



PLATAFORMA DE ESTUDOS ANALÍTICOS SOBRE SEGURANÇA DA BLUE COAT

ENXERGUE, COMPREENDA E RESPONDA RAPIDAMENTE A AMEAÇAS AVANÇADAS

O malware avançado e os ataques de "zero-day" não são detectados pelas tecnologias de segurança tradicionais. Assim, as organizações estão aceitando o fato de que, em algum momento, suas redes serão invadidas. Por isso, está acontecendo uma mudança em direção a uma estratégia mais moderna, uma abordagem abrangente que oferece informações e análise em tempo real necessárias para enxergar, compreender, responder a e fortalecer a rede contra ameaças avançadas e ataques direcionados. A plataforma de estudos analíticos sobre segurança da Blue Coat fecha a brecha de segurança ao combinar visibilidade da segurança, estudos analíticos sobre segurança e informações em tempo real para proporcionar detecção imediata e resposta eficaz a incidentes. Em resumo, ela possibilita a proteção contra ameaças avançadas e dá autonomia para superar o medo e a ansiedade relacionados a cada nova ameaça à segurança: comece a vislumbrar novas possibilidades para seus negócios.

Adaptação ao cenário de ameaças em evolução

A quantidade, a variedade e as fontes de ataques à segurança estão aumentando. Mais de 200.000 novas amostras de malware surgem a cada dia, de acordo com o Kaspersky Lab. Ameaças avançadas de "zero-day", malware de última geração e ataques direcionados de fontes externas ou mesmo de funcionários crescem a cada dia em tamanho e amplitude.

As estratégias de bloqueio tradicionais simplesmente não são eficientes contra ataques avançados. À medida que os cenários de segurança continuam a evoluir, as organizações e equipes de segurança de TI precisarão de soluções adaptáveis e personalizadas que superem as brechas nas ferramentas baseadas em assinatura atuais e fornecem visibilidade perfeita de tudo o que entra e sai da rede, mesmo diante do rápido crescimento e dos enormes volumes de tráfego de rede. E, para enfrentar com eficiência a crescente ausência de visibilidade em suas estruturas de segurança, as organizações também precisarão de soluções de segurança simples, flexíveis e econômicas.

A plataforma de estudos analíticos sobre segurança, parte integrante do Blue Coat Threat Protection Suite (pacote de proteção contra ameaças avançadas), fecha a brecha de segurança e supera os principais desafios de alcançar a proteção contra ameaças avançadas, incluindo:

- A fácil implementação de uma solução simples e flexível que funciona com os ecossistemas, processos e fluxos de trabalho de segurança atuais.
- A capacidade de aproveitar as fontes mais abrangentes de informações sobre ameaças em tempo real enquanto fornece um registro completo de toda a atividade ocorrida antes, durante e após um ataque.

92%

das brechas foram
causadas por
agentes externos.

84%

dos ataques
levaram apenas
segundos, minutos
ou horas para
comprometer
a rede.

78%

dos ataques
levaram semanas,
meses ou anos
para serem
descobertos.

Verizon Business, 2013

- Dimensionamento para acompanhar o crescimento da organização, a necessidade de gerenciamento de segurança centralizada e as crescentes demandas por desempenho de rede.

Informações claras, imediatamente

A plataforma de estudos analíticos sobre segurança proporciona aos profissionais de segurança respostas claras e concisas para perguntas importantes sobre a segurança após uma brecha, incluindo: Quem fez isso? Como? Quando? O que foi acessado? A premiada plataforma pode ser implementada no hardware de sua escolha, como appliances pré-configurados ou como um appliance virtual que registra e classifica cada pacote de tráfego de rede, da Camada 2 à Camada 7, enquanto indexa e armazena os dados para fornecer informações abrangentes sobre ameaças e estudos analíticos após a brecha sobre qualquer evento de segurança.

O resultado são evidências acionáveis para percepção situacional em tempo real; monitoramento contínuo; detecção de malware avançado; resposta e resolução de incidentes de segurança; monitoramento e análise de perda de dados; controle de TI, gerenciamento de riscos e conformidade, além de garantia de segurança.

Principais funcionalidades e vantagens

A plataforma de estudos analíticos sobre segurança é a única solução flexível, econômica e independente de hardware, enquanto se integra com fontes de informações sobre ameaças bastante confiáveis e tecnologia de sandboxing de última geração para proteção abrangente contra ameaças avançadas. Esta solução proporciona:

Classificação de aplicações: a plataforma de estudos analíticos sobre segurança revela a verdadeira identidade de qualquer aplicação que tente se ocultar dentro de sua rede. A abrangente DPI (Deep Packet Inspection, inspeção profunda de pacotes) classifica mais de 1.800 aplicações e milhares de detalhes de metadados descritivos. Esse recurso não só identifica aplicações com eficiência, como também fornece informações descritivas sobre uma sessão de rede que inclui aplicações, informações pessoais de usuários, ações pretendidas, tipos de conteúdo, nomes de arquivos e mais.

Informações sobre ameaças em tempo real: a plataforma integra-se diretamente com os Blue Coat ThreatBLADES para proporcionar uma virada real no jogo da segurança. Ao aproveitar a rede de informações globais da Blue Coat e o "efeito de rede" de mais de 75 milhões de usuários, os ThreatBLADES oferecem informações imediatas e acionáveis sobre ameaças na Web, e-mail ou baseadas em arquivos. A extração de arquivos em tempo real dos estudos analíticos sobre a segurança também extrai e inspeciona arquivos automaticamente para permitir a identificação imediata e automática de ameaças conhecidas, além de otimizar o sandboxing de malware ao eliminar ameaças conhecidas de detonação desnecessária.

Estudos analíticos sobre segurança de Camada 2 a 7: a plataforma de estudos analíticos sobre segurança fornece uma série de funcionalidades de estudos analíticos de grandes volumes de dados para fortalecer a resposta a incidentes de segurança com análise abrangente e conclusiva. Os principais recursos incluem reconstrução de sessão completa; verificação de reputação em tempo real; reconstrução de mensagens instantâneas, e-mail e imagem;

explorador de causa raiz e fornecimento de artefatos completos, não somente pacotes.

Segurança relacionada ao contexto: a plataforma integra-se com as mais modernas tecnologias de segurança de rede para se articular diretamente a partir de qualquer alerta ou relatório e obter detalhes completos sobre a carga do evento antes, durante e após o alerta. A API REST aberta e de serviços da Web acrescenta contexto completo a qualquer ferramenta de segurança e possibilita aproveitar importantes tecnologias, como Dell SonicWALL™, FireEye™, HP ArcSight™, McAfee®, Palo Alto Networks™, Sourcefire®, Splunk® e várias outras aplicações segurança.

Visibilidade de segurança total: com a plataforma de estudos analíticos sobre segurança, você obtém informações sobre milhares de aplicações, dezenas de transportes de arquivos, todos os fluxos e todos os pacotes, incluindo tráfego criptografado por meio da integração próxima com o appliance de visibilidade SSL da Blue Coat.

Explorador de causa raiz: o explorador de causa raiz simplifica a resposta a incidentes. Ao usar objetos de rede extraídos, a ferramenta reconstrói uma linha do tempo de sessões da Web, e-mails e conversas em bate-papo suspeitos. Ao criar automaticamente uma linha do tempo desses eventos, o explorador de causa raiz ajuda o analista a identificar rapidamente a origem de uma infecção ou comprometimento e reduzir significativamente o tempo de resolução.

Implementação flexível: a plataforma de estudos analíticos sobre segurança oferece várias opções de implementação para otimizar o TCO (Total Cost of Ownership, custo total de propriedade) e reduzir despesas de capital (CapEx): um nível de flexibilidade que nenhuma outra solução consegue oferecer. É facilmente implementada em hardware padrão de empresas, como appliances pré-configurados ou como um appliance virtual para uma segurança abrangente que vai desde filiais até o datacenter corporativo.

Visualize. Analise. Corrija.

A plataforma de estudos analíticos sobre segurança oferece a solução mais abrangente do setor para proteção contra ameaças avançadas. Ela proporciona visibilidade perfeita do tráfego de rede com informações acionáveis sobre ameaças à segurança, juntamente com uma maneira flexível e econômica de expandir a segurança corporativa sob demanda.

Entre em contato hoje com o representante da Blue Coat para obter mais informações ou para agendar uma demonstração. Leve suas defesas de segurança e resposta a incidentes a um novo patamar de sofisticação e proporcione novas oportunidades para a autonomia dos negócios.



Análise de ameaças em tempo real

Sede Corporativa
Sunnyvale, CA USA
+1.408.220.2200

Blue Coat Brasil
São Paulo
+55 11 3443 6879

Blue Coat México
México D.F.
+52 55 3300 5825

Blue Coat Argentina
Buenos Aires
+54 (11) 4850 1215