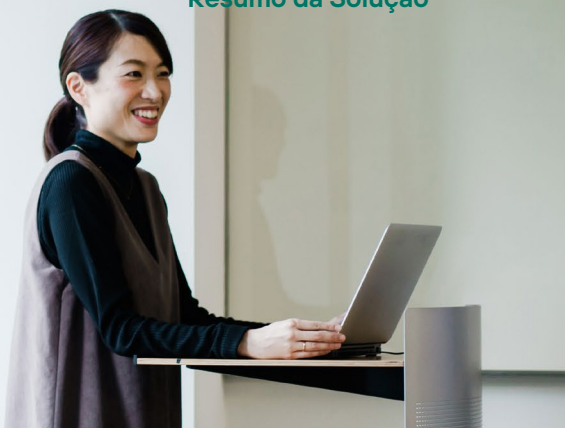
Forcepoint

Resumo da Solução



Forcepoint Zero Trust Content Disarm and Reconstruction for Portal Protection

Envie o arquivo—e não a ameaça!

Desafios

- Bloquear os ataques de dia zero.
- Reduzir a latência
- Impedir que os malwares cheguem aos endpoints

Solução

- Vá além da detecção: pare de tentar distinguir os dados bons dos ruins. O Zero Trust CDR pressupõe que todos os dados são inseguros ou hostis, o que significa que nada viaja de ponta a ponta, somente o conteúdo seguro.

Benefícios

- A proteção de portal garante que o conteúdo carregado para seus aplicativos voltados para a Internet esteja sempre livre de ameaças, sem necessidade de detectar a ameaça ou isolar a empresa do conteúdo de que ela precisa. Exploits de dia zero, ransomware, exploits de esteganografia, malwares sem arquivos e as ameaças inerentes em arquivos polimórficos: tudo é removido.
- Integração fácil com os atuais controladores de entrega de aplicativos de data center, balanceadores de carga/proxies reversos e firewalls de aplicativos da Web.

Ameaças conhecidas, desconhecidas e de dia zero ocultas em documentos e imagens de negócios costumam são usadas para carregar malware nas organizações. Em uma variedade de fluxos de trabalho de processos de negócios, incluindo sites de recrutamento, portais de cidadania e sites de serviços financeiros, as organizações precisam ter certeza de que, quando recebem documentos e imagens da Internet, não estão também carregando ameaças ocultas no conteúdo. As tentativas de anular essas ameaças usando tecnologias convencionais baseadas em detecção e detonação de sandbox introduzem latência desnecessária nos negócios, frustram os usuários e não eliminam o risco representado por ameaças desconhecidas e de dia zero.

Derrote ameaças desconhecidas

As tecnologias anti-malware existentes fornecem uma primeira linha de defesa, detectando ameaças conhecidas procurando assinaturas de exploits ou comportamentos inseguros encontrados anteriormente. Mas, repetidamente, as empresas são comprometidas por ameaças de dia zero que penetram na organização antes que as defesas baseadas em detecção possam se recuperar ou por ameaças completamente desconhecidas que são bem-sucedidas sem nunca serem identificadas adequadamente.

O Zero Trust Content Disarm and Reconstruction (CDR) for Portal Protection é a única maneira de derrotar não apenas ameaças conhecidas, mas também de dia zero e desconhecidas em documentos e imagens de negócios quando são enviados para portais, porque não depende de detecção ou detonação de sandbox. Em vez disso, usa um processo exclusivo de transformação para garantir proteção total.

Transforme a sua segurança

O Zero Trust CDR for Portal Protection funciona extraindo as informações empresariais de documentos e imagens quando chegam ao proxy reverso. Os dados que carregam as informações são descartados junto com quaisquer ameaças. Documentos e imagens novos são criados e entregues ao aplicativo de destino. Somente conteúdos seguros viajam de ponta a ponta. Os atacantes não conseguem entrar e a empresa recebe o que precisa.

Esse processo é denominado transformação. É insuperável: a equipe de segurança fica satisfeita porque a ameaça é removida e os usuários corporativos ficam satisfeitos porque obtêm as informações de que precisam.

O Zero Trust CDR é a única maneira de garantir que as ameaças sejam removidas do conteúdo. Dispensando os paradigmas falhos de detecção e isolamento de ameaças, a tecnologia exclusiva Zero Trust CDR da Forcepoint pressupõe que todos os dados são inseguros ou hostis. Não tenta diferenciar o bem do mal.

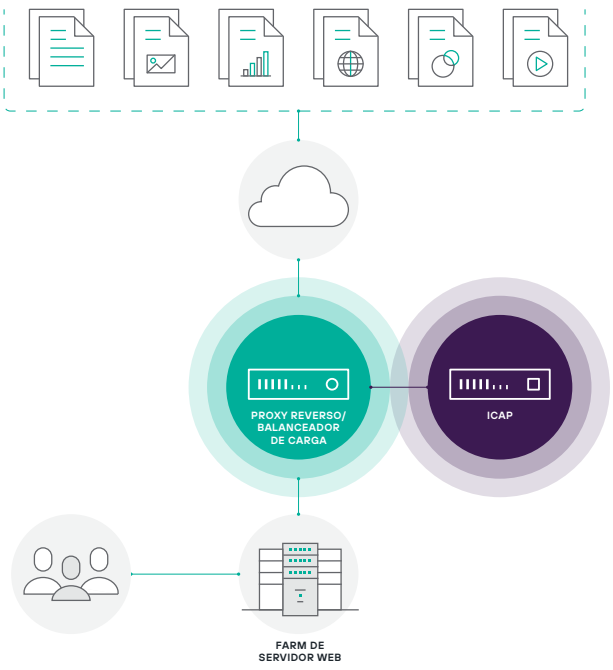
Acelere a Transformação Digital

Estamos na era dos portais de autoatendimento. Clientes atuais e potenciais são incentivados a fazer uploads de documentos para tudo, desde empréstimos pessoais e hipotecas até solicitações de seguro de automóvel. O problema é que, embora esses formatos de documentos sejam versáteis e incrivelmente úteis, também são altamente complexos, fáceis de subverter e costumam ser usados por criminosos cibernéticos para transportar payloads maliciosos.

Usando o Zero Trust CDR for Portal Protection, as organizações podem acelerar seus projetos de transformação digital, entregando aplicativos voltados para a Internet e portais de autoatendimento, com a certeza de que os documentos carregados não poderão ser usados como vetor para upload de ameaças ou comprometimentos na rede corporativa.

Garanta conteúdo digitalmente puro

Qualquer portal aumenta potencialmente a "superfície de ataque" da empresa. Os criminosos sabem disso e pretendem aproveitar qualquer vulnerabilidade. Agora, mais do que nunca, é vital garantir que o conteúdo carregado na organização seja seguro, puro e livre de ameaças. Qualquer empresa capaz de estabelecer um histórico de garantia de acesso a conteúdo comercial limpo e puro se diferenciará no que está se tornando rapidamente um faroeste cibernético.



O Zero Trust CDR for Portal Protection garante que as empresas possam colher os benefícios de seus projetos de transformação digital, com a confiança de que o conteúdo carregado com o qual lidam esteja livre de ameaças.

Integração total com as defesas existentes

A solução Zero Trust CDR for Portal Protection inclui o produto Gateway eXtension (GX) da Forcepoint. O GX é integrado a um proxy reverso existente, como balanceador de carga ou firewall de aplicativo da Web, usando ICAP. Em seguida, o conteúdo é passado para o GX pelo proxy reverso, que transforma o conteúdo para eliminar as ameaças transmitidas pelo conteúdo. O GX é simples para integrar, com configuração mínima.

Testado com os principais proxies reversos, o GX pode ser integrado facilmente a produtos de segurança de outras empresas, incluindo F5 BIG-IP, Citrix Netscaler, McAfee Web Gateway e Symantec Blue Coat. Impeça a infiltração de malware no conteúdo

Documentos do Office, arquivos PDF e imagens agora são os propagadores de malware mais comuns. A complexidade desses formatos de arquivos e dos aplicativos que os manipulam fazem com que sejam alvos naturais para os atacantes. Não importa qual seja o malware – desde ransomware e cavalos de Troia bancários a kits de acesso remoto e keyloggers – os criminosos cibernéticos sabem que o melhor lugar para ocultar sua mais recente ameaça de dia zero é dentro de um documento empresarial de rotina. Técnicas como malware sem arquivos e polimorfismo de arquivos tornam ainda mais difícil lidar com a ameaça usando a segurança cibernética convencional baseada em detecção.

O Zero Trust CDR for Portal Protection garante que os fluxos de trabalho de negócios (como importação de formulários de inscrição de clientes, upload de dados pessoais, etc.) possam continuar com total tranquilidade devido à maneira única como os documentos carregados são transformados. Todos os documentos e imagens estão sujeitos a transformação e todos ficam livres de ameaças.

Elimine as ameaças ocultas em imagens com esteganografia

A esteganografia é a ocultação secreta de dados em arquivos aparentemente inofensivos. É uma forma de codificar uma mensagem secreta dentro de outra mensagem, chamada de transportadora, de forma que apenas o destinatário desejado é capaz de lê-la.

Atualmente o Stegware, ou transformação da esteganografia em arma para ataques cibernéticos, está em ascensão. É oferecido por padrão em kits de malware como serviço na Dark Web. Tem sido usado em campanhas de malvertising para extorquir dinheiro de milhares de usuários e pressionar sites jornalísticos respeitáveis. E é usado em conjunto com redes sociais para roubar ativos financeiros de alto valor escondidos em imagens aparentemente inócuas. Tudo isso é má notícia para os profissionais de TI que usam ferramentas que identificam dados inseguros, já que a esteganografia é impossível de detectar.

O Zero Trust CDR for Portal Protection garante que cada imagem contida em um documento carregado esteja livre de qualquer conteúdo oculto usando Stegware. O processo de transformação destrói qualquer conteúdo oculto, tornando a imagem inútil para o atacante. O Zero Trust CDR for Portal Protection não apenas protege a organização contra exploits de entrada ocultos em imagens usando esteganografia: também amplia a prevenção de perda de dados existente e a iniciativa de governança (como o RGPD, Regulamento Geral de Proteção de Dados), porque interrompe completamente a perda de dados secreta por meio de esteganografia de imagem.

Desenvolvimento de uma solução vencedora

Juntamente com os nossos parceiros revendedores da Forcepoint, a equipe de soluções Forcepoint fornece uma ampla gama de serviços profissionais que ajudam você a maximizar seu investimento na tecnologia Zero Trust CDR. Podemos ajudar você a definir o escopo, planejar, instalar, configurar e gerenciar sua solução Zero Trust CDR for Portal Protection.

Certifique-se de que tudo corra bem durante e após a implementação com o Suporte Técnico Forcepoint. Nossa equipe de soluções altamente qualificada tem uma riqueza de conhecimentos e informações à sua disposição e pode atuar como uma extensão natural de sua equipe interna.

Resumo: Tenha proteção incomparável

Estamos à beira de uma revolução tecnológica. Diante de ataques cibernéticos implacáveis e combinados, as organizações estão sendo forçadas a reavaliar todos os aspectos de como adquirem, compartilham e realizam transações digitalmente.

As defesas com base em detecção de ameaças conhecidas são insuficientes. As que se baseiam em isolamento e detecção em sandbox inibem os negócios e deixam muito ao acaso. É necessário ter proteção.

O Zero Trust CDR for Portal Protection oferece proteção inigualável para qualquer portal empresarial. Garante que os documentos empresariais e imagens carregados estejam completamente livres de ameaças.

Para mais informações, acesse Forcepoint Zero Trust CDR

forcepoint.com/contact