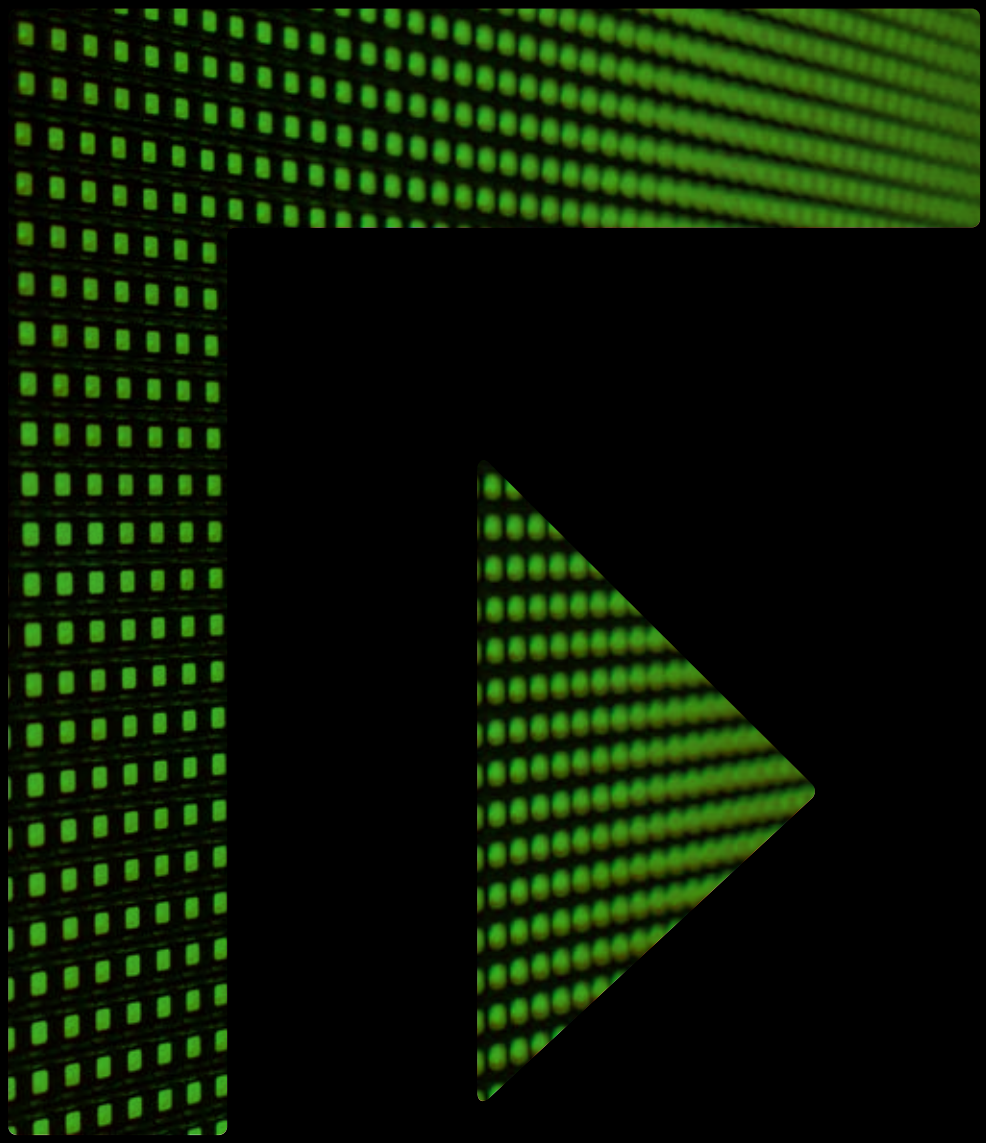


TRITON® AP-EMAIL

IMPEÇA ATAQUES DE AMEAÇAS AVANÇADAS, IDENTIFIQUE USUÁRIOS DE ALTO RISCO E CONTROLE AMEAÇAS INTERNAS

FORCEPOINT
POWERED BY Raytheon

TRITON® AP-EMAIL

IMPEÇA ATAQUES DE AMEAÇAS AVANÇADAS, IDENTIFIQUE USUÁRIOS DE ALTO RISCO E CONTROLE AMEAÇAS INTERNAS

Desde iscas de engenharia social até phishing direcionado, a maioria dos ataques digitais começam com email. Como essas ameaças avançadas e em vários estágios associam elementos de web e email nos ataques, apresentam uma 'Cadeia de Ataque' de oportunidades para interrompê-los antes que a violação ocorra.

Maximize o uso e a segurança do email

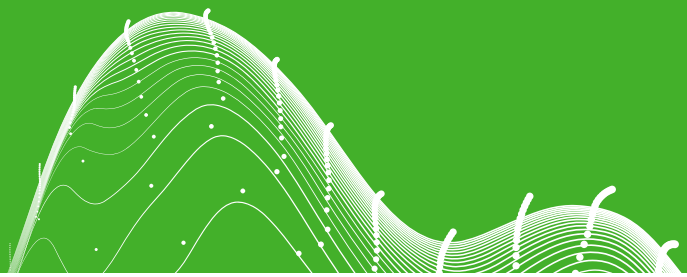
TRITON® AP-EMAIL identifica ataques direcionados, usuários de alto risco, Ameaças Internas, habilita os trabalhadores móveis e a adoção segura de novas tecnologias, como Microsoft Office 365 e Box. Desde atividade de ataques de entrada até furto de dados de saída ou tentativas de comunicações de botnet, a segurança Forcepoint™ TRITON Email protege as comunicações por email como parte de uma defesa TRITON APX completa contra ameaças avançadas.

Desafios da segurança de email

- As ameaças persistentes avançadas costumam usar email para os estágios iniciais dos ataques avançados.
- O email deve fazer mais para abordar furto de dados e ameaças internas.
- As empresas precisam adotar o Microsoft Office 365 e outros serviços para expansão e concorrência.
- Hábitos arriscados dos usuários podem facilmente levar a violações de segurança e perda de dados.

"Em última instância, estamos muito satisfeitos com os produtos da Forcepoint. O Forcepoint TRITON Email Security está fazendo seu trabalho e bloqueando quaisquer problemas antes que cheguem ao nosso servidor."

— Ray Finck, Gerente de Sistemas de Informação, Lowe Lippmann



Recursos do TRITON AP-EMAIL

IMPEÇA AMEAÇAS PERSISTENTES AVANÇADAS E OUTRAS AMEAÇAS AVANÇADAS DIRECIONADAS

Forcepoint ACE (Advanced Classification Engine) está no coração de todas as soluções TRITON e identifica iscas maliciosas, kits de exploit, ameaças emergentes, comunicações de botnet e outras atividades de ameaças avançadas na Cadeia de Ataque. Isso habilita o TRITON AP-EMAIL a identificar os estágios iniciais de um ataque. Com seus potentes recursos de avaliação de malware que incluem um sandboxing comportamental de arquivos totalmente integrado, pode até identificar ameaças de malware de Dia Zero.

PROTEJA DADOS CONFIDENCIAIS CONTRA AMEAÇAS EXTERNAS E AMEAÇAS INTERNAS

Para se preparar para uma ameaças internas maliciosa ou um ataque digital potencialmente bem-sucedido, é essencial que as comunicações de saída sejam monitorizadas. Isso também é necessário tanto para necessidades de conformidade contra furto de dados e requisitos empresariais. Apenas Forcepoint fornece a tecnologia para impedir infiltração e exfiltração de dados, com recursos como:

- Exame com reconhecimento óptico de caracteres (OCR) para identificar dados confidenciais ocultos em imagens, como documentos digitalizados ou capturas de tela.
- Detecção de arquivos criptografados para reconhecer arquivos criptografados personalizados e projetados para impedir a identificação.
- Monitoramento de drip DLP para identificar onde dados confidenciais são vazados em pequenas quantidades ao longo do tempo.

ADOTE COM SEGURANÇA NOVAS TECNOLOGIAS, COMO MICROSOFT OFFICE 365 E BOX, E APOIE SUA FORÇA DE TRABALHO EM ROAMING

Os departamentos de TI estão sobrecarregados para manter os sistemas atuais e ainda fornecer suporte para uma força de trabalho cada vez mais móvel, e as demandas para adotar novas tecnologias como Microsoft Office 365. TRITON AP-EMAIL fornece recursos líderes do setor que alavancam sistemas e outras informações para controlar comunicações, como impedir o acesso total a anexos de email confidenciais em dispositivos móveis vulneráveis, enquanto permitem acesso total em notebooks totalmente protegidos. Essas defesas de entrada e saída são todas compatíveis com Microsoft Office 365.

IDENTIFIQUE COMPORTAMENTOS DE USUÁRIO DE 'ALTO RISCO' E EDUQUE OS USUÁRIOS PARA AUMENTAR A CONSCIENTIZAÇÃO

As coleções de dados ricas no TRITON AP-EMAIL são usadas por diversas políticas para reportar e identificar sistemas que podem precisar de atenção especial da TI. Geram um relatório sobre diversos indicadores de comprometimento para identificar sistemas infectados e relatórios mais proativos sobre comportamento suspeito, ou mesmo atividades de 'funcionários insatisfeitos' como ameaças internas potenciais. Os recursos de feedback de usuários ajudam a educar os funcionários quando erros ocorrem, ajudando-os a aprender e entender melhor as práticas recomendadas para email seguro.

Módulos de proteção aprimorados

MÓDULO EMAIL CLOUD OU EMAIL HYBRID	**Alavanque serviços em nuvem para desempenho e escalabilidade** Combine defesas contra ameaças no local com serviços de filtragem prévia na nuvem para preservar a largura de banda com SLAs antispam líderes do setor. Ou escolha uma implementação 100% em Nuvem de todos os serviços TRITON AP-EMAIL.
MÓDULO EMAIL DLP	**Bloqueie o furto de dados com DLP com reconhecimento de conteúdo de classe empresarial** Prepare-se para ameaças internas e furto de dados de malware, alcance metas de conformidade e mitigue adicionalmente o risco para informações pessoais. Os recursos avançados detectam furto de dados oculto em imagens ou arquivos criptografados personalizados, ou transmitidos em pequenas quantidades ao longo do tempo para evitar a deteção.
MÓDULO EMAIL SANDBOX	**Integre sandboxing comportamental para avaliação de malware adicional** Suplemente as análises do Forcepoint ACE com um sandboxing de arquivos integrado para inspeção profunda adicional, e alavanque a análise comportamental em um ambiente virtual para revelar o comportamento malicioso de Dia Zero e outros malwares avançados. Teste arquivos de forma automática ou manual para gerar análise forense detalhada.
MÓDULO EMAIL ENCRYPTION	**Garanta a confidencialidade de comunicações confidenciais** Habilite os dispositivos móveis em seu local de trabalho, ampliando suas políticas de segurança existentes para dispositivos móveis para protegê-los contra Ameaças Avançadas, malware móvel, ataques de phishing, spoofing e mais.
MÓDULO IMAGE ANALYSIS	**Identifique imagens explícitas para exigir uso aceitável e conformidade** O módulo Forcepoint análise de imagens permite que os empregadores adotem medidas proativas para monitorar, educar e fiscalizar a política de emails da empresa em relação a anexos com imagens explícitas ou pornográficas.
TRITON APX	**A solução Forcepoint recomendada para proteção avançada** Estenda a sua proteção do TRITON AP-EMAIL para TRITON AP-WEB, TRITON AP-DATA ou TRITON AP-ENDPOINT, para proteção potente e unificada em todos os canais de ataque.

"O TRITON Email Security foi atraente porque eliminou o trabalho de administrar nossa segurança de e-mail e entregou mais do que esperávamos em termos de resiliência e facilidade de uso. De forma Geral, o TRITON Email Security habilitou-nos a entregar um serviço mais resiliente, profissional e eficaz em termos de custos para os nossos usuários"

— Martin Law, Líder de T, NCP

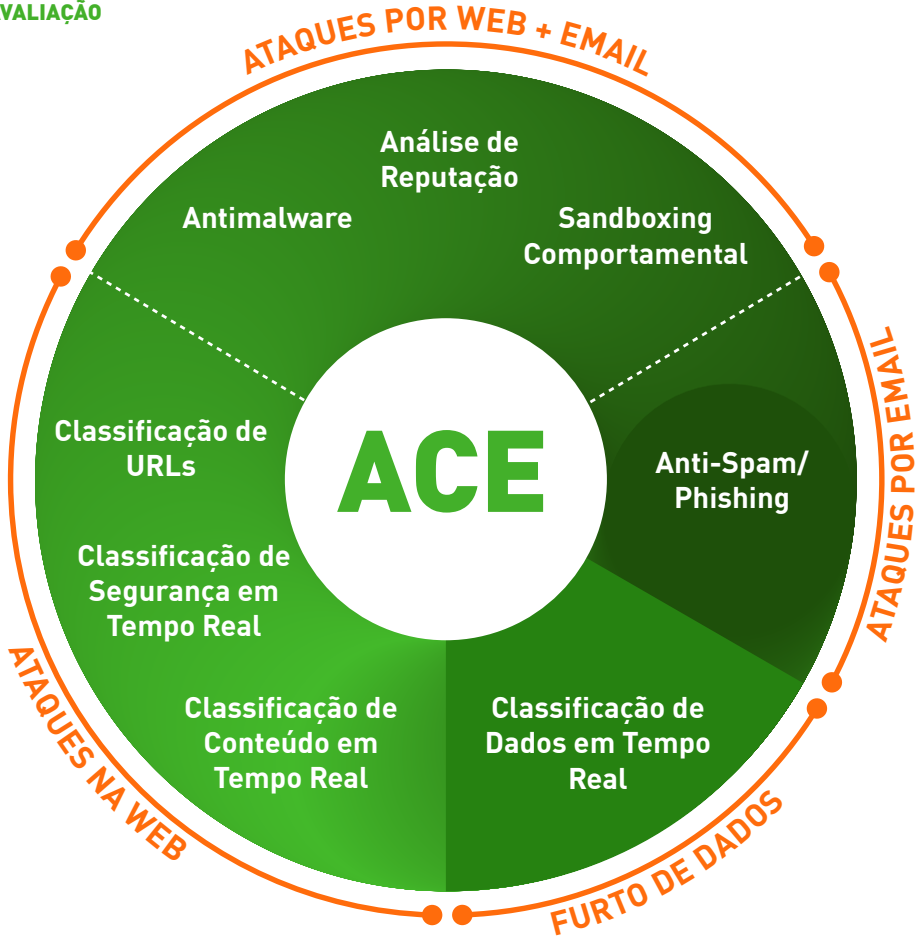
A potência por trás das soluções TRITON

ACE (Advanced Classification Engine)

Forcepoint ACE fornece defesas contextuais em linha e em tempo real para segurança Web, Email, de Dados e Móvel, usando pontuação de riscos composta e análises preditivas para fornecer a segurança mais eficaz disponível. Também fornece contenção ao analisar o tráfego de entrada e saída com defesas com reconhecimento de dados para proteção líder do setor contra furto de dados. Classificadores para análise de segurança, dados e conteúdo em tempo real, resultantes de anos de pesquisa e desenvolvimento, habilitam o ACE a detectar mais ameaças do que os mecanismos antivírus tradicionais todos os dias (a comprovação é atualizada diariamente em http://securitylabs.forcepoint.com). O ACE é a defesa primária por trás de todas as soluções Forcepoint TRITON e é apoiado pelo Forcepoint ThreatSeeker® Intelligence Cloud.

CONJUNTO INTEGRADO DE RECURSOS DE AVALIAÇÃO DE DEFESAS EM 8 ÁREAS PRINCIPAIS.

- 10.000 dados analíticos disponíveis para apoiar inspeções profundas.
- Mecanismo de segurança preditivo que vê diversos movimentos à frente.
- A operação em linha não apenas monitora, mas **bloqueia** as ameaças.



ThreatSeeker® Intelligence Cloud

O ThreatSeeker Intelligence Cloud, administrado pelo Forcepoint Security Labs™, fornece a inteligência de segurança coletiva essencial para todos os produtos de segurança Forcepoint. Reúne mais de 900 milhões de pontos de extremidade, incluindo entradas do Facebook e, em conjunto com as defesas de segurança do Forcepoint ACE, analisa até 5 bilhões de solicitações ao dia. Esse reconhecimento abrangente de ameaças de segurança habilita o ThreatSeeker Intelligence Cloud a oferecer atualizações de segurança em tempo real que bloqueiam Ameaças Avançadas, malware, ataques de phishing, fraudes e scams, e fornecem as avaliações da Web mais recentes. O ThreatSeeker Intelligence Cloud é incomparável em alcance e no uso das defesas em tempo real do ACE para analisar dados coletivos. (Quando você faz upgrade para Web Security, o ThreatSeeker Intelligence Cloud ajuda a reduzir a sua exposição a ameaças da web e furto de dados.)

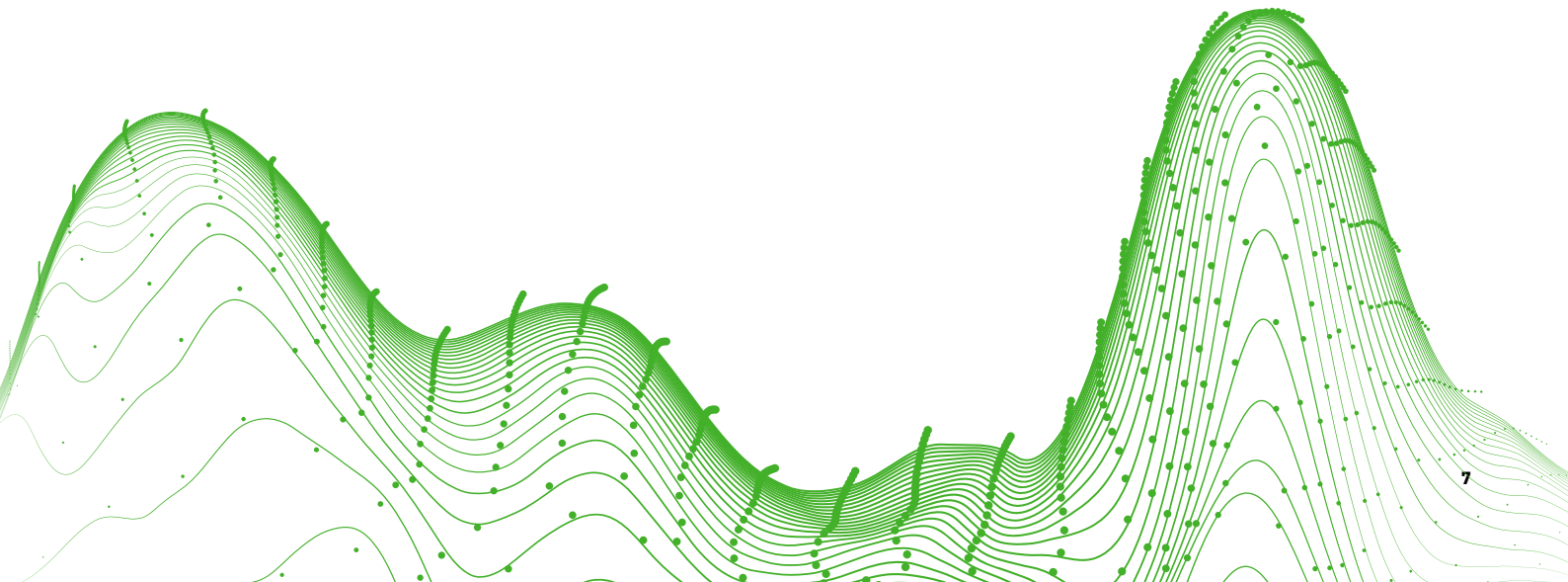
Arquitetura TRITON

Com segurança melhor da categoria, a arquitetura unificada Forcepoint TRITON oferece proteção no ponto de clique com defesas em linha e em tempo real do Forcepoint ACE. As defesas em tempo real incomparáveis do ACE são apoiadas pelo Forcepoint ThreatSeeker Intelligence Cloud e os conhecimentos dos pesquisadores do Forcepoint Security Labs. O resultado potente é uma arquitetura única, com uma interface de usuário unificada e inteligência de segurança unificada.

TRITON APX

TRITON APX fornece muitos benefícios essenciais para empresas interessadas em implementar a melhor proteção possível contra Ameaças Avançadas em todos os 7 estágios da Cadeia de Destruição. Podem ser resumidos nestas três afirmativas:

- **Implementar Segurança Adaptável -** Implantar soluções de segurança adaptáveis para rápidas mudanças tecnológicas e do cenário de ameaças.
- **Proteger em todos os lugares -** O perímetro são os dados. Proteger informações críticas contra furtos locais, na nuvem ou em dispositivos móveis.
- **Elevar o conhecimento em segurança -** Combater a carência de capacitação em cibersegurança, fornecendo inteligência preventiva e disponível em todo o ciclo de vida das ameaças.



CONTACT
www.forcepoint.com/contact

[BROCHURE_TRITON_AP_EMAIL_PTA4] 400003PT.011416

FORCEPOINT
POWERED BY Raytheon