Visibilidade sem concessões e remediação de vazamentos diretamente na fonte e em tempo real com a segurança de endpoint com autorrecuperação da Absolute

Aprimore sua estratégia de segurança com o Absolute® Data & Device Security, uma solução de segurança de endpoints adaptativa que elimina pontos cegos e resolve vazamentos em tempo real. A Absolute fornece uma conexão persistente aos seus endpoints e aos dados que eles contêm. Isso significa que você está sempre no controle, mesmo se um dispositivo não estiver conectado à sua rede corporativa ou for perdido ou roubado.

Adicione o Absolute Data & Device Security (antigo Computrace®) à sua linha de produtos para fortalecer sua linha de segurança, manter a conformidade e resolver problemas com velocidade incrível.

Veja e proteja dados e dispositivos, dentro e fora da sua rede

Você não pode proteger o que não vê. Com a Absolute, você obtém visibilidade de seus endpoints sem concessões com uma conexão bidirecional confiável a cada dispositivo. Essa conexão persistente permite obter os insights de que você precisa para avaliar riscos e aplicar medidas de segurança remotas. Esses recursos são fornecidos por meio de um console baseado em nuvem que não requer infraestrutura de TI adicional.

Os endpoints ativados com Absolute fazem check-in no centro de monitoramento baseado em nuvem periodicamente (o padrão é definido para a cada 24 horas) e fornecem informações essenciais sobre integridade e segurança.

Com a Absolute, você pode fazer auditoria e corrigir casos de não conformidade remotamente e resolver problemas de segurança rapidamente com conformidade específica de caso e detalhes de postura de segurança. Está preocupado com dispositivos off-line sem acesso à Internet? As políticas off-line possibilitam que você congele automaticamente dispositivos que não se conectaram à Internet dentro de um período de tempo definido.

Reaja imediatamente caso haja possíveis perdas ou vazamentos. Basta analisar o último estado conhecido de um sistema, determinar se há riscos e agir remotamente. Você pode escolher executar uma limpeza de disco rígido compatível com NIST, congelar um sistema e enviar uma mensagem para o usuário. Ou então pode obter a assistência de investigadores especialistas da Absolute para ajudar você com investigações forenses conduzidas remotamente e com a recuperação de um dispositivo perdido ou roubado (determinadas condições aplicáveis).

A vantagem da tecnologia Persistence

É possível obter conexão bidirecional com autorrecuperação, endpoints e os dados que eles contêm com a tecnologia patenteada Persistence® da Absolute. Essa tecnologia é incorporada ao núcleo dos PCs Dell e à maioria dos outros computadores, tablets e smartphones. Assim, ela pode ser ativada em dispositivos existentes.

Quando o agente de firmware no núcleo de um dispositivo é ativado com a instalação do cliente Absolute, a segurança de endpoint com autorrecuperação entra em vigor. A conexão bidirecional foi criada para resistir a violações de firmware e aplicativos, remoção do disco rígido e reinstalações de sistema operacional.

Prove a conformidade e o valor do investimento existente em TI

A Absolute não só permite que você veja e controle dispositivos conectados ou não à rede, mas também fortalece sua pilha de segurança existente. Por meio de geração de relatórios, alertas e integração com SIEM, a Absolute pode validar o status de outros aplicativos de segurança instalados e provar a conformidade dos dispositivos protegidos. Além disso, a Absolute inclui recursos de reparo de SCCM para possibilitar o gerenciamento consistente de clientes.

A tecnologia de autorrecuperação da Absolute pode ser estendida para que outros aplicativos de VPN, segurança crítica e gerenciamento de endpoint da sua empresa sejam resilientes.

Visibilidade e remediação com a Absolute

Proteja proativamente uma implantação inteira de dispositivos e sistemas operacionais com o console baseado em nuvem da Absolute. O centro de monitoramento global da Absolute é de nível empresarial e tem certificação ISO, e milhões de dispositivos contatam o Centro de monitoramento da Absolute todos os dias.

Relatórios e análises

Colete informações de todos os dispositivos, incluindo dados históricos. Identifique atividades e precursores de incidentes de segurança, como instalações de software e hardware fora de conformidade e alterações de endereço IP, local e usuário. Integre-se com SIEM ou use o painel de Security Vitals da Absolute.

Geotecnologia

Monitore localizações recentes e históricas de dispositivos no Google Maps™. Crie barreiras geográficas e alertas de locais fora dos limites com base em políticas corporativas e investigue dispositivos que entram em locais não autorizados.

Avaliação de riscos

Evite incidentes de segurança com a definição de políticas e alertas para eventos correlacionados com riscos de segurança elevados. Localize dispositivos fora de conformidade, receba alertas de instalações de aplicativos não autorizados e sinalize funcionários invasores. Valide e monitore o status de aplicativos críticos, inclusive o SCCM.

Resposta a riscos

Ative medidas de segurança adaptativas. Defina políticas off-line para garantir a proteção automática de dispositivos. Recupere ou exclua dados, congele um dispositivo, comunique status, produza registros de auditoria e use a exclusão de dados certificados para descomissionar dispositivos. Prove que os dados de endpoint e as redes corporativas não foram acessadas enquanto um dispositivo estava em risco.

Descoberta de dados de endpoint

Identifique e corrija dados fora de conformidade. Descubra dados confidenciais, incluindo informações pessoais de saúde e informações de identificação pessoal em dispositivos e analise os riscos associados. Descubra dados confidenciais sincronizados com aplicativos de armazenamento em nuvem.

Investigações em endpoints

Previna, identifique e elimine ameaças internas. Aproveite a equipe de investigações da Absolute para determinar a causa de um incidente de segurança de endpoint. Localize e, se necessário, recupere dispositivos perdidos ou roubados. Determine se é necessária uma notificação de vazamento de dados.

Éditions Absolute

Standard

Melhor para organizações que buscam controle de ativos confiável, dentro e fora da rede. Inclui geração de relatórios e análises de hardware e software, mapeamento e geração de relatórios da localização de dispositivos, histórico de chamadas e relatórios de controle de perdas.

Professional

Para organizações que desejam obter visibilidade sobre os riscos de segurança e a capacidade de controlar e remediar dispositivos e dados. Os relatórios e controles incluem uso de dispositivos, localização dos dispositivos (barreiras geográficas), integridade de software de segurança adjacentes, status de criptografia, compartilhamento em nuvem, autorreparação SCCM e painéis de segurança. Inclui um conector para enviar dados de segurança para as soluções SIEM.

Premium

Inclui todos os recursos do Professional, além da capacidade de descobrir dados confidenciais em endpoints e os serviços de especialistas na equipe de investigações da Absolute. Os serviços de investigação incluem investigações forenses, investigação de roubos de dispositivos e recuperação em conjunto com o reforço das leis locais (determinadas condições aplicáveis).

Requisitos técnicos

Agente DDS Absolute

- Windows 7, 8, 8.1 e 10 (32 e 64 bits)
- Mac OS X 10.6 ou posterior
- Android 4.4.2 ou posterior
- Conexão com a Internet

Console baseado em nuvem da Absolute

- Windows Internet Explorer
- Microsoft Edge (Windows 10)
- Mozilla Firefox (Windows e Mac)
- Google Chrome (Windows e Mac)
- Safari (Mac)

Saiba mais em Dell.com/DataSecurity