DELL Technologies

Dell SafeData

A plataforma absoluta

VEJA E PROTEJA SEUS DADOS E DISPOSITIVOS

A única solução incorporada ao firmware para inteligência e resiliência de endpoints

Você implementou todas as estratégias certas, mas as ferramentas tradicionais de segurança e gerenciamento de endpoints têm limitações e pontos cegos, são desativadas pelos usuários finais ou competem por recursos do dispositivo e, inadvertidamente, acabam não funcionando como esperado.

Como resultado, seus endpoints ficam difíceis de ver, controlar e proteger. Isso leva a imprecisões, ineficiência operacional e lacunas de segurança, comprometendo sua capacidade de detectar problemas e responder com segurança às ameaças. O resultado inevitável: auditorias incertas, desperdício de recursos, violação de dados e violação de conformidade.

A Dell incorpora a tecnologia Persistence® patenteada, da Absolute, no firmware antes que os dispositivos deixem a fábrica. A Persistence® corrige e reinstala automaticamente o agente Absolute em todas as sequências de boot, mesmo que o dispositivo tenha sido renomeado ou que o disco rígido tenha sido substituído.

Depois que o Absolute é ativado, ele fornece a resiliência de que você precisa por meio de um cordão digital inquebrável para que você possa sempre ver e controlar seus dispositivos e solucionar as lacunas de segurança, independentemente do que aconteça.

Saiba mais em DellEMC.com/endpointsecurity

ABSOLUTE®

INTELIGÊNCIA DE ATIVOS

Visibilidade persistente de endpoints: Ligue e desligue a rede

O Absolute garante que o cordão digital de cada dispositivo seu permaneça intacto, fornecendo a você inteligência confiável em todos os endpoints dentro ou fora da sua rede corporativa.

Você pode manter seu inventário de hardware e software sempre atualizado, simplificar o gerenciamento do ciclo de vida dos dispositivos, acelerar suas auditorias e operações diárias, receber alertas quando os dispositivos estão em movimento, detectar recursos pouco utilizados para evitar desperdícios e usar essa informação para tomar decisões mais econômicas.

Principais critérios de sucesso:

- **Incorporação e autocorreção:** A única plataforma habilitada pela tecnologia de autocorreção incorporada ao firmware do dispositivo permite que você veja e controle todo o seu parque em um painel de indicadores, independentemente da plataforma ou da rede
- **Lógica analítica de hardware:** Fique de olho em todos os endpoints e crie um inventário completo e sempre atualizado de todos os seus endpoints, com centenas de pontos de dados por dispositivo
- **Geolocalização:** Rastreie com precisão a localização física de qualquer dispositivo de seu interesse, a qualquer momento, dentro ou fora da rede, inclusive registros históricos
- **Gerenciamento do ciclo de vida útil remoto:** Simplifique o provisionamento remoto de dispositivos, a realocação e a desativação, inclusive a capacidade de automatizar a manutenção regular, solucionar problemas dos dispositivos e realizar uma limpeza certificada no fim da vida útil
- **Relatórios e alertas do software:** Mantenha seu inventário de software atualizado, erradique a TI invisível e detecte quando os aplicativos necessários estiverem ausentes
- **Utilização dos dispositivos:** Entenda como os dispositivos são usados e identifique ativos que não estão funcionando para decidir quais devem ser realocados e quais você precisa desativar

SEGURANÇA RESILIENTE DE ENDPOINTS

Avalie sua postura de segurança e imponha controles de segurança

Em um só console baseado em nuvem, relate a conformidade com padrões ou normas, compartilhando essas informações com qualquer parte interessada em sua organização. Detecte desvios e vulnerabilidades de configuração, aplique automaticamente aplicativos de segurança e implemente remotamente comandos e fluxos de trabalho para resolver as lacunas de segurança e automatizar essas tarefas obrigatórias.

O Absolute é a primeira e única solução de controle e visibilidade de endpoints a contrapor qualquer outro controle de segurança. Ao estender a resiliência do Absolute para outros aplicativos, você faz a autocorreção de toda a pilha de segurança, dimensionando essa segurança reforçada para todo o parque sem trazer dispositivos. Quando os endpoints se desviam da imagem desejada, o Absolute os força de volta ao alinhamento para evitar violações devastadoras de dados e manter a continuidade dos negócios.

Principais critérios de sucesso:

- **Análises comparativas de padrões:** Relatar a conformidade com padrões de segurança cibernética ou normas de privacidade de dados, sinalizar dispositivos sem criptografia ou antimalware e fechar a lacuna de conformidade
- **Fortalecimento da configuração:** Descubra pontos fracos e desvios das configurações de endpoint desejadas e ajuste-os em escala

Saiba mais em DellEMC.com/endpointsecurity

ABSOLUTE®

Continuidade de aplicativos: Interrompa as disrupções na produtividade do usuário e na continuidade dos negócios com aplicativos de autocorreção

Garantia de proteção dos dados: Fortaleça sua proteção de dados mantendo controles de segurança, como criptografia, antimalware, VPN, gerenciamento de endpoint e muito mais, sem intervenção humana

Detecção e resolução de vulnerabilidades: Identifique os endpoints que executam versões vulneráveis do sistema operacional e envie atualizações urgentes ou implemente soluções temporárias de proteção na rede corporativa

Fluxos de trabalho automatizados: Implemente remotamente comandos e fluxos de trabalho automatizados para solucionar lacunas de segurança com rapidez e em escala

RESPOSTA SEGURA CONTRA RISCOS

Detecte incidentes de segurança, responda e recupere com sucesso

Com o Absolute, você pode mergulhar em seus dispositivos para descobrir dados confidenciais em risco e identificar dispositivos ausentes ou comportamentos suspeitos. Em qualquer fase de um incidente — clones, vulnerabilidades, violação ou recuperação — o Absolute oferece um pacote de ferramentas persistentes para responder e se recuperar com segurança.

Receba alertas instantaneamente sobre vulnerabilidades, exposições ou novas atividades em dispositivos ausentes. Bloqueie-os e apague os dados contidos neles. Comprove aos reguladores que os dados sempre foram protegidos durante um incidente. Aproveite registros do histórico para evitar notificações de violação, saber mais sobre a causa raiz e evitar outros incidentes semelhantes.

Principais critérios de sucesso:

Descoberta de dados de endpoint: Localize dados confidenciais, como IP, PII, PHI ou PFI, que estejam em risco ou vulneráveis a violações de normas de privacidade, como HIPAA, RGPD, CJIS ou CCPA

Detecção antecipada de incidentes: Receba alertas sobre controles desativados e evidências de adulteração de dispositivos e saiba quando os dispositivos cheios de dados acabam no lugar errado

Relatórios de dispositivos ausentes: Detecte quais dispositivos estão off-line por determinado período e sinalize-os como ausentes para ser alertado assim que eles se conectarem à Internet

Proteção emergencial de dados: Congele ou limpe remotamente os dispositivos comprometidos obtendo um certificado de limpeza, impeça a transferência de dados e execute muitas outras ações corretivas em escala

Especialistas em investigação: Aproveite a equipe de investigadores experientes do Absolute que colaboram muito estreitamente com a imposição da lei para investigar, reaver um dispositivo roubado ou identificar o usuário por meio de ferramentas forenses

Prova de conformidade: Aproveite os registros do histórico para validar se a proteção de dados estava em vigor durante os incidentes e saber mais sobre a causa raiz para iterar suas políticas de segurança

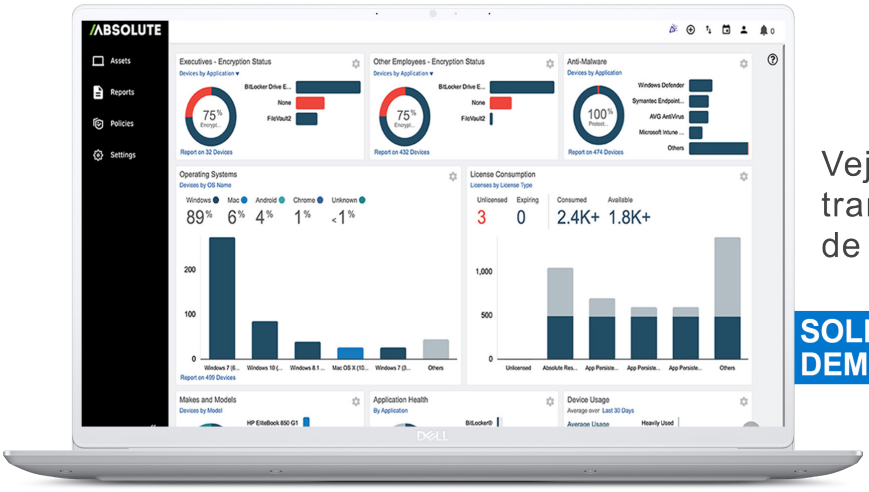
Saiba mais em DellEMC.com/endpointsecurity

ABSOLUTE®

NÃO TENHA DÚVIDAS DE QUE SEUS ENDPOINTS ESTÃO SEGUROS

As organizações distribuídas de hoje exigem visibilidade e controle persistentes de endpoints. Para acompanhar o ritmo de uma força de trabalho móvel e alcançar a resiliência organizacional, as equipes de TI e segurança contam com a poderosa fusão de inteligência de ativos, segurança resiliente de endpoint e resposta segura contra riscos. Eles contam com a plataforma Absolute.

Para saber mais sobre como o Absolute pode ajudar, acesse: absolute.com/platform



Veja como a Absolute pode transformar a TI e a segurança de sua organização

SOLICITAR UMA DEMONSTRAÇÃO

Torne seus aplicativos e ferramentas de segurança indestrutíveis — Somente com o Absolute Resilience

O Absolute Resilience contém todos os recursos de visibilidade e controle, inclusive um fluxo persistente de dados, inventários automatizados e a capacidade de limpar dados ou bloquear dispositivos de risco.

Persistência de aplicativos

Permita que seus aplicativos essenciais se recuperem e reinstalem após tentativas de desativá-los, removê-los ou reconfigurá-los.

Descoberta de dados de endpoint

Defina políticas para examinar seus dispositivos Windows e Mac ou dados confidenciais em risco, inclusive PII, PHI, PFI, SSN, RGPD e propriedade intelectual, seja na rede ou fora dela, e estimar o custo da exposição.

Alcance absoluto

Avalie e tome medidas corretivas em 100% dos seus dispositivos Windows e Mac com uma biblioteca de scripts pré-criados e personalizados.

Investigações

Deixe que a equipe do Absolute, formada por antigos profissionais de imposição da lei, rastreie seus dispositivos perdidos ou roubados e, em seguida, junte-se aos órgãos locais para recuperá-los.

Saiba mais em DellEMC.com/endpointsecurity

ABSOLUTE®

	Absolute Visibility	Absolute Control	Absolute Resilience
Absolute Console	●	●	●
Rastreamento de hardware	●	●	●
Avaliação do uso do dispositivo	●	●	●
Monitoramento do software instalado	●	●	●
Avaliação da postura de segurança	●	●	●
Monitoramento da integridade de aplicativos essenciais	●	●	●
Integração com terceiros	●	●	●
Detecção de movimento não autorizado do dispositivo		●	●
Congelamento remoto de dispositivos		●	●
Exclusão remota de dados		●	●
Ativação da proteção do firmware		●	●
Autocorreção de aplicativos essenciais			●
Identificação de informações confidenciais em dispositivos			●
Consulta e correção remotas de dispositivos em escala			●
Investigação e recuperação de dispositivos roubados			●

Plataformas compatíveis:

Entre hoje mesmo em contato com um especialista em segurança de endpoints da Dell pelo e-mail endpointsecurity@dell.com para falar dos produtos Dell SafeData que podem ajudar a melhorar sua postura de segurança

Saiba mais em DellEMC.com/endpointsecurity

ABSOLUTE®

DELL Technologies