Como Migrar de Uma Abordagem Reativa para Ser Preventivo

5 ETAPAS IMPORTANTES A

CONSIDERAR EM SUA ESTRATÉGIA DE SEGURANÇA PARA ENDPOINTS

BeyondTrust

CONTEÚDO

*Etapa negligenciada

SEGURANÇA DE ENDPOINTS

Overview e Benefícios

Em 2019, 70% das violações de dados bem-sucedidas começaram nos endpoints.* E agora, com a mudança em grande escala para o trabalho remoto em virtude da COVID 19, a explosão do número de dispositivos de usuários finais, BYOD e endpoints trabalhando fora da rede, muitas empresas ainda estão tentando encontrar as melhores estratégias de segurança.

A segurança tradicional de endpoints inclui a proteção de dispositivos móveis, laptops, desktops, servidores, dispositivos IoT e POS, além de garantir que esses dispositivos atendam a certos requisitos antes de terem acesso aos recursos de rede. O objetivo da segurança dos endpoints é limitar a superfície de ataque, bloqueando a entrada não autorizada e protegendo a rede de ameaças maliciosas.

Ameaças a endpoints podem surgir na forma de ataques externos e internos, podendo ser maliciosas ou não intencionais. **Um endpoint comprometido permite que invasores executem outros ataques a sistemas para acessar dados e comprometer outros endpoints por meio de movimentação lateral.**

Uma vez que uma rede corporativa é uma conexão de vários endpoints, a integridade e a segurança deles devem ser priorizadas antes de se implementar outras soluções de segurança na camada de aplicações. Conforme evoluímos para o gerenciamento moderno de endpoints, o foco deve mudar para o acesso a dados e aplicações em nuvem que podem não estar conectados a um ambiente corporativo.

* IDC, " Do You Think Your Endpoint Security Strategy Is Up to Scratch?", Outubro de 2019

Vimos um aumento de

30.000%

em malwares diretamente atribuídos à COVID 19 —

*—Zscaler**

*www.zscaler.com/blogs/research/30000-percent-increase-covid-19-themed-attacks

A restrição de privilégios não é apenas uma questão de segurança. Com essa estratégia, seus computadores funcionam mais rápido, melhor e por mais tempo.

—SAMI LAIHO
— Microsoft MVP e Hacker Ético

Benefícios da Segurança de Endpoints

- **Segurança Aprimorada:** remoção de privilégios de administrador, restrição de privilégios, controle de acesso "Just-In-Time (JIT)" e uso de ferramentas baseadas em assinaturas, como antivírus, reduzem o risco de incidentes de segurança e violações de dados que visam os endpoints.

- **Desempenho Aprimorado de Endpoints:** a eliminação de privilégios desnecessários se traduz em menos configurações incorretas, incompatibilidades, incidentes de segurança e outros problemas que podem causar interrupções. Além disso, protege contra a instabilidade dos endpoints.

- **Conformidade e Auditorias Simplificadas:** um sistema de endpoints integrado, gerenciado e controlado garante melhor visibilidade em toda a empresa, auxiliando os processos de compliance.

- **Excelência Operacional:** as ferramentas de segurança certas permitem que a TI ofereça suporte a mais tipos de endpoints, e busque alternativas para mudanças inteligentes no ambiente, incluindo a implementação de novas tecnologias, garantindo a padronização para monitoramento e controle de mudanças.

OS DESAFIOS

da Segurança Tradicional de Endpoints

No mundo atual, as violações de dados são inevitáveis. Sem dúvida, o risco de elas acontecerem pode ser significativamente mitigado com medidas de detecção e prevenção, porém ele nunca é nulo. Contar com opções que evitem que os usuários executem ações que possam resultar em malwares, ransomwares e phishing são de extrema importância. **Considerando que 70% das violações começam nos endpoints, a segurança deles é fundamental para gerenciar de forma mais proativa as ameaças modernas.**

Ameaças cibernéticas, ambientes de endpoints cada vez mais complexos, falta de padronização e alinhamento nas tecnologias de segurança, e equipes de TI e de segurança cada vez maiores e diversas são apenas alguns dos muitos fatores que colocam em risco o universo dos endpoints de uma empresa e, portanto, toda a rede.

Ferramentas de segurança tradicionais de endpoints, como antivírus, evitam ataques e vetores de ataque conhecidos. Ainda assim, **60% dos ataques a endpoints não são detectados pelos antivírus.** E, embora as soluções de Endpoint Detection and Response (EDR) sejam importantes em uma estratégia de segurança, elas dependem de estatísticas e modelos que nem sempre reconhecem corretamente a diferença entre ameaças e comportamentos aceitáveis, levando a conclusões errôneas ou atrasos no tempo de resposta.

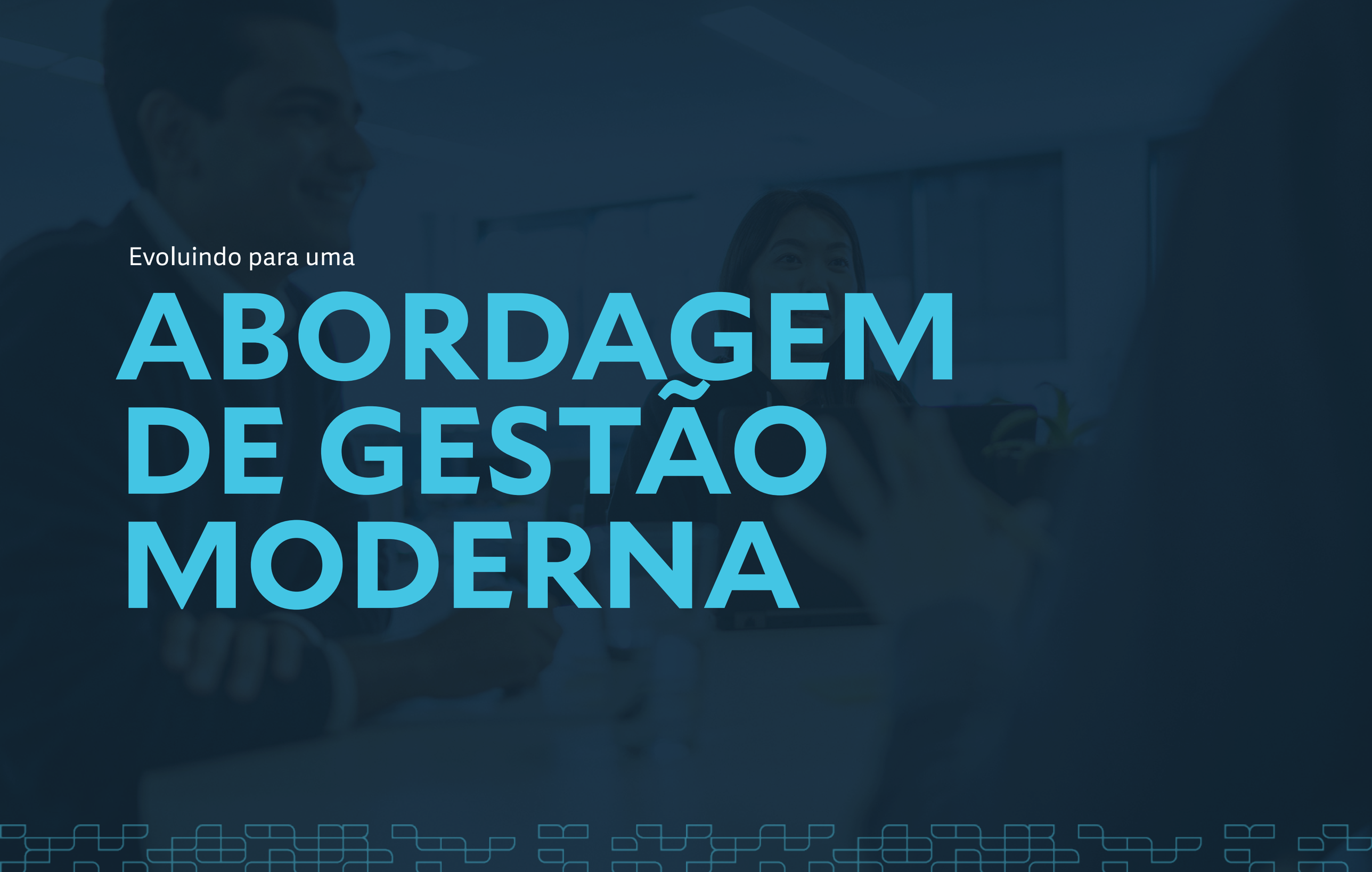
Por outro lado, as soluções de Gerenciamento de Privilégios nos Endpoints ou Endpoint Privilege Management (EPM) utilizam estratégias diferentes, evitando que os agentes de ameaças penetrem em um ambiente, removendo os privilégios necessários para comprometer um host. Isso atenua os riscos na camada de aplicações, controlando quem tem permissão de executar determinadas funções, e com quais privilégios. Esse modelo é crucial na prevenção de movimentos laterais que buscam dados confidenciais para serem comprometidos.

350.000

de novos malwares são detectados todos os dias*[1]

*www.av-test.org/en/statistics/malware/

*Como as organizações podem migrar para uma abordagem mais **preventiva** na segurança de endpoints?*



Evoluindo para uma

ABORDAGEM DE GESTÃO MODERNA

A Segurança de Endpoints é um Ecossistema, Não uma Solução Única

A segurança de endpoints evoluiu consideravelmente nas últimas décadas - de um software antivírus simples baseado em assinatura a uma tecnologia holística desenvolvida para proteger contra ameaças conhecidas ou desconhecidas aos endpoints. Hoje, a segurança de endpoints é necessária para prevenir, detectar, responder e mitigar ameaças externas e internas, e atender à crescente diversidade de dispositivos usados por colaboradores e terceiros, locais ou remotos.

Ela também precisa ser adaptável e alcançável para que possa se acomodar um ambiente de ameaças e TI em evolução. A segurança de endpoints não é apenas uma solução - é um ecossistema que deve ser preventivo, e não reativo.

Este guia descreve **5 etapas importantes** que devem ser consideradas em uma abordagem completa e preventiva para proteger todos os endpoints da sua empresa.

5 ETAPAS IMPORTANTES PARA SEGURANÇA COMPLETA NOS ENDPOINTS

Uma Abordagem Preventiva para Segurança de Endpoints

Antivírus

DETECTAR E PREVENIR

Malwares Conhecidos

Antivírus

*Ponemon Institute, "*The Third Annual Study on the State of Endpoint Security Risk*", Janeiro de 2020

Normalmente, o antivírus (AV) é o primeiro software de segurança de endpoint instalado, uma vez que ele protege contra ameaças comuns e conhecidas. **No entanto, o AV não é perfeito. Mais de 60% dos ataques não são detectados por esse tipo de software**, em virtude de ameaças *desconhecidas* ou técnicas evasivas que exploram aplicações "confiáveis". Portanto, com base nas melhores práticas de segurança, o antivírus deve ser visto apenas como um componente a mais em uma estratégia de segurança de endpoints mais completa.

Medidas muito mais eficazes, que tradicionalmente não são consideradas, devem ser usadas para complementar o AV e melhorar a eficácia da segurança dos endpoints. Isso inclui recursos como restrição de privilégios e controle de quais aplicações podem ser executadas. A combinação da estratégia de restrição de privilégios e controle de aplicações bloqueia ataques tradicionais de malwares e ransomwares. **Isso é imprescindível e nos leva à Etapa 2.**

Gerenciamento de Privilégios nos Endpoints

Etapa negligenciada

RESTRINGIR PRIVILÉGIOS

de Usuários Finais e Impedir Ataques de Dia Zero

Etapa negligenciada

Com a segurança de perímetro agora mais forte do que nunca, os dispositivos de usuários finais são alvos de ameaças. Em geral, os usuários têm acesso irrestrito a navegadores e e-mails, tornando mais fácil para um hacker "atrai-los" com técnicas de engenharia social. Se o usuário tiver privilégios de administrador local ao abrir um anexo ou link infectado, a "carga" pode ser executada com seus privilégios, dando ao hacker o controle da máquina, permitindo a ele instalar silenciosamente backdoors e reconfigurar (ou desabilitar) outros controles de segurança.

Muitos usuários finais ainda têm privilégios totais, credenciais de administrador ou até contas de admin temporárias/ compartilhadas para realizar seus trabalhos. Os usuários administradores também podem desinstalar ou desativar outras ferramentas de segurança em seus sistemas que, intencionalmente ou não, podem apresentar riscos adicionais.

Sem privilégios de administrador, o usuário não pode baixar ou executar softwares maliciosos que desencadeiam ataques de ransomwares ou malwares. Isso reduz drasticamente a superfície de ataque e limita os agentes de ameaças. Sem a presença de infecção, tais agentes não têm a capacidade de se mover lateralmente para comprometer dados confidenciais. **Segundo um estudo da BeyondTrust, a remoção dos privilégios de administrador poderia ter mitigado 77% das vulnerabilidades encontradas nos softwares da Microsoft em 2019. ***

Com o gerenciamento de privilégios, os usuários podem executar tarefas sem usar credenciais de root ou de administrador - concedendo os privilégios às aplicações. Esta abordagem de gestão "sem senha" permite que as empresas controlem privilégios, dando aos usuários direitos suficientes para realizar suas tarefas.

*BeyondTrust, "*Relatório de Vulnerabilidades Microsoft 2020*"

Remover os privilégios dos usuários finais é uma das maneiras mais eficazes de melhorar a segurança geral de sua empresa. Uma gestão de privilégios mais refinada pode atingir essa meta sem impactar a produtividade.

—DAN BLUM

Cybersecurity Strategist e Autor do Rational Cybersecurity for Business

03

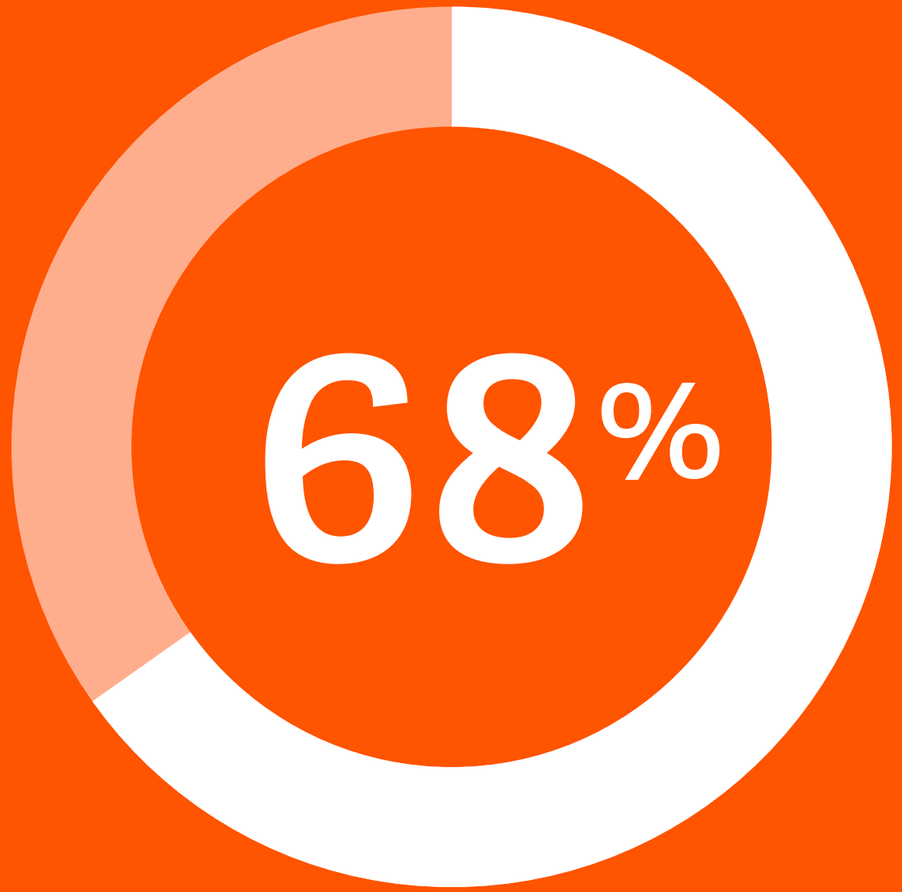
Gerenciamento de Privilégios nos Endpoints

Etapa negligenciada

USAR O CONTROLE PRAGMÁTICO DE APLICAÇÕES

e Bloquear Códigos Maliciosos

Gerenciamento de Privilégios nos Endpoints



das empresas foram atingidas por um ou mais ataques a endpoints em 2019*

* Ponemon Institute, *The Third Annual Study on the State of Endpoint Security Risk"*, Janeiro de 2020

Etapa negligenciada

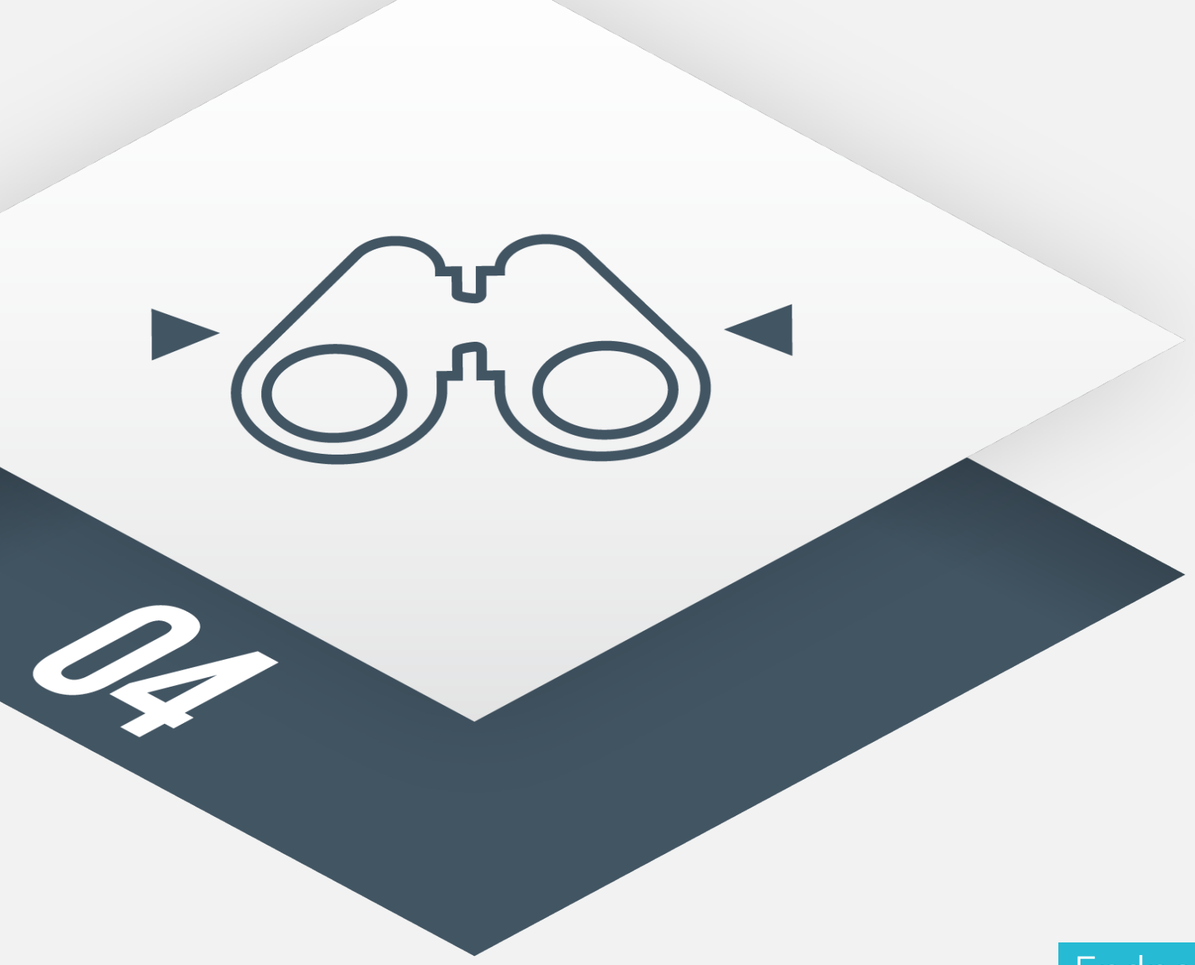
Nem todos os ataques a endpoints utilizam privilégios para comprometer uma máquina, e é aqui que o controle de aplicações entra em ação. Os controles de aplicações impedem que usuários e agentes de ameaças executem comandos inadequados em um endpoint.

Os hackers normalmente visam e exploram aplicações confiáveis para permitir acesso de longo prazo a um sistema. Ao comprometer as aplicações, o código malicioso pode ser injetado ou vinculado a elas sem ser detectado. Isso acontece muito com aplicações de e-mails e as baseadas na web.

O controle de aplicações decide quais delas um usuário pode executar, independente dos privilégios, e permite que as empresas definam aplicações boas e ruins com base nas necessidades do negócio. Ao usar o controle de aplicações, as equipes de segurança podem reforçar a segurança do sistema, tornando muito mais difícil para um atacante causar danos.

Tradicionalmente, o controle de aplicações é visto como uma tarefa difícil, tendo sido utilizado em ambientes mais estáticos. No entanto, ao implantá-lo em camadas sobre as soluções de gerenciamento de privilégios, a funcionalidade crítica do sistema operacional torna-se confiável por default (usuários sem privilégios não podem introduzir novos códigos aos arquivos de programas, Windows, System32 ou Drivers). Isso o torna uma abordagem pragmática que só precisa ser aplicada a diretórios e arquivos específicos, onde os agentes de ameaça normalmente "desistem".

Utilizar uma solução de gerenciamento de privilégios nos endpoints como segunda e terceira camadas fornece não apenas um modelo para restrição de privilégios, mas também para controle de aplicações. O resultado é uma redução drástica na superfície de risco dos endpoints. Além disso, o controle de aplicações é um requisito de conformidade.



Endpoint Detection & Response

MONITORAR CONTINUAMENTE

Atividades Maliciosas

Considerando que nem todos os riscos serão mitigados por antivírus ou por restrição de privilégios, tampouco por controle de aplicações, é muito importante contar com uma solução **EDR (Endpoint Detection and Response) para garantir a segurança dos endpoints.** Os EDR servem para ajudar as empresas a identificar e reagir a ameaças que contornam suas outras defesas. Eles são executados localmente em estações de trabalho ou servidores para monitorar processos, tarefas, aplicações, usuários conectados e, mais importante, para determinar se atividades maliciosas ou não autorizadas estão presentes no sistema. Eles são complementares ao EPM, uma vez que reconhecem e alertam sobre possíveis atividades invasoras em um sistema fora do escopo do EPM. Os alertas EDR podem incluir atividades relacionadas à rede, aplicações mal-intencionadas conhecidas, tentativas de usar programas integrados de forma mal-intencionada e outras atividades. E, se o EDR detectar um evento, a possibilidade de sucesso do ataque se torna menor, porque os privilégios e aplicações potencialmente maliciosos tiveram sua execução mitigada pelo EPM. O número de falsos positivos diminuirá, reduzindo o tempo necessário para revisar os dados do evento.

É importante lembrar que uma solução EDR por si só não oferece recursos completos de monitoramento. Profissionais de segurança bem treinados e processos sólidos são necessários para maximizar seu investimento em EDR e realmente melhorar a segurança de sua empresa. Sem a equipe certa e o compromisso de tempo, as soluções EDR podem acumular dados e alertas, o que pode, por sua vez, aumentar os custos de recursos.

O EDR sozinho não dá à sua empresa os recursos completos de monitoramento.

05

Outras Ferramentas de Segurança de Endpoints

BLOQUEAR USUÁRIOS FINAIS

Com Base em Casos de Uso

O Endpoint Privilege Management torna todas as outras ferramentas de segurança de endpoints mais eficazes, reduzindo o ruído e minimizando a superfície de ataque.

As estratégias de segurança de endpoint não são todas padronizadas. Depois que sua empresa implementou as **Etapas 1 a 4**, é fundamental revisar os casos de uso específicos e avaliar outras soluções com base em suas necessidades.

Alguns tipos de ferramentas de segurança de endpoints a serem consideradas incluem:

- Soluções de análise de endpoints, como avaliação de vulnerabilidades, monitoramento de logs e soluções SIEM, são aprimoradas pelo Gerenciamento de Privilégios, garantindo que apenas aplicações aprovadas e corrigidas sejam executadas.
- Soluções EDR, incluindo plataformas de proteção de endpoint (EPP) e aplicações de filtragem de e-mail e Web, também são complementadas por EPM evitando que uma parte significativa das atividades maliciosas ocorra, permitindo que essas ferramentas se concentrem em uma quantidade menor de atividades.

Além disso, existem muitos tipos diferentes de ferramentas de segurança que também podem ser consideradas pelas empresas na jornada de proteção de endpoints. Como exemplo, podemos citar soluções de prevenção de perda de dados, criptografia (endpoints e segurança de dados), endpoint hardening, gerenciamento de patch, configuração segura, acesso remoto e Web Proxy, entre outras. E, assim como as demais soluções, o EPM reduz drasticamente a superfície de ataque, removendo privilégios de administrador e evitando ameaças desde o dia zero.

BeyondTrust Endpoint Privilege Management

ABORDAGEM DE REDUÇAO PREVENTIVA DE RISCOS

BeyondTrust Privilege Management para Windows e MacOS

Uma solução de segurança de endpoints preventiva que remove privilégios de administrador, fornece aos usuários privilégios suficientes para realizar seus trabalhos com produtividade, e oferece redução de risco incomparável. Modelos de implantação disponíveis on premise ou na nuvem possibilitam uma rápida adoção e percepção de valor.

Principais Características

Restrição de Privilégios: Restrinja os privilégios de administrador para usuários, contas, aplicações e processos, liberando apenas os recursos necessários para a realização de atividades.

Gestão sem Senha: Execute funções sem a necessidade de credenciais privilegiadas com a abordagem de gestão Just-in-Time (JIT).

Controle de Aplicações: Obtenha controle total sobre o que os usuários podem instalar ou executar com tratamento de exceções automatizado e refinado.

Templates de Início Rápido: Modelos de estilo de trabalho flexíveis e prontos para uso permitem que você implemente políticas de privilégios mínimos em dias, não meses - trabalhando com eficácia para cada função, e em vários sistemas operacionais.

Proteção de Aplicações Confiáveis: Os templates pré-definidos impedem ataques envolvendo aplicações confiáveis, capturando scripts ruins e anexos de e-mail infectados - interrompendo imediatamente trojan horses, ataques sem arquivo e muito mais.

Power Rules: Utilize scripts PowerShell para automatizar fluxos de trabalho, criar comportamentos personalizados ou construir integrações com ITSM e outras ferramentas; ecossistemas integrados aprimoram ainda mais a segurança.

Auditoria e Relatórios: Forneça uma única trilha de auditoria de todas as atividades do usuário para simplificar a conformidade. Utilize dashboards e relatórios gráficos para fácil visualização e acesso.

Temos uma equipe de seis engenheiros que gerenciam todo o ambiente de desktop e móvel. Por isso, precisávamos de uma solução que permitisse que eles fizessem o trabalho da maneira rápida e eficiente. A solução Endpoint Privilege Management realmente permitiu que eles cumprissem com seus objetivos.

—RYAN POWELL
Gerente de Operações

Conclusão

As 5 etapas importantes para segurança de endpoints permitem uma abordagem completa e preventiva para proteger todos os endpoints em sua emprsa, sejam eles remotos ou não. A estratégia de restrição de privilégios e a permissão de controle pragmático de aplicações costumam ser esquecidos, mas são cruciais para garantir a segurança completa dos endpoints.

A solução BeyondTrust Endpoint Privilege Management reduz significativamente a superfície de ataque e as brechas para violação, removendo privilégios de administrador e adotando uma abordagem “sem senha”. Por meio de white lists inteligentes e regras personalizadas, os usuários finais podem realizar seu trabalho com produtividade, sem impactar o ecossistema de segurança já existente.

As soluções BeyondTrust ajudam na adoção de uma abordagem preventiva em camadas, garantindo uma experiência transparente para o usuário, fornecendo a ele o acesso certo, no momento certo.

Recursos Adicionais

- BeyondTrust Glossary: Endpoint Security
- Guia: Gerenciamento de Privilégios nos Endpoints
- Relatório de Vulnerabilidades Microsoft 2020
- Guia rápido: para Habilitar e Protejer sua Força de Trabalho Remota
- DEMO ON DEMAND: Privilege Management para Windows e MacOS
- Quadrante Mágico 2020 do Gartner para Gestão de Acessos Privilegiados

BeyondTrust

Sobre a BeyondTrust

A BeyondTrust é líder mundial em Gerenciamento de Acessos Privilegiados (PAM), capacitando empresas a proteger e gerenciar todo o seu universo de privilégios. Nossos produtos e plataformas integrados oferecem a solução PAM mais avançada do setor, permitindo que as organizações reduzam rapidamente sua superfície de ataque em ambientes tradicionais, em nuvem e híbridos.

O conceito de Gerenciamento Universal de Privilégios da BeyondTrust protege privilégios, senhas, endpoints e acessos, dando às equipes de TI e segurança a visibilidade e o controle de que precisam para reduzir o risco, alcançar a conformidade e aumentar o desempenho operacional. Nossos produtos permitem o nível certo de privilégios apenas pelo tempo necessário, criando uma experiência transparente para os usuários e aumentando sua produtividade.

Com uma herança de inovação e um forte compromisso com os clientes, as soluções BeyondTrust são fáceis de implantar, gerenciar e escalar conforme os negócios evoluem. Mais de 20.000 clientes confiam na BeyondTrust, incluindo 70% das empresas Fortune 500 e uma rede global de parceiros. Saiba mais em www.beyondtrust.com/pt.

V2020_09_ENG