Función destacada: Device Control con mejoras para dispositivos USB y Bluetooth

julio 30, 2020
by SentinelOne

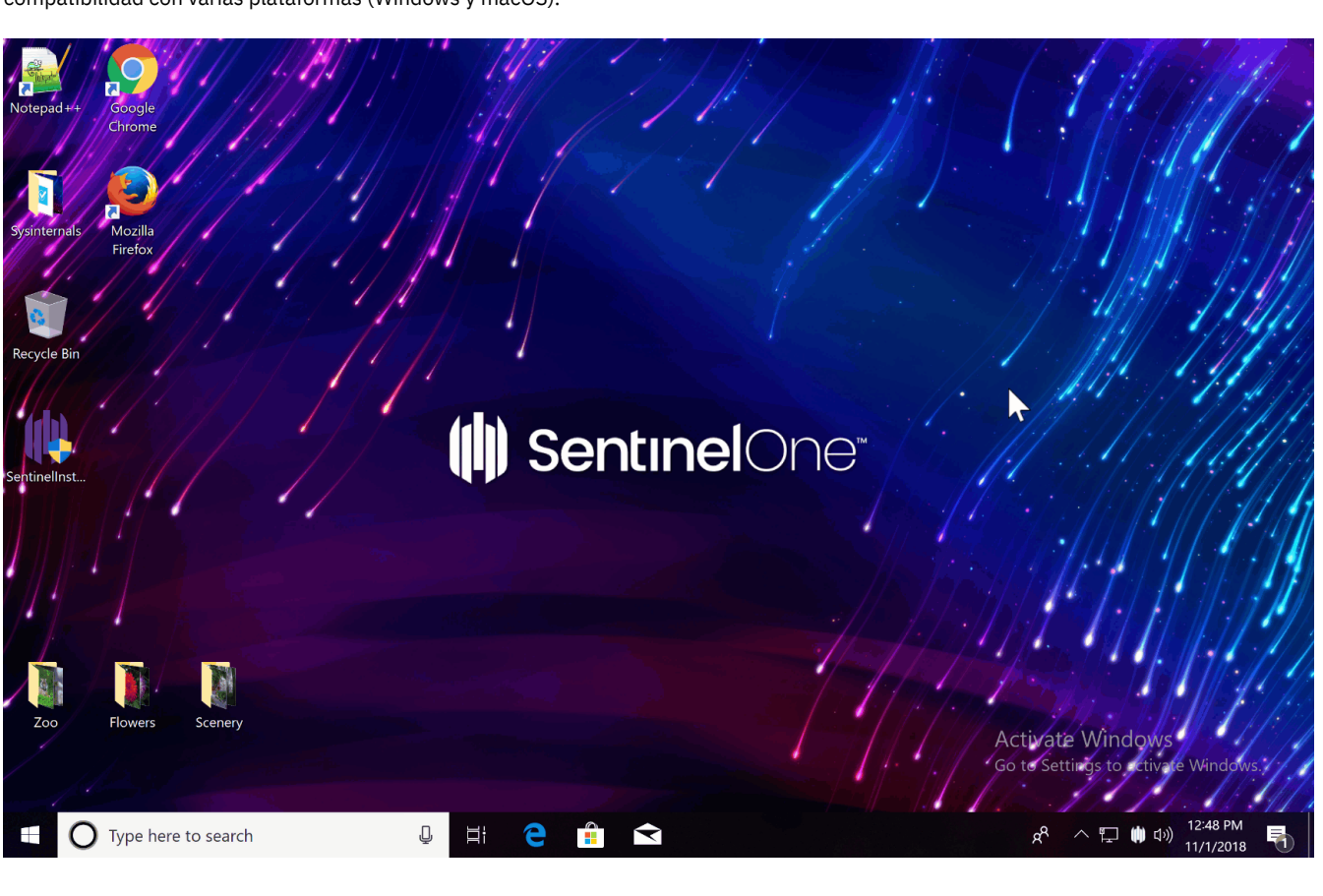
En 2018, anunciamos la llegada a nuestra plataforma de la función Device Control que permite a los administradores y a los equipos de seguridad administrar el uso de unidades USB y otro tipo de dispositivos periféricos en la red. Hoy, nos complace anunciar su nueva actualización. Esta función permite ahora administrar dispositivos USB, Bluetooth y Bluetooth Low Energy con el máximo nivel de pormenorización posible. Gracias a esta actualización, los equipos de TI y del SOC pueden garantizar la continuidad de las actividades para todos los usuarios que necesiten utilizar dispositivos externos, y además, limitando al mínimo la superficie de ataque.

¿Cuáles son los riesgos de seguridad asociados a las unidades USB y otros periféricos?

Los periféricos conectados mediante USB o Bluetooth son omnipresentes y siguen siendo un componente esencial de los dispositivos profesionales, como los portátiles, estaciones de trabajo e incluso los dispositivos IoT inteligentes. Esta prevalencia de los periféricos conectados a los endpoints de la empresa no ha pasado desapercibida para los ciberdelincuentes. Según un informe reciente, en los últimos 12 meses prácticamente se han duplicado las ciberamenazas dirigidas a sistemas de tecnología operativa (TO) a través de dispositivos USB extraíbles. El malware transferido a través de estos soportes extraíbles se ha utilizado, entre otras cosas, para abrir puertas traseras, establecer el acceso remoto persistente y distribuir cargas útiles maliciosas.

Los ciberdelincuentes han encontrado nuevas formas creativas de convencer a sus víctimas para que conecten en sus equipos corporativos unidades USB desconocidas. Por ejemplo, en un incidente, unas personas recibieron un sobre que contenía una tarjeta regalo falsa de BestBuy, una empresa especializada en la venta de productos electrónicos, acompañada de una llave USB que contenía malware. Además, las unidades USB representan uno de los principales vectores de fuga de datos críticos y confidenciales, y el reciente cambio al teletrabajo no ha hecho sino aumentar el riesgo de que los empleados conecten periféricos no aprobados por la empresa en su nuevo entorno de trabajo.

Para diseñar esta funcionalidad, tuvimos en cuenta determinados factores, como la estabilidad del sistema, la interoperabilidad y la compatibilidad con varias plataformas (Windows y macOS).



Control de dispositivos: una administración de directivas simple para autorizar, prohibir o limitar el uso de dispositivos

Para simplificar la implementación, hemos diseñado esta función de manera que ahora ofrece un excelente nivel de pormenorización y de flexibilidad a la hora de crear directivas de Device Control para la empresa.

Estas directivas pueden aplicarse a toda la empresa, a un sitio determinado o incluso a un grupo concreto de dispositivos. Una directiva se compone de un conjunto de reglas de Device Control.

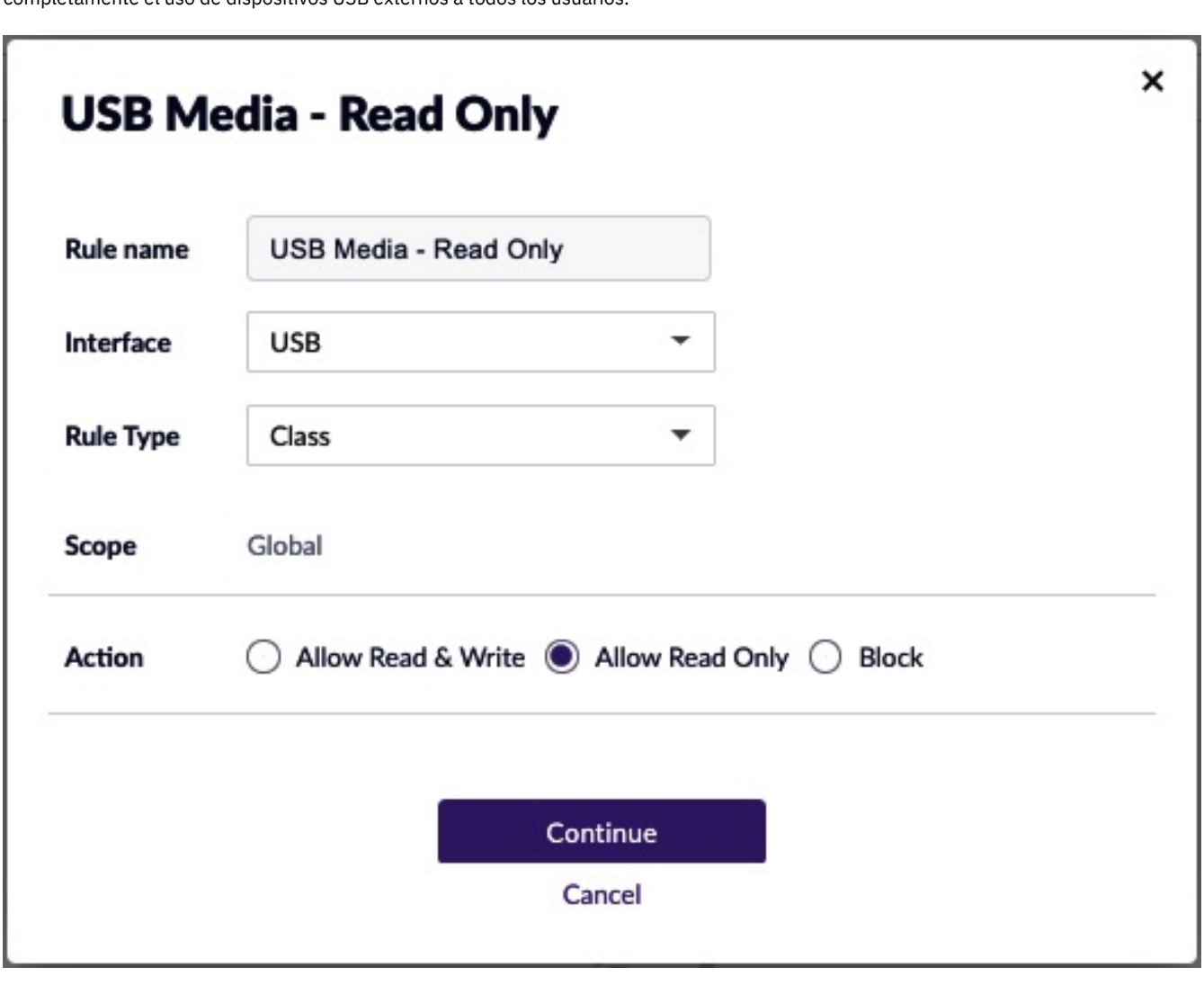
La definición de las reglas empieza por seleccionar el tipo de interfaz (USB o Bluetooth) y, a continuación, el tipo de regla y la acción deseada. Por ejemplo, podemos controlar dispositivos USB en función de los siguientes atributos:

- Vendor ID (ID de proveedor)
- Class (Categoría)
- Serial ID (ID de serie)
- Product ID (ID de producto)

A continuación, la acción deseada:

- Allow Read & Write (Autorizar lectura y escritura)
- Allow Read Only (Autorizar solo lectura)
- Block (Prohibir el acceso)

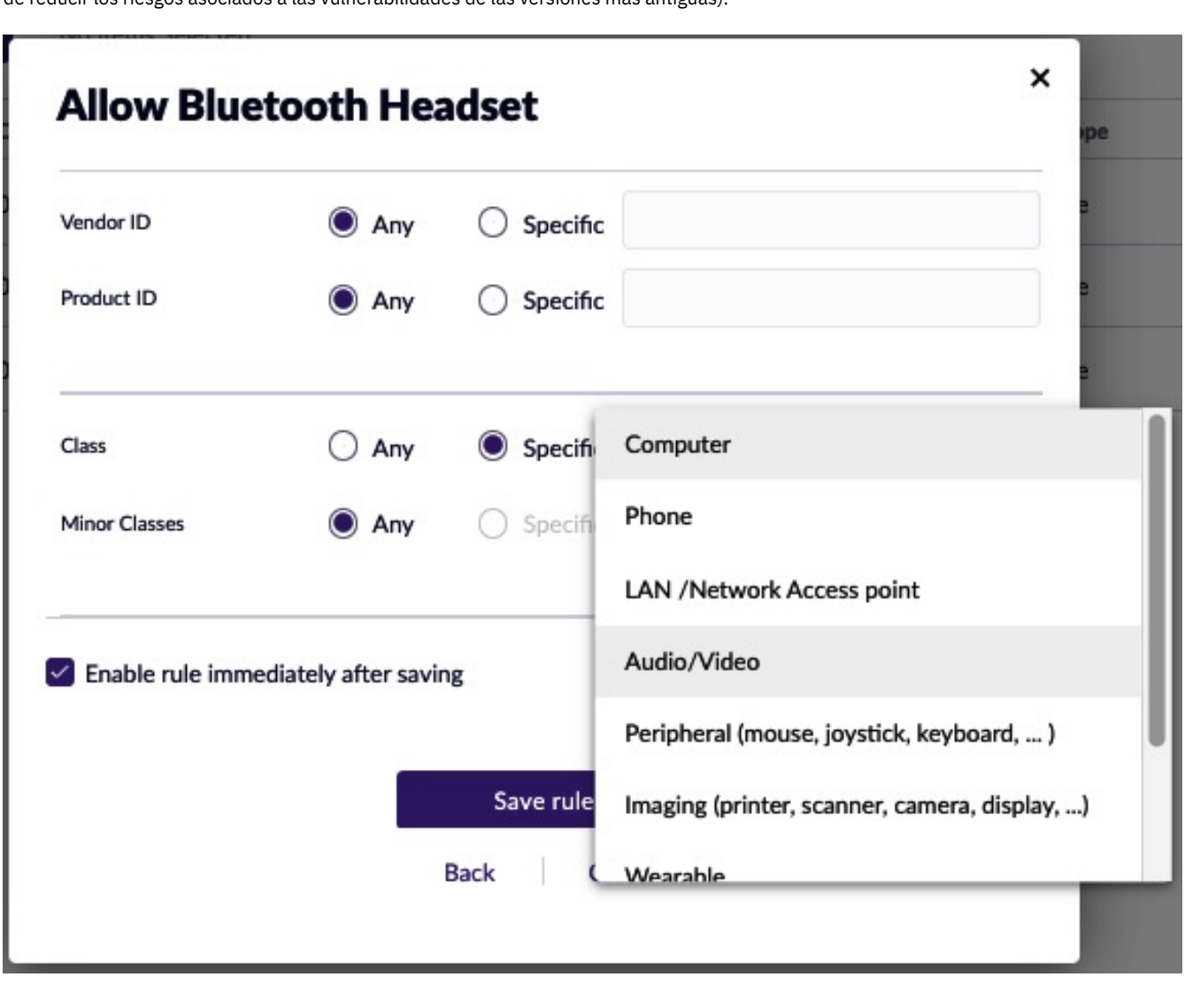
Esto permite al administrador definir directivas pormenorizadas. Por ejemplo, es posible crear una regla que permita a determinados usuarios acceder a ciertos tipos de dispositivos USB, que autorice a otros a utilizar unidades USB de solo lectura y que prohíba completamente el uso de dispositivos USB externos a todos los usuarios.



Cómo cubrir las brechas de seguridad de Bluetooth

El protocolo Bluetooth está plagado de vulnerabilidades. La mayoría de ellas se encuentran en las versiones más antiguas de Bluetooth y las empresas preocupadas por la seguridad no deben permitir que sus usuarios conecten estos dispositivos a los endpoints (y, por consiguiente, a las redes) de la empresa.

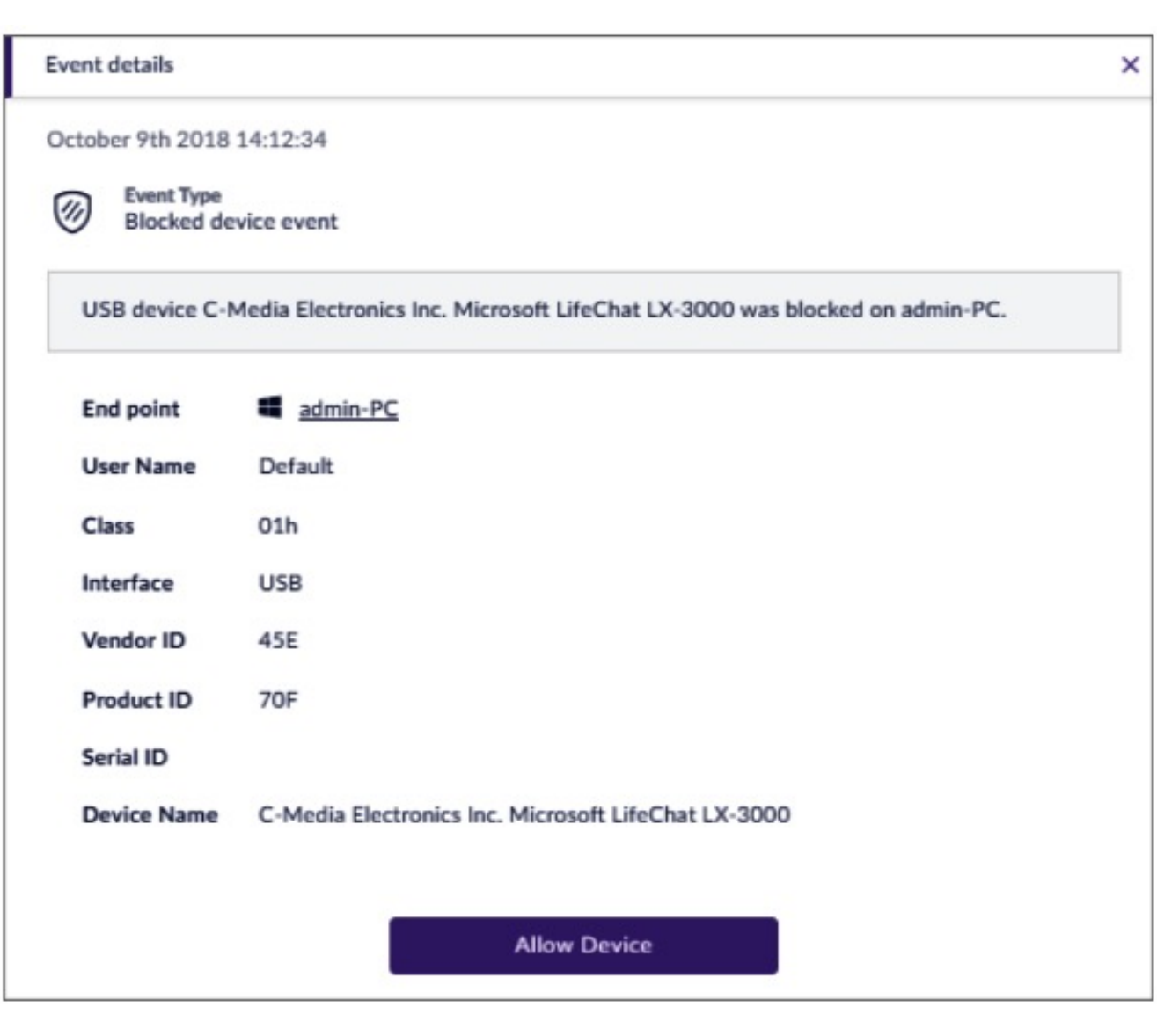
SentinelOne Device Control permite autorizar o limitar el uso de *todos* los dispositivos Bluetooth o de determinados dispositivos Bluetooth (p. ej., teclados, ratones o auriculares), o incluso autorizar o no el uso de dispositivos en función de la versión del protocolo Bluetooth (a fin de reducir los riesgos asociados a las vulnerabilidades de las versiones más antiguas).



Flexibilidad y control de todos los dispositivos

Con SentinelOne Device Control los administradores pueden definir fácilmente directivas, aunque también somos conscientes de que en la empresa se incorporan nuevos dispositivos a diario. Sabemos que los administradores necesitan flexibilidad para responder rápidamente y aprobar nuevos dispositivos tan pronto como aparecen en (y son bloqueados por) el sistema.

Por esta razón, los administradores pueden ver en el registro de actividades de la consola de administración todos los dispositivos que han sido bloqueados y aprobarlos directamente si así lo desean.



Conclusión

Junto a SentinelOne Firewall Control, Device Control ofrece lo que algunos consideran las piezas que faltaban para poder sustituir completamente las soluciones antivirus tradicionales por productos de próxima generación. Al igual que otras funciones de la plataforma, estas se proporcionan en todas las plataformas a través del agente único de SentinelOne, y desde la misma consola de administración.

¿Te gusta este artículo? Síguenos en LinkedIn, Twitter, YouTube or Facebook para ver el contenido que publicamos.

Lee acerca de Ciberseguridad

- 10 maneras de proteger su Active Directory