Vantagens Forcepoint

FORCEPOINT

O Desafio Atual da Cibersegurança

Na era da transformação digital, as empresas mais bem-sucedidas do mundo lideram seus setores monetizando seus dados e propriedade intelectual. E é fundamental proteger esses dados e a Propriedade Intelectual (PI) contra vazamento ou adulteração; as perdas podem comprometer os lucros e a reputação da marca duramente conquistados. Os CISOs e outros executivos responsáveis pela segurança entendem o que está em jogo. Mas o trabalho destes profissionais está mais difícil do que nunca, no atual modelo operacional de TI, que inclui nuvens públicas, BYOD e mobilidade. Os dados estão em todos os lugares e podem ser acessados em qualquer ponto.

As superfícies de ataques continuam a aumentar exponencialmente, tornando ainda mais difícil bloquear ameaças. As abordagens tradicionais de segurança digital, que dependem de produtos autônomos, não foram projetadas para este mundo novo.

Mas a abordagem centrada nas pessoas da Forcepoint é diferente. Nossa abordagem de segurança dinâmica e centrada no ponto humano se adapta conforme o nível de risco apresentado pelos comportamentos do usuário, fornecendo aos profissionais de segurança um caminho novo para proteger seus dados e usuários de forma proativa, em qualquer lugar.

> 60% da TI corporativa está off-premises e na nuvem.[1]

> Os líderes de segurança e gestão de riscos devem adotar uma abordagem estratégica de análise contínua e adaptável de riscos e confiança (CARTA, Continuous Adaptive Risk and Trust Assessment). Isso é vital para habilitar com segurança o acesso às iniciativas de negócios digitais em um mundo de ataques avançados e direcionados. Habilitará decisões em tempo real com base em riscos e confiança, com respostas adaptáveis.[2]
>
> Pesquisa do Gartner, 10 principais estratégicas e tendências para 2018

1 https://www.idc.com/getdoc.jsp?containerId=US41883016

2 Gartner, Top 10 Strategic Technology Trends for 2018, por David W Cearley et al., 3 de outubro de 2017.

As abordagens tradicionais estão em um ponto de superação

A abordagem típica para a cibersegurança depende do uso de produtos pontuais que não interoperam. Tecnologias diferentes funcionam para determinados casos de uso, mas a falta de integração entre elas resulta na geração de um número avassalador de alertas. As equipes de segurança são desafiadas a tentar diferenciar uma ameaça real de milhares de alarmes falsos. Quando conseguem encontrá-la, danos substanciais podem já ter ocorrido.

A sobrecarga de alertas é um sintoma de um grande problema: a dependência de uma abordagem binária e centrada em ameaças, onde atividades "boas" e "ruins" podem ser abordadas com políticas estáticas. Mas a intenção subjacente à grande maioria dos outros eventos que recaem entre os dois extremos do espectro é desconhecida. Sem entender o contexto por trás da atividade, as equipes de segurança precisam investigar cada uma manualmente. Adotar uma abordagem centrada em ameaças leva a um cenário sem vencedores.

Uma empresa é vítima de um ataque de ransomware a cada 14 segundos.[3]

US$ 3,62 milhões é o custo total médio de uma violação de dados.[4]

E mais, as equipes de cibersegurança parecem estar destinadas ao fracasso. Estima-se que mais de 80% dos incidentes de segurança digital exploram vulnerabilidades bem conhecidas.[5]
A forma como atuamos hoje simplesmente não funcionará no futuro.

3 https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
4 Ponemon Institute, 2017 Cost of Data Breach Study
5 SANS Institute, Cyber Security Trends: Aiming Ahead of the Target to Increase Security in 2017

Por que cibersegurança centrada em pessoas?

Mais de 80% das violações relacionadas a hacking exploram credenciais comprometidas. Os serviços simples de autenticação e autorização de usuários e dispositivos não conseguem monitorar o comportamento e não oferecem controle sobre os dados depois que o acesso foi concedido. Também é praticamente impossível se defender, com métodos tradicionais de cibersegurança, contra hackers que comprometeram bons funcionários, com acesso sem permissão aos seus sistemas.

Além disso, os bons funcionários cometem erros, que levam involuntariamente a perdas de dados. E, às vezes, funcionários insatisfeitos podem não ter as melhores intenções.

Em vez de tentar proteger integralmente redes próprias e administradas por terceiros, bloqueando diversos pontos de acesso e tentando entender um número avassalador de eventos de segurança, é essencial entender o comportamento digital de todos os usuários – funcionários, clientes e parceiros – à medida que interagem com dados e sistemas para avaliar proativamente o risco que suas atividades podem representar.

Líder em proteção adaptável aos riscos

A abordagem de segurança legada e centrada em eventos não faz mais sentido no complexo cenário digital de hoje. A segurança mais eficaz é adaptável a riscos, fornecendo o contexto necessário para aplicar dinamicamente as políticas relevantes, até o nível individual. E é somente pelo contexto que podemos entender se uma identidade ou um comportamento de usuários específicos são legítimos, arriscados ou maliciosos.

A abordagem adaptável a riscos da Forcepoint identifica, analisa e garante a execução das políticas—protege seus usuários, dados e redes em tempo real e aumenta a eficácia de seus investimentos em segurança.

Diferente de outros sistemas, as nossas soluções não lotam o seu SIEM com alertas que requerem disposição manual. Possibilita saber como é a atividade normal e produtiva dos funcionários e todas as formas peculiares como as pessoas interagem com dados, aplicando automaticamente as políticas certas para seus perfis de riscos.

Simultaneamente, fornece insight sobre a localização de seus dados e como se deslocam, dentro e fora da organização. Nosso modelo adaptável a riscos fornece maior visibilidade, uma política única para sistemas distribuídos, aplicação rápida e compliance mais rigorosa.

É hora de segurança digital centrada em pessoas.

O que é a Forcepoint?

A Forcepoint foi criada com o objetivo de fornecer soluções de cibersegurança de próxima geração.

- É uma das maiores empresas privadas de segurança digital no mundo, com milhares de clientes empresariais e governamentais em mais de 150 países
- Líder em prestação de serviços para a comunidade mundial de Inteligência e missões digitais de alta segurança
- Um dos portfólios de produtos de segurança mais abrangentes no setor

O Ponto Humano

Ao se afastar de uma abordagem de cibersegurança centrada em ameaças, você pode restringir o seu foco para as duas importantes constantes em segurança—pessoas e dados.

Proteger o ponto humano significa assegurar a interseção de pessoas, dados críticos e propriedade intelectual, que começa com o compreensão de seu ritmo e o fluxo de seus dados. Possibilita saber como é a atividade normal e produtiva dos funcionários e todas as formas peculiares como as pessoas interagem com dados.

A **Proteção de Dados Dinâmica Forcepoint** é a primeira solução convergente do setor para DLP de próxima geração que oferece proteção adaptável aos riscos. Associa os recursos de DLP líderes do setor da Forcepoint com um recurso de análise centrada em comportamentos para proteger contra exfiltração de dados. A Proteção de Dados Dinâmica estabelece uma linha “normal” de comportamento do usuário e aplica um conjunto de contramedidas de segurança automatizadas com base na pontuação de riscos de um usuário. Tudo sem intervenção do administrador.

Portfólio da Forcepoint Centrado em Pessoas

A Forcepoint está convergindo suas capacidades para simplificar a implementação e a gestão de sua pilha de segurança e eliminar falhas de segurança. Todos os recursos são os melhores da categoria, você pode começar onde quiser e expandir conforme as suas necessidades cresçam. Nossa política unificada e a análise e orquestração comuns dinamizam a administração.

As soluções da Forcepoint incluem:

Análises Comportamentais da Forcepoint
Análises do comportamento de usuários e organizações para um mundo com perímetro zero. Líder em insights acionáveis com base em pontuação adaptável a riscos.

Forcepoint DLP
Descoberta e proteção para cumprir as leis e as normas setoriais.

Forcepoint Insider Threat
Visibilidade de usuários e contexto de incidentes para dados confidenciais. O entendimento mais abrangente de intenção do usuário, com a confiança de mais de 1 milhão de endpoints.

Forcepoint CASB
Visibilidade e controle sobre todo o seu ambiente de nuvem. O suporte para aplicativos de nuvem mais abrangente, com avaliação de riscos personalizada exclusiva, baseada em comportamento dos usuários e classificação do acesso aos dados.

Forcepoint SD-WAN e Next Generation Firewall (NGFW)
Segurança de rede altamente segura, eficiente e disponível. Reduz as despesas de rede em 50%, reduz os ataques digitais em até 86% e diminui o tempo de resposta a incidentes em até 73%.

Forcepoint Data Guard
Colaboração segura e compartilhamento de informações para agências do governo. Elimina transferências manuais dispendiosas e demoradas de dados altamente regulados e confidenciais.

Forcepoint Web and Email Security
Proteção unificada contra ameaças avançadas em qualquer lugar e em qualquer dispositivo. A detecção de ameaças é de 100%, sem falsos positivos.

Reconhecimento do Setor

Nove vezes consecutivas no Quadrante Mágico do Gartner para prevenção contra perda de dados corporativos.
*Gartner, Magic Quadrant for Enterprise Data Loss Prevention, 16 de fevereiro de 2017. Anteriormente posicionado como Websense nos relatórios do Quadrante Mágico de Prevenção contra Perda de Dados com Reconhecimento de Conteúdo e no Quadrante Mágico de Monitoramento e Filtragem de Conteúdo e Prevenção contra Perda de Dados. O Gartner não endossa qualquer fornecedor, produto ou serviço incluído em suas publicações de pesquisas e não recomenda que usuários de tecnologia selecionem apenas os fornecedores com as classificações mais altas ou outra designação. As publicações de pesquisas do Gartner consistem nas opiniões da organização de pesquisa do Gartner e não devem ser interpretadas como declarações de fatos. O Gartner nega todas as garantias, expressas ou implícitas, com relação a esta pesquisa, incluindo todas as garantias de comerciabilidade ou adequação a uma finalidade específica.

Sobre a Forcepoint

A Forcepoint está transformando a segurança digital, com foco no que é mais importante: o comportamento das pessoas ao interagir com sistemas e dados críticos. Essa abordagem centrada nas pessoas para a segurança digital libera os funcionários para inovar, com o entendimento do ritmo normal do comportamento dos usuários, e do fluxo de entrada e saída de dados em uma organização. As soluções baseadas em comportamentos da Forcepoint adaptam-se ao risco em tempo real e são entregues em uma plataforma de segurança convergida para proteger usuários de redes e acesso à nuvem, evitar que dados confidenciais saiam da rede corporativa e eliminar falhas causadas por pessoas internas. Com sede em Austin, Texas, a Forcepoint protege o ponto humano para milhares de clientes empresariais e governamentais em mais de 150 países.

forcepoint.com/contact

[CORPORATE-OVERVIEW-GLOBAL-BROCHURE-US-EN] 400019.030719

FORCEPOINT