و استقرار آن توسط یک پکیج و یا یک برنامه و راه دوم، انجام توالی وظایف توسط Configuration Manager. مایکروسافت پیشنهاد می کند که Device Guard در مرحله اولیه استقرار، پیکربندی شود تا به صورت پیش فرض فعال باشد.

اولین پیشنیاز Hyper-V Hypervisor (Microsoft-Hyper-V-Hypervisor) است. Device Guard از Hyper-V به منظور محافظت و ایزوله کردن مولفه های ویندوز و پروسه ها در مقابل سطح بالای سیستم عامل استفاده می کند.

پیشنیاز دوم، تولید قوانین Device Guard است. در این گزارش فایل قوانین، SIPolicy.p7b نام دارد.

بعد از اینکه نصب شد، توالی وظایف زیر برای فعال سازی Device Guard و اعمال قوانین Device Guard نیاز است:



مراحل توالی وظایف Device Guard به شرح زیر می باشد (تمامی مراحل زیر به جز مرحله آخر، در خط فرمان Run اجرا می شود):

- فعال سازی قابلیت ایزوله سازی در مد کاربر:

dism.exe /NoRestart /Online /Enable-Feature:IsolatedUserMode /All

- فعال سازی امنیت مبتنی بر مجازی سازی:

reg.exe add “HKLMSYSTEMCurrentControlSetControlDeviceGuard” /v “EnableVirtualizationBasedSecurity” /t REG_DWORD /d 1 /f

- درخواست قابلیت امنیت پلتفرم:

reg.exe add “HKLMSYSTEMCurrentControlSetControlDeviceGuard” /v “RequirePlatformSecurityFeatures” /t REG_DWORD /d 2 /f

- فعال سازی صحت کد در Hypervisor:

reg.exe add “HKLMSYSTEMCurrentControlSetControlDeviceGuard” /v “HypervisorEnforcedCodeIntegrity” /t REG_DWORD /d 1 /f

- نصب قانون صحت کد:

xcopy \servershareSIPolicy.p7b C:Windowssystem32CodeIntegrity /y

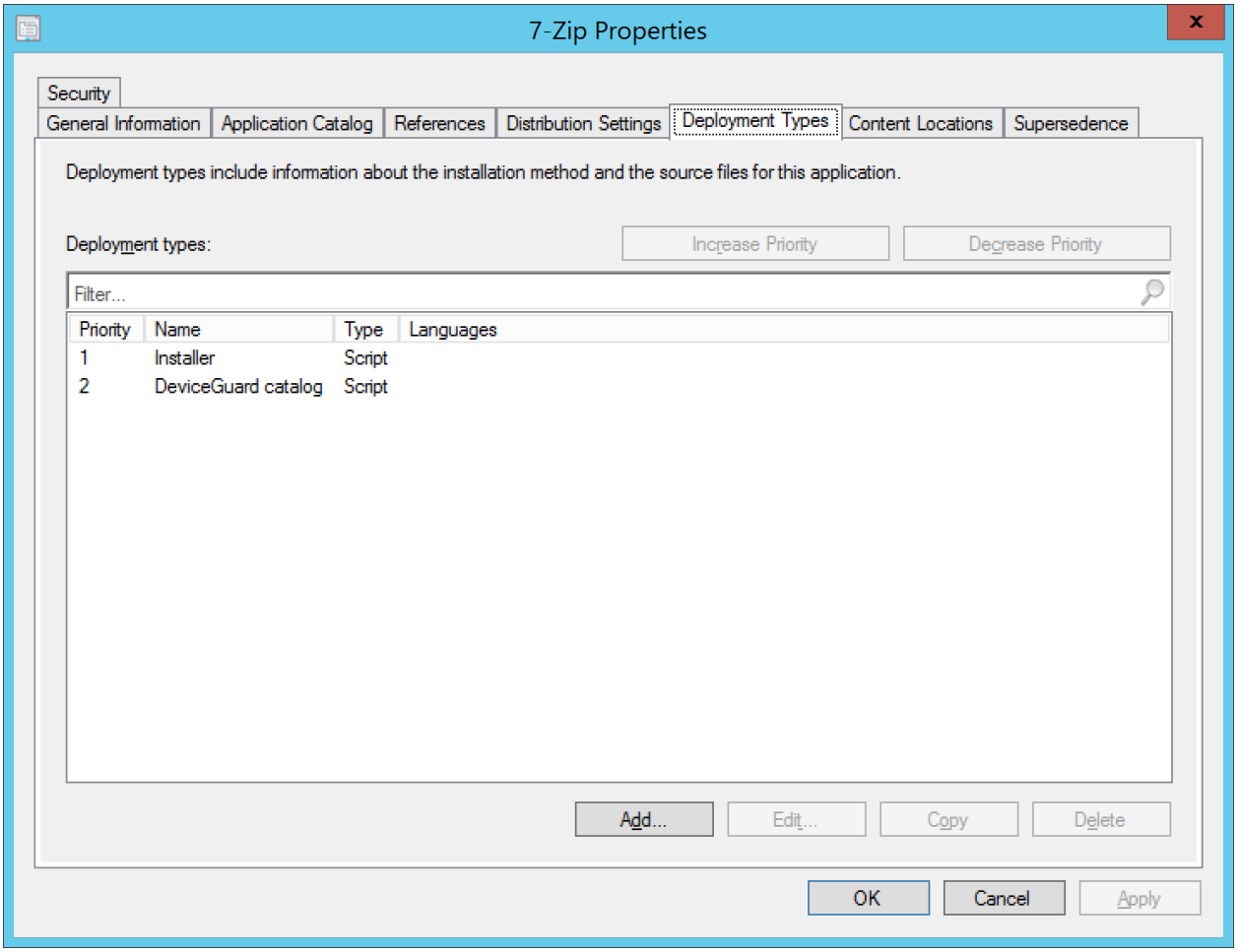
۶-۴ استقرار یک برنامه با قابلیت پشتیبانی از Device Guard

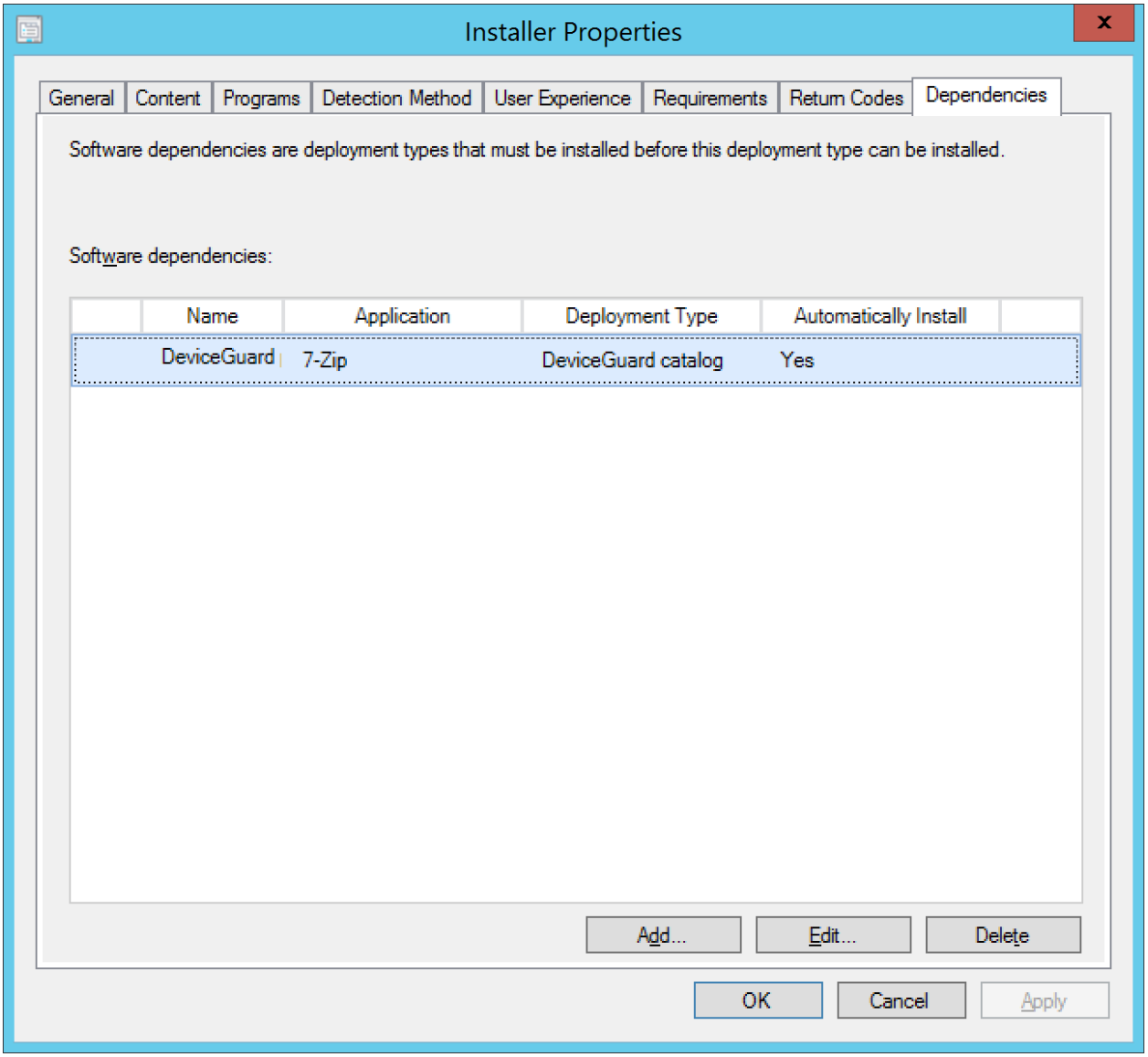
به محض اینکه Device Guard فعال شد و قوانین مربوط به آن اعمال شد، ویندوز ۱۰ اجرای برنامه ها را بر روی دستگاه محدود می کند (برنامه های امضا شده توسط Windows Store شامل قانون صحت کد نخواهند شد. برای محدود کردن اجرای برنامه های موجود در Windows Store باید از ویژگی AppLocker استفاده نمود). برای برنامه هایی که به صورتی دیجیتالی امضا نشده اند و یا اینکه با یک گواهینامه ای که در قانون صحت کد ذکر نشده، امضا شده باشند، مستندات Device Guard جزئیاتی را ارائه می دهد تا بتوان یک فایل کاتالوگ برای معرفی این برنامه به Device Guard تولید کرد. این کاتالوگ می تواند امضا شود و همراه برنامه ارائه شود تا امکان اجرا بر روی سیستم هایی که Device Guard فعال دارند را داشته باشد.

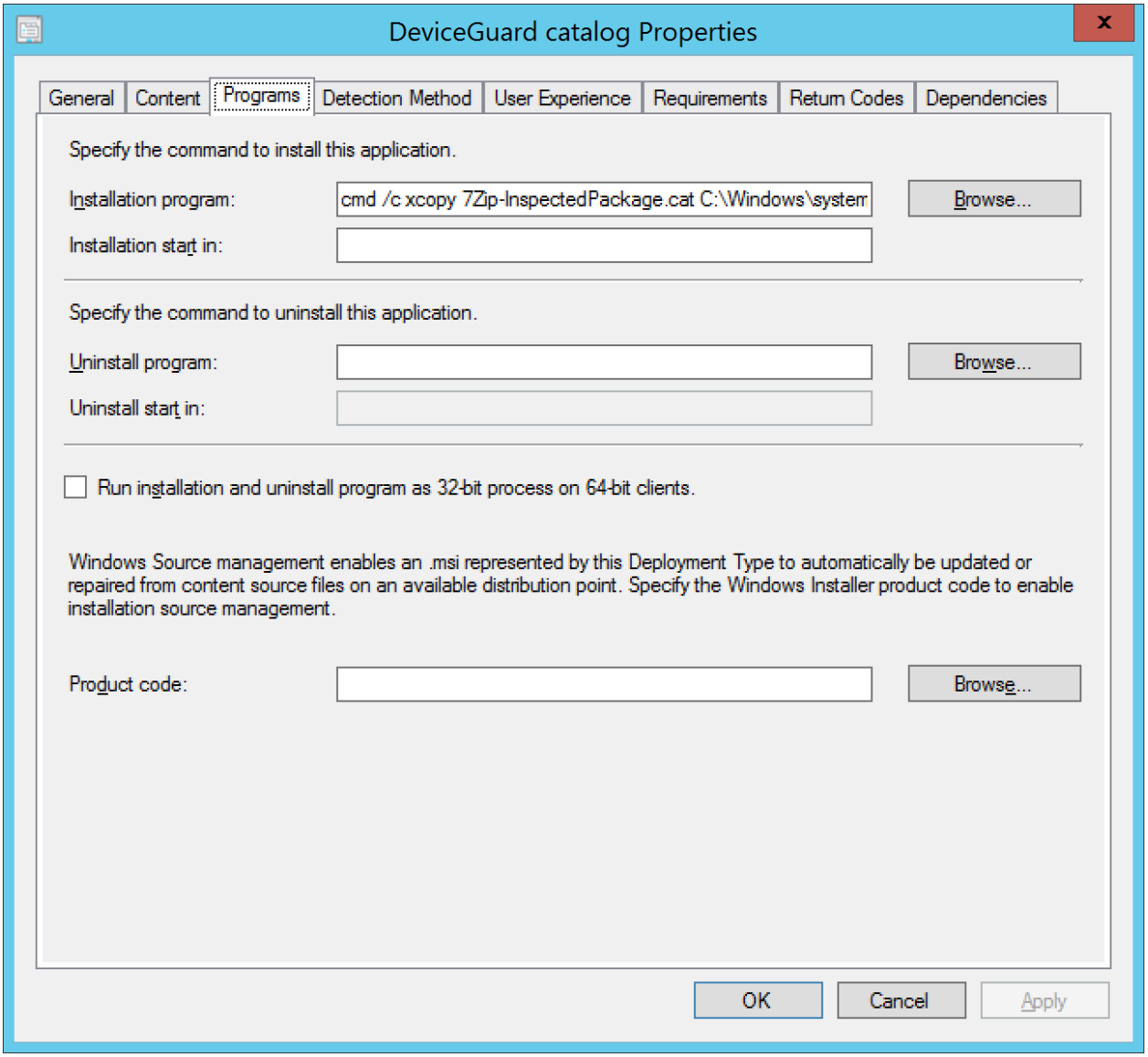
کاتالوگ های امضا شده را می توان توسط اعمال نفوذ قابلیت های ذاتی یک برنامه Configuration Manager به راحتی گسترش داد. برای اینکار کافیست کاتالوگ را درون همان دایرکتوری که فایل های نصب برنامه قرار دارد، قرار داد.

- ایجاد برنامه (در اینجا برنامه 7-Zip را مثال زده ایم).
- ایجاد یک مدل استقرار[۲۱] (DT) توسط خط فرمان.
- ایجاد یک مدل استقرار ثانویه (اسکریپت) توسط فرمان زیر در خط فرمان:
- دیگر تنظیماتی که می توان بر روی این DT (مدل استقرار) اعمال نمود. مانند روش تشخیص کاتالوگ و یا پیش نیاز ها.
- نصب DT اولیه را وابسته به نصب DT دومی کنید. این باعث می شود تا کاتالوگ نخست کپی شود و سپس کد خط فرمان برای راه اندازی آن اجرا شود.

[۲۱] Deployment Type


7-Zip Properties
Security
General Information
Application Catalog
References
Distribution Settings
Deployment Types
Content Locations
Supersedence
Deployment types include information about the installation method and the source files for this application.
Deployment types:
Increase Priority
Decrease Priority
Filter...
Priority
Name
Type
Languages
1
Installer
Script
2
DeviceGuard catalog
Script
Add...
Edit...
Copy
Delete
OK
Cancel
Apply


Installer Properties
General
Content
Programs
Detection Method
User Experience
Requirements
Return Codes
Dependencies
Software dependencies are deployment types that must be installed before this deployment type can be installed.
Software dependencies:
Name
Application
Deployment Type
Automatically Install
DeviceGuard
7-Zip
DeviceGuard catalog
Yes
Add...
Edit...
Delete
OK
Cancel
Apply


DeviceGuard catalog Properties
General
Content
Programs
Detection Method
User Experience
Requirements
Return Codes
Dependencies
Specify the command to install this application.
Installation program:
cmd /c xcopy 7Zip-InspectedPackage.cat C:\Windows\system
Browse...
Installation start in:
Specify the command to uninstall this application.
Uninstall program:
Browse...
Uninstall start in:
Run installation and uninstall program as 32-bit process on 64-bit clients.
Windows Source management enables an .msi represented by this Deployment Type to automatically be updated or repaired from content source files on an available distribution point. Specify the Windows Installer product code to enable installation source management.
Product code:
Browse...
OK
Cancel
Apply

۷ منابع

- https://technet.microsoft.com/en-us/itpro/windows/whats-new/whats-new-windows-10-version-1507-and-1511
- https://technet.microsoft.com/en-us/itpro/windows/keep-secure/device-guard-deployment-guide
- http://www.theregister.co.uk/2015/09/16/microsoft_windows_10_device_guard/
- http://searchsecurity.techtarget.com/tip/Microsoft-Device-Guard-tackles-Windows-10-malware