DELL Technologies

Dell SafeData

La plataforma Absolute

VER Y ASEGURAR SUS DATOS Y DISPOSITIVOS

Única solución incorporada en el firmware para la inteligencia y la resiliencia del terminal

Ha implementado todas las estrategias correctas, pero las herramientas tradicionales de administración y seguridad de terminales tienen limitaciones y puntos ciegos. Estas son deshabilitadas por los usuarios finales o compiten por los recursos del dispositivo y sin querer acaban por no funcionar como estaba previsto.

Como resultado, es difícil ver, controlar y asegurar sus terminales. Esto da lugar a imprecisiones, ineficiencias operativas y brechas de seguridad, lo que pone en riesgo su capacidad para detectar problemas de manera confiable y responder con confianza a las amenazas. El resultado ineludible: auditorías inciertas, despilfarro de recursos, vulneraciones de datos y violaciones del cumplimiento de las normas.

Dell incorpora Persistence®, la tecnología patentada de Absolute, en el firmware antes de que los dispositivos salgan de fábrica. Persistence® se recupera de manera automática y reinstala el agente de Absolute en cada secuencia de arranque, incluso si se ha recreado la imagen del dispositivo o si se ha reemplazado el disco duro.

Una vez que Absolute se activa, proporciona la resiliencia que necesita a través de una conexión digital irrompible. De esta manera, siempre podrá ver y controlar sus dispositivos, y hacer frente a las brechas de seguridad, pase lo que pase.

Más información en DellEMC.com/endpointsecurity

ABSOLUTE®

INTELIGENCIA DE LOS RECURSOS

Visibilidad persistente de terminales: dentro o fuera de la red

Absolute garantiza que la conexión digital con cada dispositivo permanezca intacta, al proporcionar inteligencia confiable en todos sus terminales, con o sin conexión a la red corporativa.

Puede mantener su inventario de hardware y software siempre actualizado, optimizar la administración del ciclo de vida del dispositivo, acelerar las auditorías y las operaciones diarias, recibir alertas cuando los dispositivos están en movimiento, detectar recursos poco utilizados para evitar el despilfarro y utilizar esta información para tomar decisiones más rentables.

Criterios para tener éxito:

Integración y autorreparación: Única plataforma que funciona con tecnología de autorreparación integrada en el firmware de su dispositivo y que le permite ver y controlar toda su flota desde un solo panel, independientemente de la plataforma o la red.

Análisis de hardware: Controle cada terminal y cree un inventario completo y siempre actualizado de todos sus terminales, con cientos de puntos de datos por dispositivo.

Ubicación geográfica: Rastree con precisión la ubicación física de cualquier dispositivo de su interés, en cualquier momento, con o sin conexión a la red, incluidos los registros históricos.

Administración del ciclo de vida remota: Optimice el aprovisionamiento, la reasignación y el retiro de dispositivos remotos, incluida la capacidad de automatizar el mantenimiento regular, abordar los problemas de los dispositivos y realizar un borrado certificado al final del ciclo de vida.

Informes y alertas de software: Mantenga actualizado su inventario de software, encuentre la TI oculta y detecte si faltan aplicaciones necesarias.

Utilización del dispositivo: Comprenda cómo se utilizan los dispositivos e identifique los recursos inactivos para decidir cuáles deben reasignarse y cuáles deben desaparecer.

SEGURIDAD RESILIENTE DE TERMINALES

Evalúe su postura de seguridad y aplique los controles de seguridad

Desde una única consola basada en la nube, haga un informe sobre el cumplimiento de estándares o normativas y comparta esta información con cualquier parte interesada de su empresa. Detecte desviaciones y vulnerabilidades de la configuración, aplique automáticamente las aplicaciones de seguridad e implemente comandos y flujos de trabajo de manera remota para abordar las brechas de seguridad y automatizar esas tareas “imprescindibles”.

Absolute es la primera y única solución de visibilidad y control de terminales que persiste ante cualquier otro control de seguridad. Al extender la resiliencia de Absolute a otras aplicaciones, realiza la autorreparación de toda su pila de seguridad y el escalamiento de esta seguridad reforzada a toda su flota sin incorporar dispositivos. Cuando los terminales se alejan de la imagen deseada, Absolute los obliga a volver a alinearse para evitar vulneraciones de datos devastadoras y mantener la continuidad comercial.

Criterios para tener éxito:

Análisis comparativo de estándares: Informe sobre el cumplimiento de los estándares de seguridad cibernética o las normativas de privacidad de datos, marque los dispositivos que carecen de cifrado y antimalware y cierre la brecha de cumplimiento

Reforzamiento de la configuración: Descubra las debilidades y desviaciones de las configuraciones deseadas de terminales y ajústelas a escala

Más información en DellEMC.com/endpointsecurity

ABSOLUTE®

Continuidad de las aplicaciones: Detenga las interrupciones en la productividad del usuario y la continuidad comercial con las aplicaciones de autorreparación.

Garantía de protección de datos: Refuerce su protección de datos mediante controles de seguridad persistentes, como el cifrado, el antimalware, la VPN, la administración de terminales, entre otros, sin intervención humana

Detección y resolución de vulnerabilidades: Detecte los terminales que ejecutan versiones vulnerables del sistema operativo y envíe actualizaciones urgentes o implemente soluciones alternativas de protección con o sin conexión a la red corporativa

Flujos de trabajo automatizados: Implemente comandos y flujos de trabajo automatizados de manera remota para abordar las brechas de seguridad de manera rápida y a escala.

RESPUESTA SEGURA ANTE RIESGOS

Detecte incidentes de seguridad, responda y recupérese correctamente

Con Absolute, puede profundizar en sus dispositivos para descubrir información confidencial que está en riesgo e identificar dispositivos faltantes o comportamientos sospechosos. En cualquier etapa de un incidente (detección, vulnerabilidad, infracción o recuperación), Absolute le ofrece un conjunto de herramientas persistentes para responder y recuperarse de manera confiable.

Reciba alertas de forma instantánea sobre vulnerabilidades, exposiciones o una actividad nueva en dispositivos faltantes. Bloquéelos y borre los datos que contienen. Demuestre a los reguladores que los datos estuvieron siempre protegidos durante un incidente. Aproveche los registros históricos para evitar notificaciones de infracciones, obtener información sobre la causa raíz y evitar más incidentes similares.

Criterios para tener éxito:

Descubrimiento de datos de terminales: Localice la información confidencial, como la IP, la información personalmente identificable (PII), la información médica personal (PHI) o la información financiera personal (PFI), que esté en riesgo o sea vulnerable a la violación de las normativas de privacidad, como la Ley de Portabilidad y Responsabilidad de los Seguros Médicos (HIPAA), el Reglamento General de Protección de Datos (RGPD), los Servicios de Información sobre Justicia Penal (CJIS) o la Ley de Privacidad del Consumidor de California (CCPA).

Detección temprana de incidentes: Reciba alertas sobre controles deshabilitados y pruebas de manipulación de dispositivos, y sepa cuándo los dispositivos cargados de datos terminan en el lugar incorrecto.

Informes de dispositivos faltantes: Detecte qué dispositivos han estado offline durante cierto período de tiempo y márquelos como faltantes para recibir alertas tan pronto como se conecten a Internet.

Protección de datos de emergencia: Congele o borre de forma remota los dispositivos en peligro al obtener un certificado de saneamiento, evite la transferencia de datos y realice muchas otras acciones correctivas a escala.

Expertos en investigación: Aproveche el equipo de Absolute formado por investigadores con experiencia que trabajan en estrecha colaboración con las fuerzas de seguridad para procesar, recuperar un dispositivo robado o identificar al usuario mediante herramientas forenses.

Prueba de cumplimiento: Aproveche los registros históricos para validar que la protección de datos estuvo vigente durante los incidentes y obtenga información sobre la causa raíz para iterar sus políticas de seguridad.

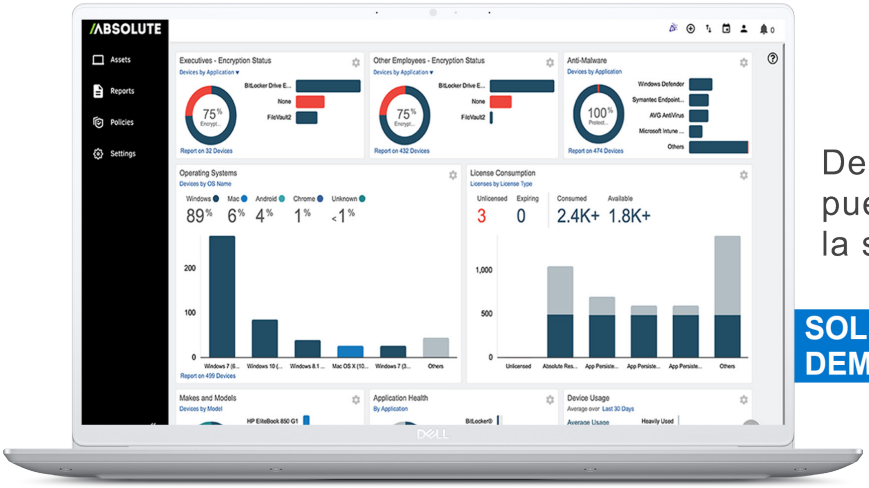
Más información en DellEMC.com/endpointsecurity

ABSOLUTE®

ELIMINE LAS DUDAS SOBRE LA SEGURIDAD DE SUS TERMINALES

Las empresas distribuidas de hoy en día necesitan la visibilidad y el control persistentes de terminales. Para adaptarse a un personal móvil y lograr la resiliencia de la empresa, los equipos de TI y seguridad dependen de la potente fusión de la inteligencia de recursos, la seguridad resiliente de los terminales y la respuesta segura ante los riesgos. Es decir, dependen de la plataforma Absolute.

Para obtener más información sobre cómo Absolute puede ayudarlo, visite el enlace siguiente: absolute.com/platform



Descubra cómo Absolute puede transformar la TI y la seguridad de su empresa.

SOLICITE UNA DEMOSTRACIÓN

Haga que sus aplicaciones y herramientas de seguridad sean indestructibles, solo con Absolute Resilience

Absolute Resilience contiene todas las características de visibilidad y control, como un flujo persistente de datos, inventarios automatizados y el poder de borrar datos o de bloquear los dispositivos de riesgo.

Persistencia de las aplicaciones

Brinde a sus aplicaciones cruciales la capacidad de repararse y reinstalarse a sí mismas después de intentar deshabilitarlas, eliminarlas o reconfigurarlas.

Descubrimiento de datos de terminales

Establezca políticas para escanear los dispositivos de su Windows y Mac o la información confidencial en riesgo, como la información personalmente identificable (PII), la información médica personal (PHI), la información financiera personal (PFI), el número de seguro social (SSN), el Reglamento General de Protección de Datos (RGPD) y la propiedad intelectual —con o sin conexión a la red— y, a continuación, calcule el costo de la exposición.

Alcance de Absolute

Evalúe y tome medidas correctivas en el 100 % de los dispositivos de Windows y Mac con una biblioteca de scripts prediseñados y personalizados.

Investigaciones

Permita que el equipo de Absolute, formado por exprofesionales de las autoridades policiales, rastree sus dispositivos perdidos o robados y luego asóciese con las agencias locales para recuperarlos.

Más información en DellEMC.com/endpointsecurity

ABSOLUTE®

	Absolute Visibility	Absolute Control	Absolute Resilience
Consola de Absolute	●	●	●
Realizar un seguimiento del hardware	●	●	●
Medir el uso del dispositivo	●	●	●
Monitorear el software instalado	●	●	●
Evaluar la postura de seguridad	●	●	●
Monitorear el estado de las aplicaciones cruciales	●	●	●
Integraciones de otros fabricantes	●	●	●
Detectar movimientos no autorizados en el dispositivo		●	●
Congelar dispositivos de forma remota		●	●
Eliminar datos de forma remota		●	●
Habilitar la protección del firmware		●	●
Hacer autorreparación de aplicaciones cruciales			●
Identificar información confidencial en los dispositivos			●
Consultar y corregir de forma remota dispositivos a escala			●
Investigar y recuperar dispositivos robados			●

Plataformas soportadas:

Póngase en contacto hoy mismo con un especialista en seguridad de terminales de Dell por correo electrónico en endpointsecurity@dell.com para consultar sobre los productos Dell SafeData que pueden ayudarlo a mejorar su postura de seguridad.

Más información en DellEMC.com/endpointsecurity

ABSOLUTE®

DELL Technologies