In de spotlights: verbeterde controle van USB- en Bluetooth-apparaten

juli 30, 2020
by Eyal Erlich

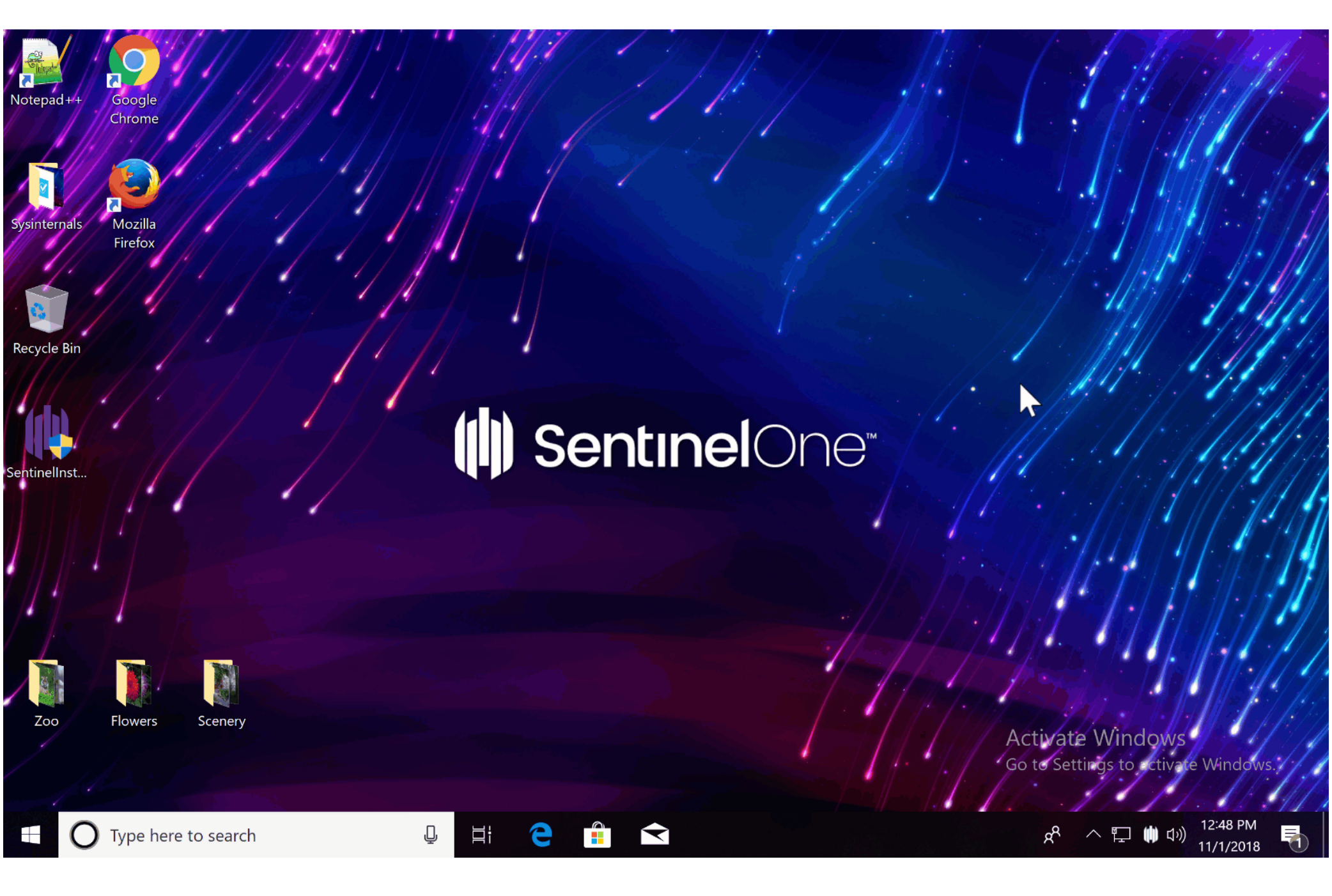
In 2018 hebben we Device Control toegevoegd aan ons platform. Beheerders en beveiligingsteams konden hiermee het gebruik van USB- en andere randapparatuur in het hele netwerk beheren. Vandaag kondigen we de nieuwste updates van deze functie aan. Hiermee is het mogelijk USB-, Bluetooth- en Bluetooth Low Energy-apparaten uitermate fijnmazig te beheren. Met onze bijgewerkte Device Control-functie kunnen IT- en SOC-teams de bedrijfscontinuïteit waarborgen voor alle eindgebruikers die externe apparaten moeten kunnen gebruiken en tegelijkertijd de aanvalsmogelijkheden tot een absoluut minimum beperken.

Wat zijn de beveiligingsrisico's van USB- en andere randapparaten?

Randapparaten die via USB of Bluetooth worden aangesloten, zijn alomtegenwoordig in het bedrijfsleven. Ze zijn nog steeds onmisbaar voor zakelijke apparatuur, van laptops tot werkstations en zelfs slimme IoT-apparaten. De talrijke aanwezigheid van randapparaten die zijn verbonden met endpoints in de organisatie, is ook bij cybercriminelen niet onopgemerkt gebleven. Uit een recent rapport blijkt bijvoorbeeld dat cyberdreigingen van operationele technologiesystemen via verwisselbare USB-media in het afgelopen jaar bijna zijn verdubbeld. Malware op verwisselbare media wordt onder andere gebruikt om backdoors te openen, persistente externe toegang te geven en andere schadelijke payloads af te leveren.

Aanvallers vinden steeds weer nieuwe creatieve manieren om mensen te verleiden een vreemde USB-stick in hun bedrijfscomputer te steken. In één geval ontvingen slachtoffers bijvoorbeeld een envelop met een nepcadeaukaart van een bekende winkelketen, samen met een USB-stick waarop malware stond. USB-stations zijn ook een belangrijke vector voor het stelen van vertrouwelijke en bedrijfskritische data. Door de recente toename in het werken vanuit huis (of waar dan ook behalve op kantoor) is het risico dat werknemers randapparaten aansluiten die niet door het bedrijf zijn goedgekeurd, alleen maar groter geworden.

Bij het ontwerpen van deze functie hebben we rekening gehouden met accountvereisten zoals systeemstabiliteit, interoperabiliteit en ondersteuning voor meerdere platforms (Windows en macOS).



Device Control: eenvoudig policy management om apparaten toe te voegen, te blokkeren of te beperken

Om de implementatie gemakkelijker te maken, biedt deze functie maximale fijnmazigheid *en* flexibiliteit bij het definiëren van een Device Control policy voor de onderneming.

U kunt een Device Control policy instellen voor de hele onderneming, voor een specifieke locatie of zelfs voor een specifieke groep apparaten. Een policy wordt opgebouwd uit een set Device Control-regels.

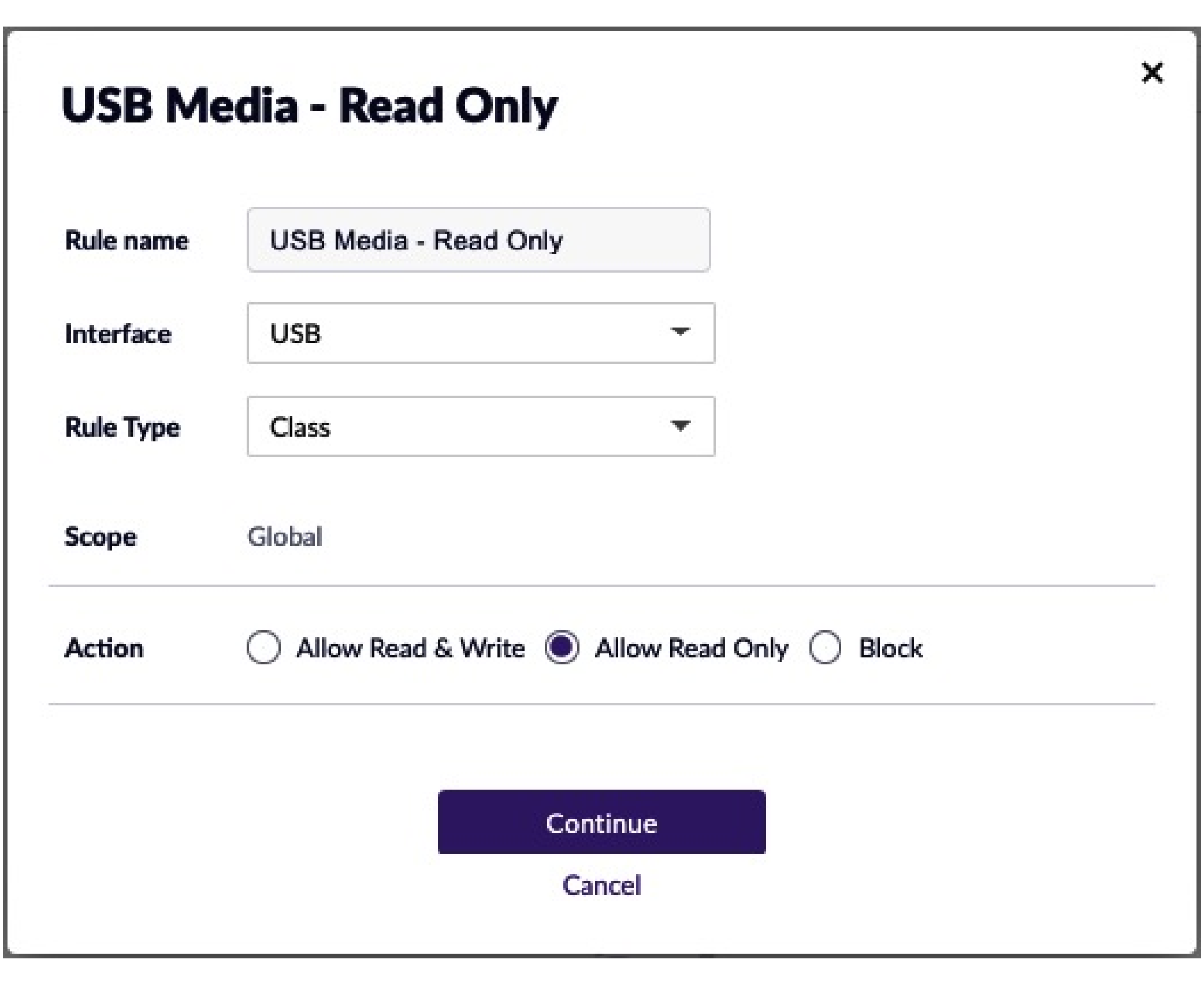
Een regel wordt gedefinieerd door eerst het type interface (USB of Bluetooth) te kiezen en vervolgens het type regel en de actie. We kunnen USB-apparaten bijvoorbeeld beheren op basis van de volgende attributen:

- Vendor ID
- Class
- Serial ID
- Product ID

En vervolgens de gewenste actie:

- Allow Read & Write
- Allow Read Only
- Block

Op deze manier kan de beheerder gedetailleerde policy-regels maken. Het is bijvoorbeeld mogelijk om een regel te maken waarmee specifieke gebruikers toegang hebben tot bepaalde typen USB-apparaten, andere gebruikers verwisselbare USB-media alleen mogen gebruiken om bestanden te lezen en voor alle overige gebruikers het gebruik van USB-apparaten helemaal wordt geblokkeerd.



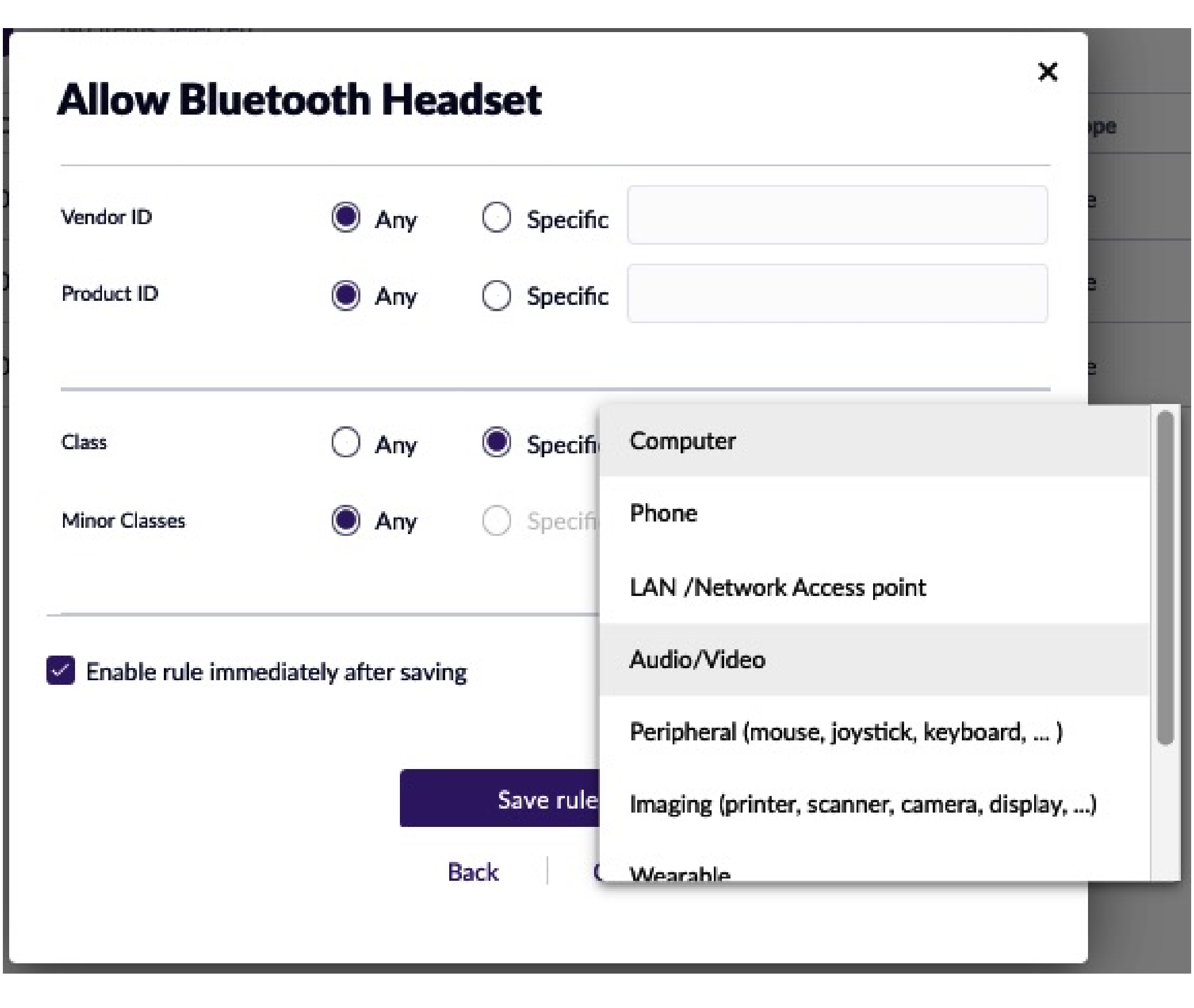
USB Media - Read Only

Rule name: USB Media - Read Only
Interface: USB
Rule Type: Class
Scope: Global
Action: ○ Allow Read & Write ● Allow Read Only ○ Block

Bluetooth-beveiliging: gaten dichten

Het Bluetooth-protocol heeft van oudsher veel kwetsbaarheden. De meeste hiervan zitten in oudere Bluetooth-versies en bedrijven die beveiliging belangrijk vinden, moeten gebruikers geen toestemming geven om dergelijke apparaten verbinding te laten maken met hun endpoints (en dus ook hun netwerk).

Met SentinelOne Device Control kan het gebruik van *alle* Bluetooth-apparaten worden toegestaan of beperkt, maar ook op basis van het type (bijvoorbeeld toetsenbord, muis, koptelefoon) of op basis van de versie van het Bluetooth-protocol (om het risico van kwetsbaarheden in oudere Bluetooth-versies te verkleinen).



Allow Bluetooth Headset

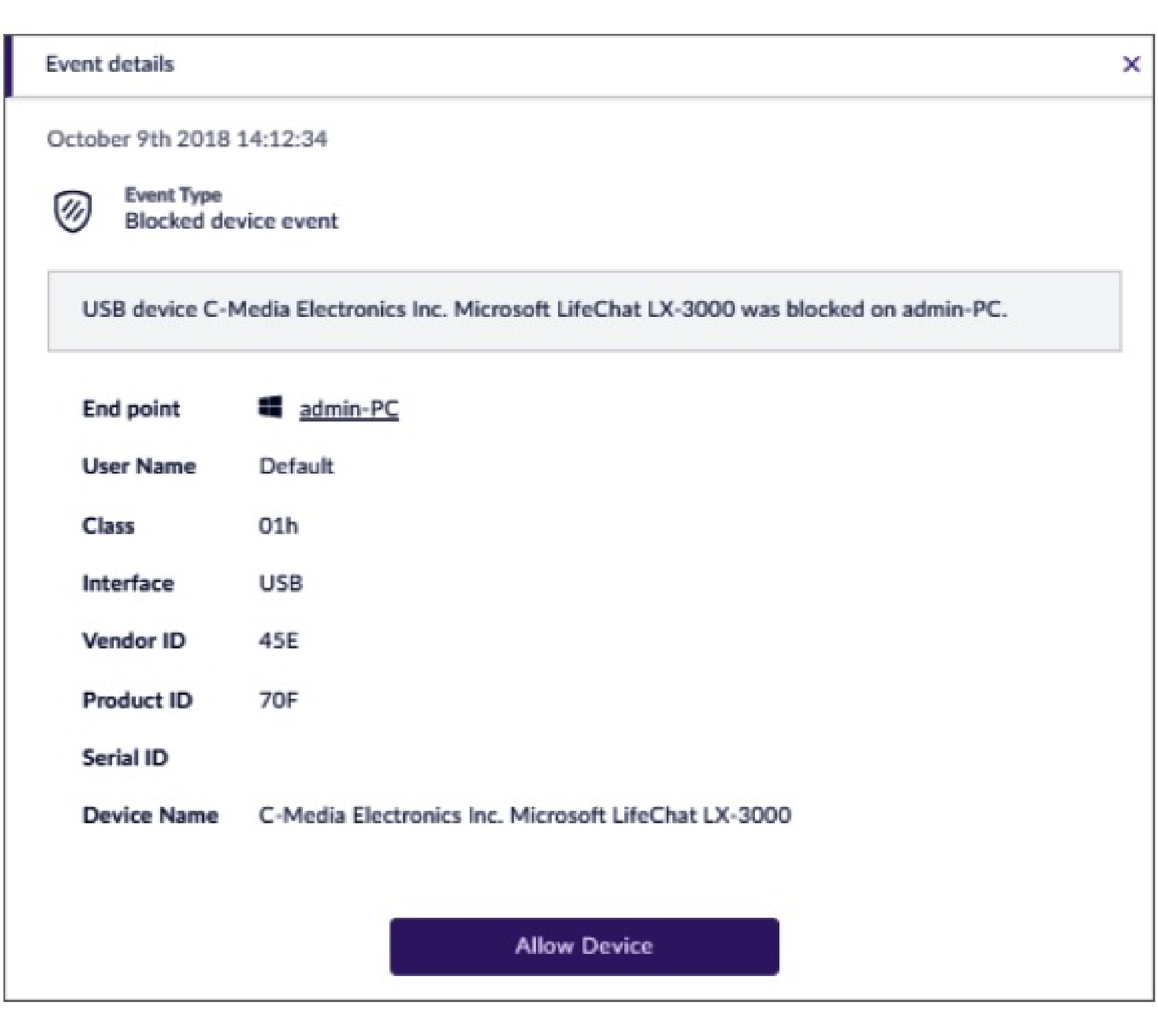
Vendor ID: ● Any ○ Specific
Product ID: ● Any ○ Specific
Class: ○ Any ● Specifi
Minor Classes: ● Any ○ Specifi

☑ Enable rule immediately after saving

Flexibiliteit en controle over elk apparaat

Met SentinelOne Device Control kunnen beheerders heel eenvoudig policies definiëren. Tegelijkertijd weten we dat er elke dag weer nieuwe apparaten in het bedrijf kunnen worden geïntroduceerd. Beheerders hebben daarom de flexibiliteit nodig om te reageren op het moment dat dit nodig is en nieuwe USB-apparaten goed te keuren zodra die op het systeem verschijnen (en erdoor worden geblokkeerd).

Een beheerder kan nu elk apparaat zien dat in het activiteitenlogboek van de beheerconsole is geblokkeerd en desgewenst van daaruit goedkeuren.



Event details

October 9th 2018 14:12:34

Event Type
Blocked device event

USB device C-Media Electronics Inc. Microsoft LifeChat LX-3000 was blocked on admin-PC.

End point	admin-PC
User Name	Default
Class	01h
Interface	USB
Vendor ID	45E
Product ID	70F
Serial ID	
Device Name	C-Media Electronics Inc. Microsoft LifeChat LX-3000

Conclusie

Samen met SentinelOne Firewall Control biedt Device Control de ontbrekende stukjes om oudere antivirusoplossingen volledig te vervangen door een product van de volgende generatie. Net zoals de andere functies van het platform worden ook deze twee door de agent van SentinelOne geleverd, op alle platforms en vanuit dezelfde beheerconsole.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

©2022
Privacybeleid Servicevoorwaarden