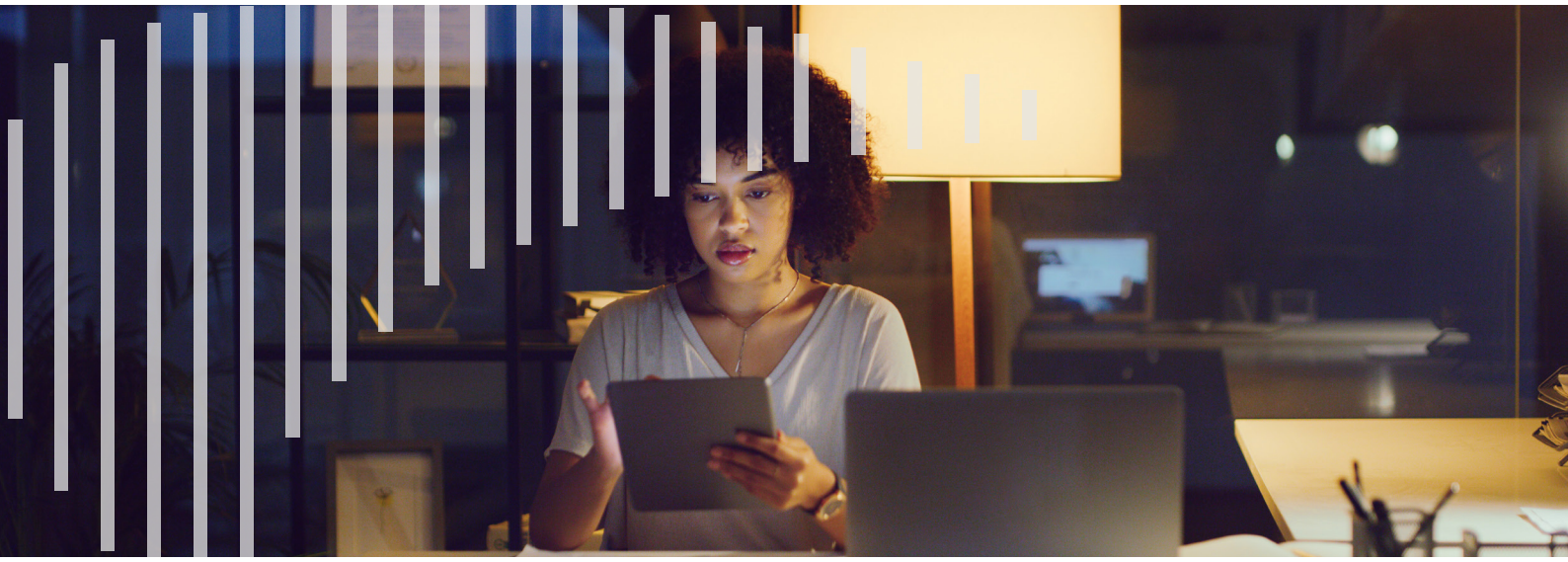

RESUMO EXECUTIVO

O que os administradores precisam observar na hora de comprar uma solução de segurança de endpoints

Uma nova perspectiva sobre os desafios na proteção de endpoints.

Resumo

Administradores enfrentam os desafios dos produtos de segurança de endpoints. Este resumo examina vários desses desafios persistentes, incluindo:

- Segurança, manutenção e execução
- Ameaças criptografadas e avançadas
- Gerenciamento de alertas e correção
- Elaboração e manutenção de políticas
- Visibilidade no estado de tenants
- Vulnerabilidades sem patches de segurança

O gerenciamento e a segurança de endpoints são fundamentais no cenário atual de crimes cibernéticos. Usuários finais utilizam continuamente a rede com seus dispositivos de endpoints. Ao mesmo tempo, esses endpoints são o campo de batalha no cenário atual de ameaças. Constantemente ameaças criptografadas chegam desapercebidas aos endpoints, ransomware está aumentando e o roubo de credenciais persiste silenciosamente. A crescente ameaça de ransomware e outros ataques maliciosos baseados em malware demonstraram que as soluções de proteção de clientes não podem ser avaliadas com base somente no cumprimento dos regulamentos da conformidade dos endpoints.

Estes desafios se agravam quando se tem que gerenciar multitenants, seja em uma única organização ou para vários clientes. Isto exige políticas e configurações diferentes baseadas em grupo de usuários, dispositivos e localização.

Os desafios na proteção de endpoints

Produtos de segurança de endpoints já estão no mercado há anos, mas os administradores ainda enfrentam desafios, tais como:

- Atualizar os produtos de segurança
- Aplicar as políticas e a conformidade na rede
- Obter relatórios e gerenciar o acesso
- Detectar ameaças que vêm de canais criptografados
- Compreensão dos alertas e medidads de correção
- Gerenciar licenças
- Bloquear as ameaças avançadas, tais como ransomware
- Onde estão as vulnerabilidades críticas?
- Conhecer o estado dos tenants e manter as políticas globais.

Atualizar os produtos de segurança

Os administradores têm que garantir que os endpoints estejam executando a versão correta dos componentes do software de segurança de acordo com a política de conformidade.

Para impedir ataques emergentes, os administradores da segurança da rede têm que gerenciar seus endpoints e avaliar constantemente a postura de segurança e gerar regularmente relatórios.

Alguns administradores precisam interromper o tráfego leste-oeste que circula entre seus centros de dados, que é muitas vezes o responsável pela maior parte do tráfego em seus switches. Eles têm que ter a opção de colocar um dispositivo em quarentena localmente caso ele não

esteja cumprindo os regulamentos da conformidade ou esteja infectado. Nestes casos, o firewall deve bloquear o acesso deste dispositivo à internet e à LAN, restringindo os caminhos da rede aos mesmos locais de quarentena que o firewall está usando.

Além disso, para garantir a integridade de dados, os administradores de segurança têm que garantir que todos os dados que trafegam entre o console único do cliente e o console de gerenciamento central não possam ser manipulados enquanto estão transitando.

Aplicar as políticas e a conformidade na rede

Se os endpoints não estão cumprindo as políticas, os administradores têm que impedir o dispositivo de endpoint de usar serviços UTM para trafegar pelo firewall. Usuários finais também têm uma importante função na segurança de endpoints. Eles trabalham em notebooks corporativos e em outros endpoints. Usuários precisam saber imediatamente se algum software ou comportamento malicioso foi detectado, para poder agir ou, se necessário, apresentar um ticket .

Se os funcionários trabalham longe do escritório, pode-se aplicar a política de uso da rede de sua organização com um filtro de rede ou de conteúdo incorporado à sua solução de segurança. Também é vital bloquear o acesso a sites maliciosos conhecidos e alguns também consideram importante bloquear os sites improdutivos ou com conteúdo adulto. Se os usuários podem acessar vídeos através de servidores locais via VPN, também se deve considerar estrangular a largura de banda para sites com uso intensivo de dados.

Obter relatórios e gerenciar o acesso

Em alguns casos, os administradores podem gerenciar vários firewalls, mas seus usuários estão configurados em um único grupo. Eles têm que obter uma autenticação única (SSO) de todos administradores de firewall ou de consoles de gerenciamento de segurança para gerenciar as políticas do cliente. Ao mesmo tempo, os regulamentos de conformidade impõem frequentemente que todas as funções de administrador sigam o princípio do privilégio mínimo. Assim o gerenciamento unificado de clientes deve ter um controle de acesso baseado em funções suficiente para acesso privilegiado. Por exemplo, alguém pode estar limitado a duas funções; uma com acesso para leitura e gravação e outra somente com acesso à leitura.

Ameaças que vêm de canais criptografados

Cada vez mais aplicações de rede são protegidas por canais criptografados, como HTTPS, e com malware também recorrendo à criptografia para burlar a inspeção baseada em rede, a inspeção profunda de tráfico SSL/TLS (DPI/SSL) se tornou indispensável. No entanto, isso não é facilmente aplicável sem a implementação em massa de certificados SSL/TLS confiáveis em todos os endpoints, visando evitar desafios de experiência do usuário e de segurança. Esse passo requer um mecanismo subjacente para distribuir e gerenciar certificados e a maneira como os navegadores determinam sua confiança.

Compreesnsão dos alertas e medidads de correção

Geralmente os usuários finais estão menos cientes dos riscos de segurança do que os profissionais de segurança. Assim seria importante que sua plataforma de proteção de endpoints os alerte sobre a mudança do perfil de risco quando viajam com seus notebooks entre locais diferentes e os oriente sobre como manter a segurança.

Para corrigir rapidamente qualquer problema quanto à política de conformidade corporativa, pode ser benéfico tanto para os usuários finais como para a TI ter acesso a informações de autoatendimento. Se o dispositivo do usuário não cumpre as políticas e ele está em quarentena, usuários precisam de orientação sobre quais as ações necessárias para estar em conformidade novamente.

Gerenciamento de licenças

Administradores devem assegurar que qualquer software de segurança de endpoint adquirido seja atualizado automaticamente em sua interface de gerenciamento, de modo que possam manter seus endpoints licenciados corretamente. Por exemplo, todas as informações sobre licença relacionadas a um cliente devem ser monitoradas e armazenadas centralmente. No caso de uma nova compra de licença, um sinal de alerta deve ser enviado ao gerenciamento centralizado do cliente unificado para alertar e iniciar o processo de direitos do software.

Alguns administradores devem periodicamente executar relatórios de conformidade de todas as licenças terceirizadas implementadas para pagar seus parceiros.

Bloquear ameaças avançadas, tais como ransomware

Muitas vezes as abordagens tradicionais de segurança de endpoints podem deixar lacunas no cumprimento de exigências administrativas. A abordagem baseada em assinaturas de longa data das tecnologias antivírus tradicionais não conseguiu acompanhar o ritmo de desenvolvimento de novos malware e do refinamento das técnicas de evasão. Isso faz com que seja necessária uma abordagem diferente para a proteção de endpoints. Ela não deve somente disponibilizar mecanismos avançados de detecção de ameaças, mas também oferecer suporte a uma estratégia de defesa em camadas nos endpoints, incluindo a integração com um ambiente de sandboxing.

Uma das principais limitações das soluções pontuais atuais (conhecidas como clientes AV aplicados) é que o desenvolvimento é específico para um terceiro determinado e foi incorporado às ofertas desse terceiro. Os administradores precisam de um modelo mais aberto que permita implementar de forma relativamente rápida módulos de segurança adicionais se o negócio ou indústria o exigirem.

Onde estão as vulnerabilidades críticas?

Com o grande aumento em aplicações empresariais, a ameaça de vulnerabilidades das aplicações tem crescido exponencialmente. Somente em 2019, CVSS críticas de 9,0+ foram atribuídas a vulnerabilidades, dando dores de cabeça aos administradores de TI e resultando em falhas na segurança. As organizações precisam de um modo que identifique o número e a classificação das vulnerabilidades, de modo que possam criar patches ou desinstalar aplicações de risco.

Conhecer o estado dos tenants e manter as políticas globais.

As grandes organizações têm que gerenciar um grande número de endpoints, segurança de endpoints por várias regiões, grupos de usuários ou por tipos de dispositivos; ou ambos. O sucesso desta tarefa está baseada na criação rápida de novos tenants e se eles têm um dashboard global que lhes dê permita ver o estado dos tenants. Nessas situações os administradores precisam reformular rapidamente uma política global que se aplique a tenants e grupos. MSSPs and MSPs precisam também ter a liberdade de elaborar políticas para tenants que não sejam afetadas por mudanças na política global. A função de gestão deveria oferecer-lhes estatísticas de alto nível sobre infecções e vulnerabilidades sem a necessidade de examinar detalhadamente cada um dos clientes.

Conclusão

Como os endpoints são cada vez mais usados como vetores de ataques cibernéticos, os profissionais de segurança têm que tomar medidas para proteger esses dispositivos. Além disso, com o crescimento do teletrabalho, há uma grande necessidade de fornecer proteção constante para todos os clientes em todos os lugares.

Os administradores de segurança têm que avaliar as soluções de endpoints tendo em mente as exigências reais.

Saiba mais. Leia nosso resumo com a solução, "Como adequar a segurança de endpoints à sua organização," ou visite www.sonicwall.com/capture-client.

Sobre SonicWall

A SonicWall fornece o modelo Boundless Cybersecurity na era da computação hiper distribuída e uma realidade de trabalho onde todos estão remotos, móveis e inseguros. Ao revelar ameaças ainda desconhecidas, fornecendo visibilidade em tempo real e, possibilitando a contínua inovação da economia, a SonicWall resolve as falhas na segurança cibernética para corporações, governos e SMBs em nível mundial. Para obter mais informações, visite www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Faça referência ao nosso website para informação adicional.
www.sonicwall.com

ExecBrief-WhatAdminNeed-A4-VG-3575