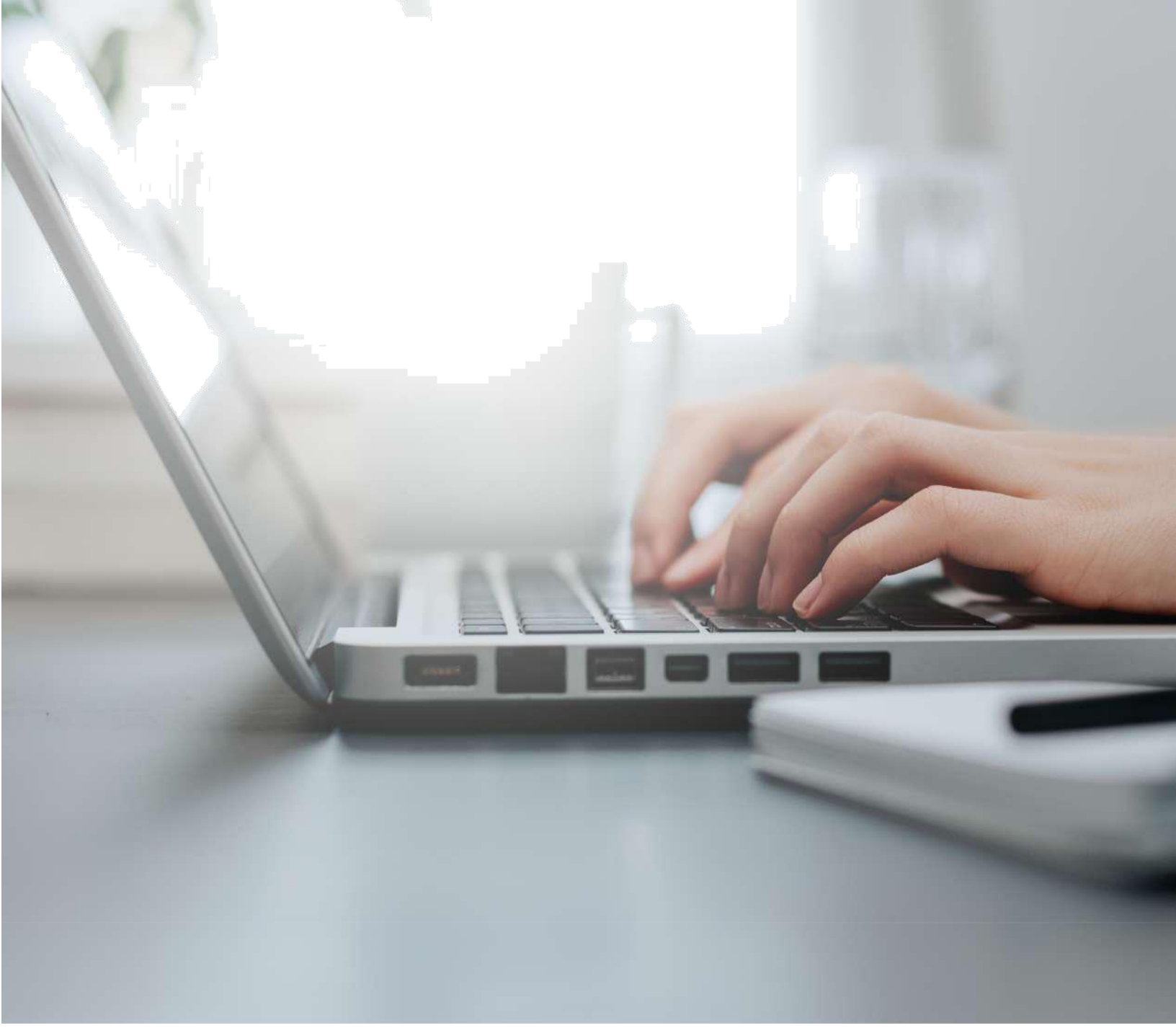


ABSOLUTE

Visibilidad y control persistente de cada endpoint

Lenovo

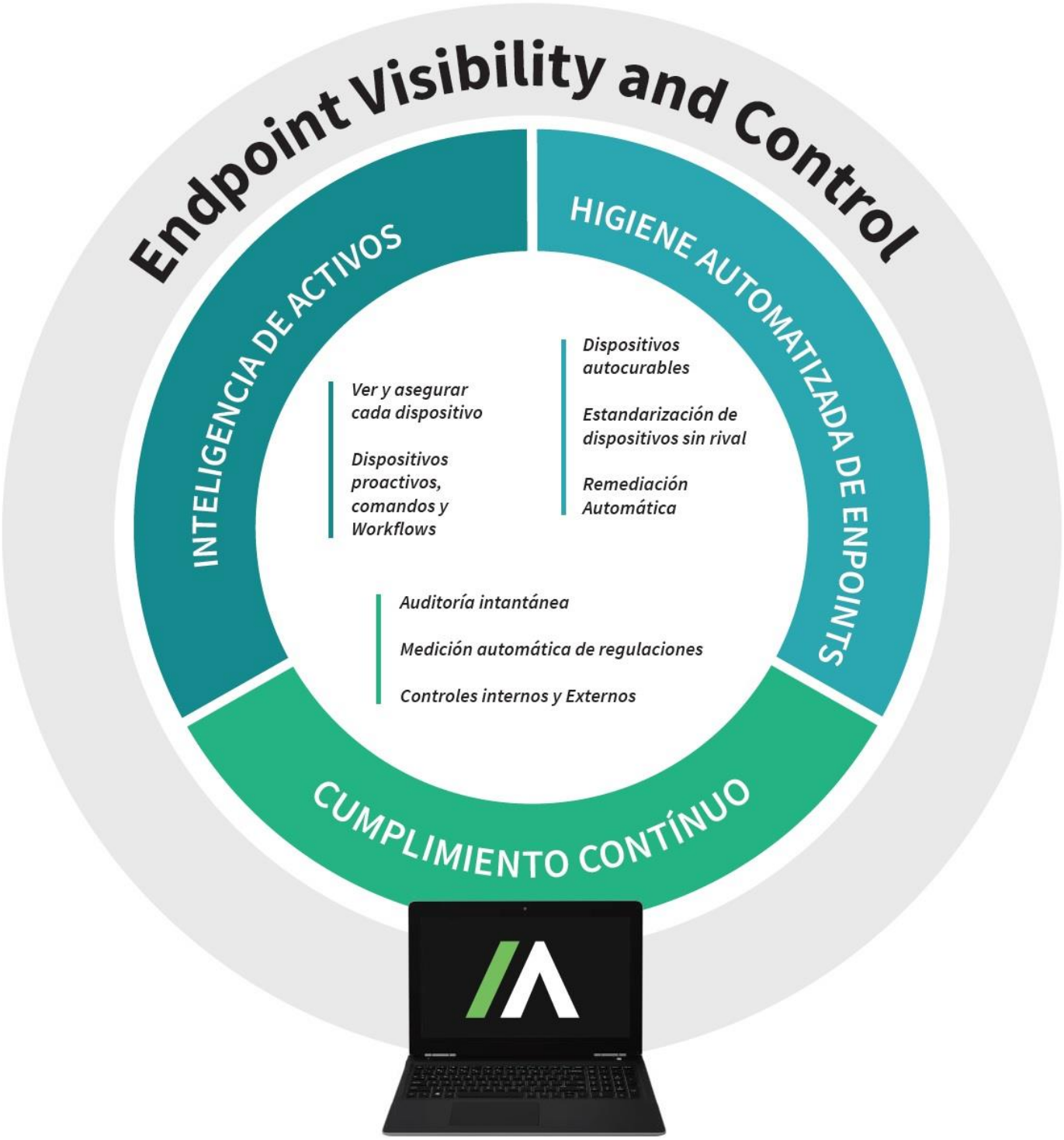
EL CONTEXTO DE LOS DISPOSITIVOS OSCUROS

En la actualidad los dispositivos se apagan, los datos se desvían sin previo aviso, los usuarios descuidan las políticas de seguridad, los controles se desactivan constantemente y las aplicaciones en la nube agregan otra capa de complejidad. Por ello, con el tiempo los equipos acumulan deudas de seguridad y tienden a comprometerse cuando estas exposiciones son explotadas.

En este sentido, la información de las empresas crece exponencialmente con el tiempo, la pérdida de dispositivos es tan peligrosa como el hackeo o malware, y las diferentes capas de integración generan una complejidad difícil de manejar.

Para contar con la visibilidad y control necesarios, es clave disponer de una tecnología persistente en los terminales. **Absolute proporciona resiliencia para cada dispositivo gracias a una tecnología de seguridad autocurable, que permite que en la administración de activos tecnológicos** siempre esté conectada para proteger a los equipos, sus datos, aplicaciones y usuarios, dentro y fuera de la red. Así, al cerrar la brecha entre la seguridad y las operaciones de informática, las organizaciones pueden actuar para **proteger cada dispositivo, remediar sus vulnerabilidades y garantizar el cumplimiento de estándares frente a amenazas internas y externas.** La tecnología Persistence patentada de Absolute ya está incorporada en el firmware de sus equipos de cómputo y cuenta con la confianza de más de 12,000 clientes en todo el mundo.

PARA ELIMINAR DISPOSITIVOS OSCUROS



Lenovo

ESTRATEGIAS EMPRESARIALES EN QUE INTERVIENE ABSOLUTE

Adopción de Mejores Prácticas de CiberSeguridad

Cumplir Regulaciones

Seguridad contra malas Acciones

Reducir los Costos de Seguridad

Asegurar la Fuerza de Trabajo Distribuido

Ambientes de Cero confianza

Lenovo

ABSOLUTE

PROYECTOS DE TI Y SEGURIDAD

DÓNDE IMPLEMENTAR

Limpieza del Endpoint

Ciclo de Vida de los Activos

Reducir el área de ataque

Proteger la data distribuida

Auditoría de Cumplimiento de Regulaciones

Modernizar Operaciones de TI

Lenovo

ABSOLUTE

Absolute Resilience

	ABSOLUTE RESILIENCE
	Excelente
RASTREAR HARDWARE	
Reportar y alertar sobre cientos de atributos de hardware	•
Monitorear reportes de arrendamiento de dispositivos	•
Seguimiento de las activaciones de nuevos dispositivos y el historial de conexiones	•
Aprovechar los reportes personalizados y predefinidos	•
Marcar los dispositivos perdidos y recibir alertas cuando se conecten a Internet	•
MONITOREAR SOFTWARE	
Evaluar el software instalado por dispositivo o población	•
Reportar y alertar sobre cambios de configuración de software o incumplimiento de políticas	•
Aprovechar los catálogos predefinidos o personalizados para identificar software y suites	•
EVALUAR LA POSTURA DE SEGURIDAD	
Reporte del estado de la encriptación	•
Reporte del estado del antimalware	•
COMPRENDER EL USO DEL DISPOSITIVO	
Evaluar uso del dispositivo analizando eventos de inicio de sesión/desbloqueo e interacción del dispositivo	•
Reportar sobre el uso diario promedio por dispositivo	•
Reportar sobre los sitios web visitados y el tiempo activo dedicado a cada uno[1]	•
MONITOREO DE UBICACIÓN DEL DISPOSITIVO	
Rastree la ubicación del dispositivo con 365 días de historial	•
Defina geocercas para detectar movimientos de dispositivos no autorizados	•
CONGELAR DISPOSITIVOS REMOTAMENTE	
Congele un dispositivo con un mensaje personalizado, programado o a demanda	•
Configurar un temporizador sin conexión para congelar dispositivos automáticamente	•
BORRAR DATOS DE DISPOSITIVOS	
Eliminar archivos de forma selectiva	•
Realice limpieza del dispositivo al final de su vida útil con certificado de cumplimiento	•
HABILITAR LA PROTECCIÓN DEL FIRMWARE	
Administre la contraseña del supervisor a escala[1]	•
CONSULTAR Y REMEDIAR DISPOSITIVOS INMEDIATAMENTE A ESCALA	
Ejecute más de 130 flujos de trabajo prediseñados desde la Librería de Reach	•
Ejecute scripts personalizados de Powershell o BASH en dispositivos	•
IDENTIFICAR ARCHIVOS SENSIBLES EN DISPOSITIVOS	
Descubra datos de PII, PHI, PFI, SSN, GDPR y propiedad intelectual dentro/fuera de la red	•
Realizar una evaluación de riesgos de datos con exposición de costos estimada	•
Identifique dispositivos con archivos confidenciales sincronizados con almacenamiento en la nube (Dropbox, iCloud, Box, OneDrive)	•

Lenovo

ABSOLUTE

	ABSOLUTE RESILIENCE
	Excelente
PERSISTA Y AUTO-REPARE APLICACIONES CRÍTICAS	
Cisco® AnyConnect VPN	•
Citrix Workspace™	•
CrowdStrike Falcon®	Solo Reporte
ESET® Endpoint Anti-Virus	•
F5® BIG-IP Edge Client	•
Ivanti® Endpoint Manager	•
McAfee® EPO	•
Microsoh® BitLocker	•
Microsoh® SCCM	•
Pulse Secure™	•
SentinelOne®	•
Tanium™	•
VMware® Carbon Black	•
VMware Workspace ONE™	•
WinMagic SecureDoc Encryption	•
Zihen Zenith	•
Otras aplicaciones	Complemento
INVESTIGAR Y RECUPERAR DISPOSITIVOS ROBADOS	
Recuperar dispositivos robados	•
Garantía de servicio para dispositivos no recuperados [2] (solo Educación)	•
CARACTERÍSTICAS DE LA PLATAFORMA ABSOLUTE	
Consola basada en la nube	•
Alertas predefinidas y personalizadas	•
Conector SIEM universal	•
Control de acceso basado en roles	•
Inicio de sesión único	•
Autenticación de 2 factores	•
QuickStart incorporado	•
Conector ITSM de Absolute para ServiceNow®	•

[1] Solo disponible para clientes de Educación.
[2] Solo disponible para **Dispositivos Lenovo elegibles**.
[3] Clientes de Educación de Norteamérica, Reino Unido y Australia únicamente. Términos y Condiciones aplican. Ver **Preguntas Frecuentes** para más detalles.

ABSOLUTE®

Lenovo