SONICWALL

O QUE OS ADMINISTRADORES PRECISAM OBSERVAR QUANDO COMPRAM UMA SOLUÇÃO DE SEGURANÇA DE ENDPOINT

Uma nova perspectiva sobre os desafios da proteção de endpoint

Resumo

Os administradores enfrentam desafios na gestão de produtos de segurança de endpoint. Este resumo examina vários desses desafios persistentes, incluindo:

- Manutenção e aplicação de segurança
- Ameaças criptografadas e avançadas
- Gerenciamento de alertas e correção
- Criação e manutenção de políticas
- Visibilidade da integridade dos usuários
- Vulnerabilidades sem correção

Introdução

O gerenciamento e a segurança de endpoints são fundamentais no ambiente cada vez mais evoluído do cibercrime atual. Os usuários finais utilizam a rede constantemente com seus dispositivos de endpoint. Ao mesmo tempo, esses endpoints são o campo de batalha do cenário de ameaças atual. As ameaças criptografadas estão atingindo cada vez mais os endpoints sem verificação, o volume de ransomware está aumentando e o roubo de credenciais persiste silenciosamente. Porém, a ameaça cada vez maior de ransomware e outros ataques mal-intencionados baseados em malware provou que as soluções de proteção do cliente não podem ser avaliadas com base apenas na conformidade do endpoint.

Além disso, esses desafios só se agravam quando é necessário gerenciar vários usuários, seja em uma única organização, seja para vários clientes. Isso geralmente exige políticas e configurações diferentes com base no grupo de usuários, no dispositivo e na localização.

Os desafios da proteção de endpoint

Os produtos de segurança de endpoint existem no mercado há anos, mas os administradores têm problemas com:

- Atualização dos produtos de segurança
- Aplicação de políticas e conformidade
- Obtenção de relatórios
- Ameaças provenientes de canais criptografados
- Compreensão dos alertas e das medidas de correção
- Gerenciamento de licenças
- Bloqueio de ameaças avançadas, como ransomware
- Criação e atualização de políticas ao redor do mundo
- Compreensão da integridade de cada usuário
- Desconhecimento da localização de vulnerabilidades críticas

Garantir atualização dos produtos de segurança

Os administradores precisam garantir que os endpoints gerenciados estejam executando a versão correta dos componentes do software de segurança instalados conforme exigido pela política de conformidade.

Para impedir ataques emergentes, os administradores de segurança de rede precisam de endpoints gerenciados para avaliar a postura de segurança e relatar seu status constantemente.

Alguns administradores precisam interromper o tráfego entre servidores em seus data centers, que geralmente pode ser responsável pela maior parte do tráfego em seus switches. Eles precisam da opção de colocar um dispositivo em quarentena localmente caso ele não esteja em conformidade ou esteja infectado. Nesses casos, o firewall deve bloquear o acesso à Internet e o acesso desse dispositivo à LAN, restringindo assim os caminhos de rede aos mesmos locais de quarentena que o firewall está aplicando.

Todos os administradores de grandes e pequenas empresas precisam de visibilidade das vulnerabilidades de aplicações presentes em endpoints protegidos. O conhecimento da escala de uma vulnerabilidade crítica ajudará a organização a desenvolver um plano para corrigir essas aplicações para evitar uma violação com mais eficiência.

Além disso, os administradores de segurança precisam garantir que todos os dados entre o cliente unificado e o console de gerenciamento centralizado estejam protegidos contra violação durante o trânsito, a fim de garantir a integridade dos dados.

Aplicação de políticas e conformidade

Se os endpoints estão em um estado contrário à política, os administradores precisam ser capazes de impedir que o dispositivo de endpoint use serviços de UTM para passar o tráfego pelo firewall. Os usuários finais também têm um papel importante na segurança do endpoint. Eles trabalham em laptops corporativos e outros endpoints. Os usuários precisam saber imediatamente se algum software ou comportamento mal-intencionado foi detectado, para poderem tomar medidas ou abrir um chamado, se necessário.

Os administradores de empresas com vários usuários e MSSPs precisam ser capazes de ativar políticas para novos usuários e corrigir as políticas atuais para quando uma nova ameaça for detectada ou quando uma nova propriedade da Web estiver consumindo largura de banda ou afetando a produtividade, por exemplo.

Obtenção de relatórios

Em alguns casos, os administradores podem gerenciar vários firewalls, mas seus usuários são configurados em um único conjunto. Eles precisam ser capazes de obter single sign-on (SSO) de todos os administradores de firewall ou consoles de gerenciamento de segurança para gerenciar as políticas do cliente. Ao mesmo tempo, as normas de conformidade geralmente determinam que todas as funções de administrador sigam o princípio de privilégio mínimo, de modo que o gerenciamento unificado de clientes deve ter controle de acesso baseado em funções suficiente para acesso privilegiado. Por exemplo, ele pode ser limitado a duas funções, uma com acesso de leitura/gravação e outra com acesso apenas para leitura.

Eles também precisam ter uma visão macro da integridade de seus usuários em uma visão global. Eles precisam ver um resumo de cada usuário. Isso pode ser avaliado pelo número de infecções, pelas vulnerabilidades presentes, pela versão da segurança de endpoint instalada ou pelos dispositivos que estão on-line e em operação. Eles também podem precisar ver o que e quem está gerando mais alertas de conteúdo da Web.

Ameaças provenientes de Canais Criptografados

Com mais aplicações da Web sendo protegidas por canais criptografados como HTTPS, e o malware também recorrendo à criptografia para contornar a inspeção baseada na rede, tornou-se indispensável habilitar a Deep Packet Inspection de tráfego SSL/TLS (DPI-SSL). Entretanto, isso não é facilmente aplicado sem a implantação em massa de certificados SSL/TLS de confiança para todos os endpoints, com o objetivo de evitar desafios de experiência do usuário e de segurança. Isso exige um mecanismo subjacente para distribuir e gerenciar certificados e a maneira como os navegadores determinam sua confiança.

Compreensão dos alertas e das medidas de correção

Os usuários finais normalmente estão menos cientes do risco de segurança do que os profissionais de segurança e, portanto, precisam que a plataforma de proteção de endpoint os alerte sobre a mudança do perfil de risco, enquanto se deslocam com seus laptops entre diferentes locais, e os oriente sobre como manter a segurança.

Por exemplo, um alerta pode ser gerado de um cliente unificado ou software de terceiros ou redirecionar para uma fonte externa, como uma página da Web.

Para corrigir rapidamente todos os problemas de conformidade com as políticas da empresa, pode ser benéfico para os usuários finais e para a TI que os usuários finais tenham acesso a informações de autoatendimento. Se o dispositivo de um usuário não está de

acordo com as políticas e esse usuário é colocado em quarentena, os usuários também precisam de orientação sobre as medidas necessárias para estar em conformidade novamente.

Gerenciamento de licenças

Os administradores precisam garantir que todo software de segurança de endpoint adquirido seja atualizado automaticamente para sua interface de gerenciamento, para que possam manter a licença correta dos endpoints. Por exemplo, todas as informações de licença relacionadas a um cliente devem ser monitoradas e armazenadas centralmente. No caso de uma nova compra de licença, um sinal deve ser enviado ao gerenciamento centralizado do cliente unificado para alertar e iniciar o direito do software.

Em uma programação periódica, alguns administradores precisam executar relatórios de conformidade em todas as licenças de terceiros implantadas para pagar seus parceiros.

Bloqueio de ameaças avançadas, como ransomware

Às vezes, as abordagens tradicionais podem deixar lacunas no cumprimento dos requisitos administrativos. A abordagem baseada em assinaturas de longa data das tecnologias antivírus tradicionais não conseguiu acompanhar o ritmo de desenvolvimento de novas formas de malware e suas técnicas de evasão – impondo a necessidade de uma abordagem diferente para a proteção do cliente. Ela não deve apenas 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 o acréscimo relativamente rápido de módulos de segurança adicionais quando a empresa ou o setor exige.

Conclusão

Em decorrência do aumento do uso de endpoints como vetor de ciberataques, os profissionais de segurança precisam tomar medidas para proteger os dispositivos de endpoint. Além disso, a proliferação do teletrabalho, da mobilidade e do BYOD impõe a necessidade de oferecer proteção constante para todos os clientes, em todo lugar.

Os administradores de segurança precisam avaliar as soluções de endpoint tendo em mente os requisitos do mundo real.

Saiba mais. Leia o resumo da solução, "Fitting endpoint security to your organization" (Como adequar a segurança de endpoint a sua organização), ou visite www.sonicwall.com/capture-client.

© 2020 SonicWall Inc. TODOS OS DIREITOS RESERVADOS.

A SonicWall é uma marca comercial ou marca registrada da SonicWall Inc. e/ou de suas afiliadas nos EUA e/ou em outros países. Todas as outras marcas comerciais e marcas registradas são de propriedade dos respectivos proprietários.

As informações contidas neste documento são fornecidas em conexão com a SonicWall Inc. e/ou com os produtos de suas afiliadas. Nenhuma licença, expressa ou implícita, por preclusão ou de outra forma, a algum direito de propriedade intelectual é concedida por este documento ou em conexão com a venda de produtos da SonicWall. EXCETO CONFORME ESTABELECIDO NOS TERMOS E CONDIÇÕES ESPECIFICADOS NO CONTRATO DE LICENÇA DESTE PRODUTO, A SONICWALL E/OU SUAS AFILIADAS NÃO ASSUMEM NENHUMA RESPONSABILIDADE E EXIMEM-SE DE TODA GARANTIA EXPRESSA, IMPLÍCITA OU JURÍDICA RELATIVA A SEUS PRODUTOS, ENTRE ELAS, A GARANTIA IMPLÍCITA DE COMERCIALIZAÇÃO, ADEQUAÇÃO A UMA DETERMINADA FINALIDADE OU NÃO VIOLAÇÃO. EM NENHUMA CIRCUNSTÂNCIA A SONICWALL E/OU SUAS AFILIADAS SERÃO RESPONSÁVEIS POR PERDAS E DANOS, MULTA COMPENSATÓRIA, DANOS EMERGENTES OU IMPREVISTOS (ENTRE ELES, DANOS POR LUCROS CESSANTES, INTERRUPÇÃO DE NEGÓCIOS OU PERDA DE INFORMAÇÕES) DECORRENTES DO USO OU DA IMPOSSIBILIDADE DE USO DESTE DOCUMENTO, MESMO QUE A SONICWALL E/OU SUAS AFILIADAS TENHAM SIDO INFORMADAS SOBRE A POSSIBILIDADE DE TAIS DANOS. A SonicWall e/ou suas afiliadas não fazem declarações ou garantias quanto à exatidão ou à integridade do conteúdo deste documento e reservam-se o direito de fazer alterações às especificações e descrições de produtos a qualquer momento sem notificação prévia. A SonicWall Inc. e/ou suas afiliadas não assumem nenhum compromisso de atualizar as informações contidas neste documento.

Quem Somos

A SonicWall oferece Boundless Cybersecurity ou Cibersegurança sem Limites para a era da hiperdistribuição, em uma realidade de trabalho em que todos estão remotos, têm mobilidade e estão menos seguros. Com o conhecimento do desconhecido, a disponibilização de visibilidade em tempo real e a viabilização de uma economia revolucionária, a SonicWall fecha a lacuna nno setor de cibersegurança para corporações, governos e pequenas e médias empresas no mundo inteiro. Para obter mais informações, visite www.sonicwall.com.

Em caso de dúvidas sobre o possível uso deste material, escreva para:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Consulte nosso website para obter informações adicionais.
www.sonicwall.com/pt-br/