White paper

Segurança na Web: Proteja seus dados na nuvem

Resumo

Sabemos que as equipes de segurança não podem estar em todos os locais, mas o cenário atual exige que as empresas estejam prontas para proteger seus dados em todos os lugares onde uma ameaça possa se manifestar. E, neste caso, “em todos os lugares” engloba redes, dispositivos móveis, ambientes virtuais, e também a nuvem ou o data center.

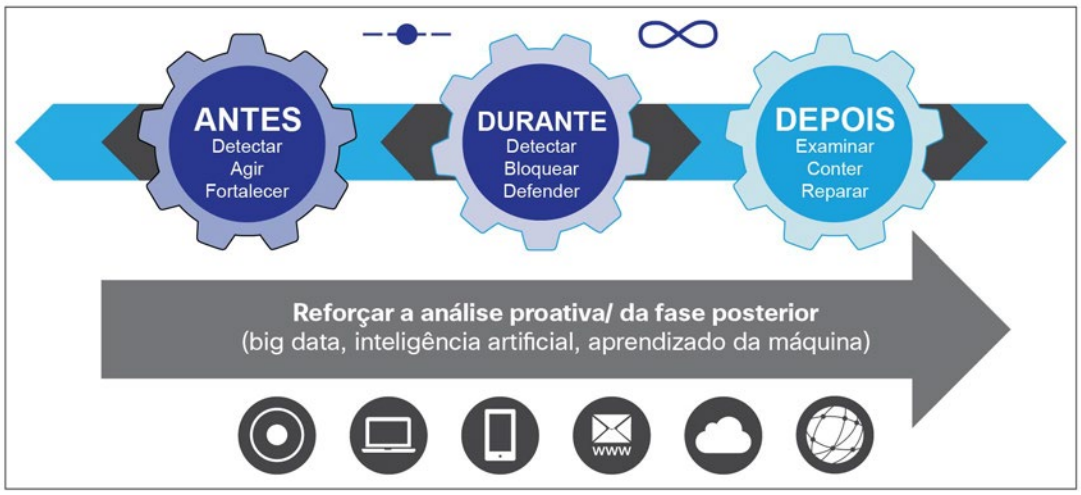
Hoje, as ameaças são desenvolvidas para vencer qualquer tipo de defesa. Os invasores trabalham ativamente para entender quais são as soluções de segurança implantadas. E estão mudando seus padrões de comportamento para torná-los menos perceptíveis e detectáveis. De acordo com o **Relatório de Segurança Anual da Cisco de 2014**, a principal missão da maioria desses invasores é roubar dados valiosos para sua empresa.[1]

Enquanto isso, o crescimento do modelo de empresa distribuída e o surgimento de novas tendências de negócios, como a computação em nuvem, a mobilidade e o BYOD (consumerização de TI), diminuíram o perímetro tradicional de segurança e estão expandindo a superfície de ataque. As equipes de segurança estão se esforçando para acompanhar esse ritmo de mudanças. Entretanto, não conseguem priorizar quais ameaças devem ser investigadas e estão deixando passar muitas delas por nem sequer percebê-las.

É fácil entender por que as soluções de segurança preventivas e pontuais não oferecem a proteção adequada para as empresas modernas. Como sabemos, nenhum método de detecção é perfeito, e inevitavelmente algumas ameaças serão mais sofisticadas e disfarçadas a ponto de ultrapassarem todas as camadas de defesa. O que é necessário fazer então? Segurança contínua e retrospectiva criada para cobrir todo o ciclo da ameaça - antes, durante e depois de um ataque.

[1] Relatório de Segurança Anual da Cisco de 2014: http://www.cisco.com/c/en/us/products/security/annual_security_report.html.

Figura 1. O ciclo do ataque



Cisco Cloud Web Security Essentials

O Cisco® Cloud Web Security ajuda as empresas a enfrentarem o desafio de manter a segurança contínua em toda a rede. A solução oferece às empresa distribuídas recursos de segurança e controle líderes de mercado, com o mais amplo conjunto de opções de implantação disponível no setor. Uma versão na nuvem do Cisco Web Security, a plataforma do Cloud Web Security estende a segurança da Web a dispositivos móveis e ambientes distribuídos. Ela protege usuários por meio da inteligência contra ameaças global da Cisco, de recursos avançados de defesa e da proteção do usuário em roaming.

O Cloud Web Security oferece ferramentas intuitivas para criar, aplicar e monitorar a política de entrada e saída na Web, permitindo à empresa controle total sobre como os usuários finais acessam o conteúdo da Internet. Resumindo, o Cloud Web Security é um perímetro de segurança na nuvem. Ele fornece controle e execução abrangentes das políticas contextuais. Além de isso, o CWS também:

- Bloqueia ameaças de forma dinâmica e em tempo real
- Protege a rede e os usuários contra conteúdos indesejáveis da Web
- Otimiza os recursos de rede reduzindo o congestionamento da largura de banda
- Facilita a geração de relatórios e o monitoramento abrangentes das atividades on-line
- Protege a empresa contra o vazamentos de dados

O Cloud Web Security integra os firewalls, roteadores de filiais e o software do cliente da Cisco para disponibilizar proteção onde quer que seja o ambiente de trabalho dos usuários. Todo o tráfego é roteado por uma rede global de data centers, seja ele originado na matriz, nos escritórios das filiais ou por meio de usuários móveis ou remotos. O Cloud Web Security elimina o backhaul, acelera a implantação de segurança na Web e ajuda a maximizar o valor dos investimentos atuais na Cisco.

"Com as aquisições recentes das empresas de segurança Sourcefire e Cognitive Security, a Cisco agora pode oferecer uma versão aprimorada do Cloud Web Security para bloquear ameaças avançadas de malware, especialmente na fase “posterior” ao ciclo do ataque, além de melhorar a detecção de ameaças em tempo real “durante” um possível ataque. A Cisco oferece essa solução com a opção de assinatura Premium, descrita abaixo.

Cloud Web Security Premium

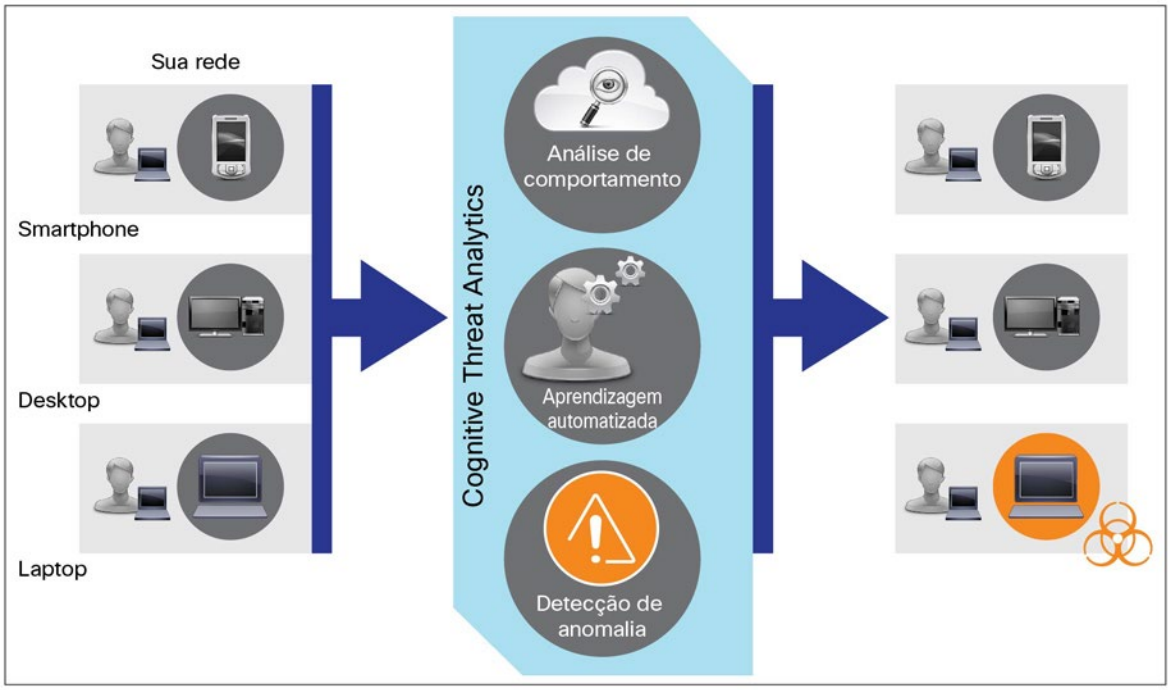
O pacote Premium do Cloud Web Security inclui todos os recursos do pacote Essentials, mas também incorpora dois sistemas de detecção de malware inovadores: o Cognitive Threat Analytics (CTA) e o Advanced Malware Protection (AMP). Esses sistemas automatizam a busca de ameaças de alto risco no tráfego da Web das empresas. O Cloud Web Security Premium oferece proteção point-in time adicional, segurança retrospectiva e análise contínua para ajudar as empresas a localizarem e abordarem as ameaças mais relevantes. Além disso, reduz o tempo para detecção de ameaças que já estão ativas em suas redes.

As equipes de segurança agora podem oferecer segurança contínua na Web para proteger os sistemas em todo o ciclo do ataque. Veja a seguir mais detalhes sobre esses dois sistemas de detecção de malware.

Cognitive Threat Analytics

O Cognitive Threat Analytics, ou CTA, desenvolvido pela empresa Cognitive Security, é um sistema de análise do comportamento da rede em tempo quase real. Ele usa estatísticas avançadas e aprendizagem automática para identificar atividades incomuns na rede: sintomas de uma rede infectada. A solução não depende de um conjunto de regras, ou seja, nenhuma intervenção humana é necessária para “ajustar” a tecnologia. Uma vez habilitado, o CTA começa imediatamente a procurar possíveis ameaças. Os dados são correlacionados na nuvem para aumentar a velocidade, a agilidade e a intensidade dos recursos de detecção de anomalias do CTA.

Figura 2. Visão geral do CTA



O CTA aprende com o que vê. Com o tempo, ele se adapta identificando novos canais de comando e controle não detectados anteriormente pelo setor de segurança. Ele avalia o comportamento dos usuários (por exemplo, usuários individuais) na rede e usa o modelo comportamental para prever como esses usuários devem agir. O CTA usa um modelo de longo prazo do comportamento da rede para correlacionar atividades aparentemente diferentes. Em seguida, ele compara esses dados correlacionados aos comportamentos dos usuários individuais em toda a rede daquele cliente específico para que possa detectar ameaças mais rapidamente.

Independentemente do que for a ameaça detectada, se houver uma discrepância significativa ou prolongada no comportamento esperado, o CTA irá sinalizá-la. As ações do CTA são como as de uma equipe de segurança tentando identificar um ladrão em uma loja antes que ele tenha a chance de roubá-la: o que essa pessoa está fazendo de diferente em relação aos outros consumidores? Está carregando uma sacola grande em vez de utilizar o carrinho de compras? Está tentando sair pela porta dos fundos em vez de pela porta da frente? Mesmo que o comportamento suspeito seja infundado, vale a pena investigar.

O CTA identifica anomalias e direciona os analistas de segurança para os possíveis problemas, ajudando a reduzir a carga de trabalho deles e a priorizar as ameaças. Ele também complementa a tecnologia atual de segurança da Cisco, tornando as soluções mais precisas e mais aptas a detectar comportamentos desconhecidos ou incomuns na rede. Os recursos de segurança da Cisco são, portanto, estendidos para a fase “posterior” ao ciclo do ataque. Acima de tudo, o CTA oferece um tipo segurança que evolui junto as constantes mudanças no cenário de ameaças à rede.

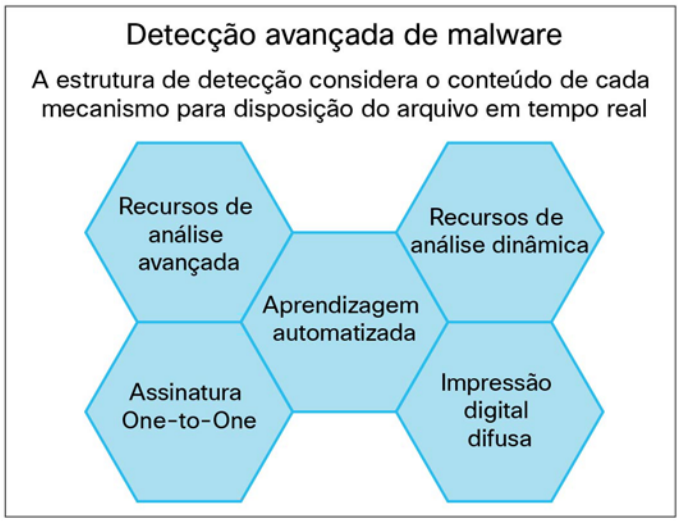
Advanced Malware Protection

O segundo sistema de detecção no Cloud Web Security Premium é o Advanced Malware Protection (AMP) da Sourcefire. O AMP não depende de assinaturas de malware, que podem levar semanas ou meses para serem criadas para cada nova amostra de malware. Em vez disso, ele usa uma combinação de reputação, sandbox e análise retrospectiva do arquivo para identificar e bloquear ameaças em todo o ciclo do ataque.

Reputação de arquivos

A reputação do arquivo é a capacidade de analisar os bancos de dados de arquivos para determinar se um arquivo é “limpo”, reconhecidamente um malware ou desconhecido. O AMP “captura uma impressão digital” de cada arquivo, à medida que ele passa pelo serviço Cloud Web Security e consulta a rede de inteligência em nuvem coletiva da Cisco e da Sourcefire para obter um parecer sobre a reputação ou uma “pontuação”. Com os resultados, o AMP poderá bloquear automaticamente os arquivos mal-intencionados e aplicar políticas definidas pelo administrador. A Figura 3 mostra os diferentes mecanismos que funcionam em tempo real para detectar malwares avançados e determinar a reputação do arquivo.

Figura 3. Advanced Malware Protection



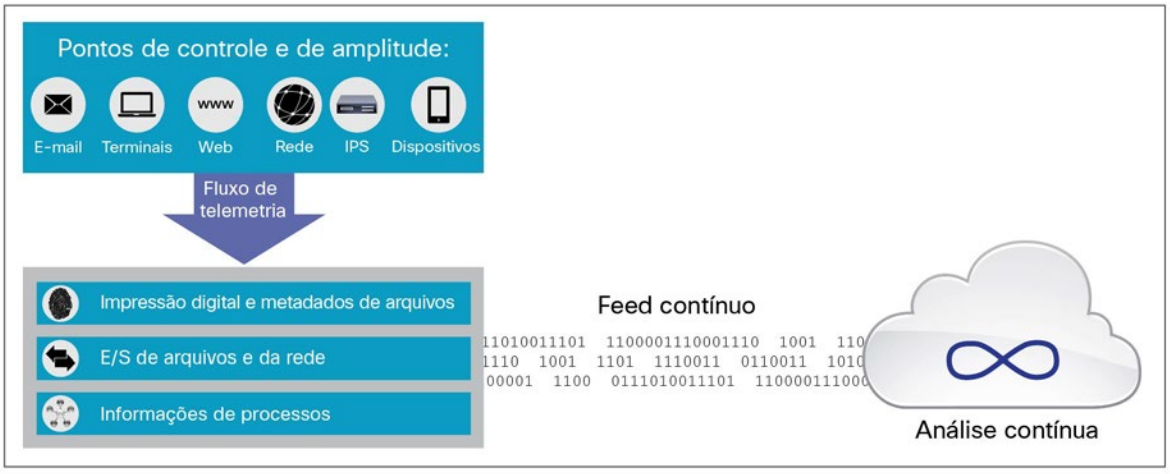
Sandbox de arquivos

O sandbox de arquivos é um recurso fundamental do AMP e, no fim das contas, do Cloud Web Security Premium também. Com o sandbox de arquivos, o AMP analisa os arquivos desconhecidos que passam pela rede. Em um ambiente de sandbox altamente seguro, o AMP reúne detalhes precisos sobre o comportamento de um arquivo e combina esses dados com a análise detalhada manual e automática para determinar o nível de ameaça do arquivo. Essa informação é então alimentada na rede de inteligência em nuvem coletiva da Cisco e da Sourcefire e usada para atualizar dinamicamente o conjunto de dados em nuvem do AMP. O relatório ativo permite que as equipes de segurança visualizem relatórios de fácil leitura e com dados completos sobre os arquivos analisados.

Retrospecção de arquivos

Talvez o aspecto mais importante do AMP consista nos seus recursos de análise retrospectiva, que proporcionam às empresas a capacidade de “voltar no tempo” para localizar a ocorrência de ataques e, em seguida, avaliar os danos. A retrospecção de arquivo oferece a análise contínua de arquivos que passaram pelo gateway de segurança, usando as atualizações em tempo real da Cisco e a rede de inteligência em nuvem da Sourcefire.

Figura 4. Processo de análise retrospectiva do AMP

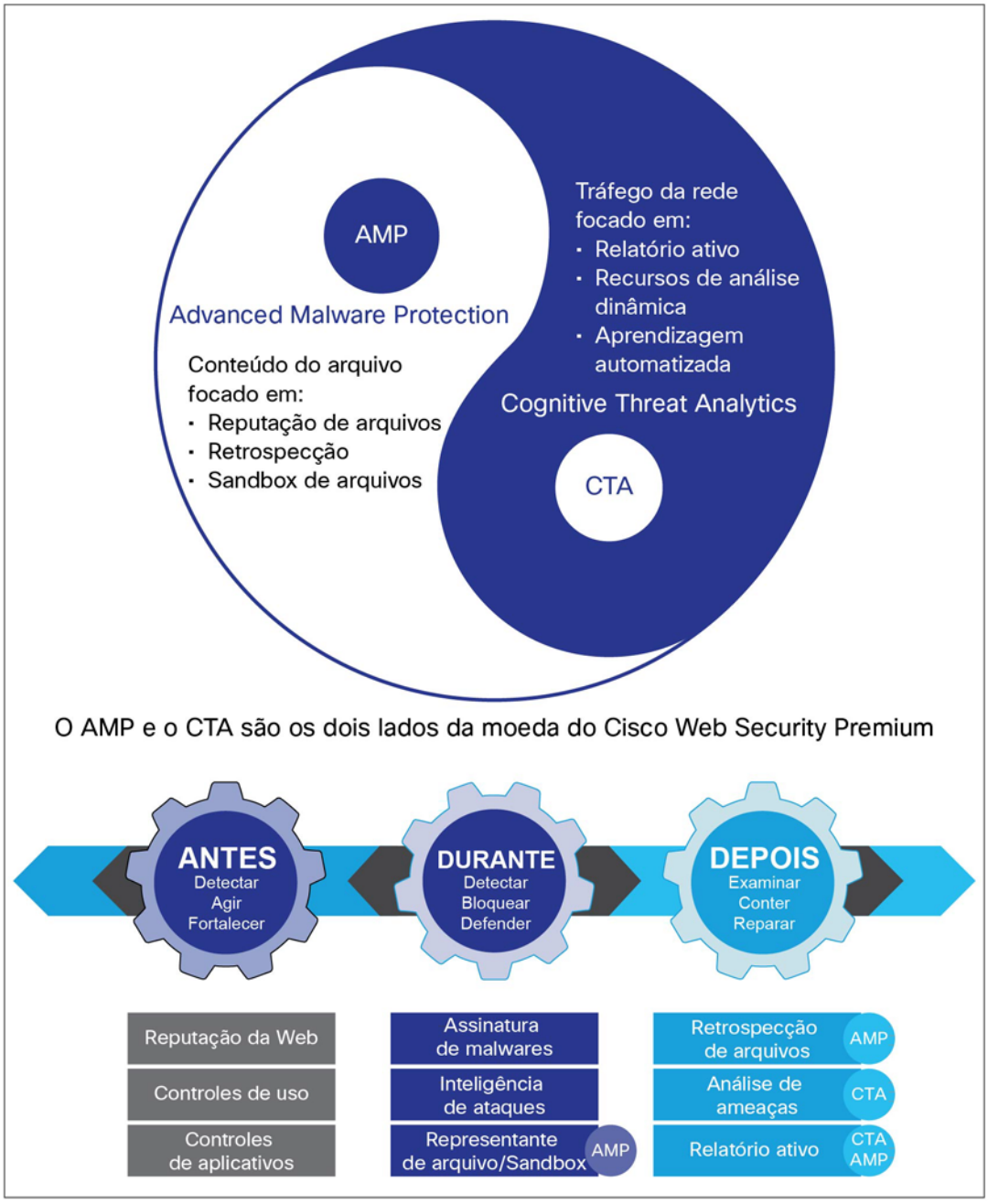


Às vezes, a análise retrospectiva revela que um arquivo considerado “limpo” quando passou pelas proteções de perímetro é, na realidade, um malware avançado bem disfarçado. O AMP alertará imediatamente o administrador de segurança e identificará qual usuário da rede pode ter sido contaminado e quando isso ocorreu. As equipes de segurança podem assim conter o ataque com rapidez, antes que haja chance de disseminação.

Conclusão

O Cloud Web Security Premium com CTA e AMP está alinhado à estratégia da Cisco de ajudar as empresas a enfrentarem os desafios de segurança conhecidos e novos. Ele ajuda a detectar, entender e deter as ameaças. A análise contínua e a inteligência de segurança em tempo real são oferecidas pela nuvem e compartilhadas em todas as soluções de segurança para aumentar a eficiência. A combinação dessas três soluções ajuda as empresas a identificarem novos canais de comando e controle não detectados anteriormente pelo setor de segurança, e a enfrentarem os desafios em todas os ciclos do ataque.

Figura 5. Cloud Web Security com AMP e CTA: segurança durante o ciclo de ataque



Antes: descobrir, agir, dificultar

O Cloud Web Security Premium oferece reputação da Web, controles de uso, controles de aplicações (que incluem as de microaplicações), assinaturas de malware e informações sobre ataques para oferecer segurança antes e durante um ataque.

Durante: detectar, bloquear e defender

O AMP aumenta a segurança na fase “durante” do ciclo do ataque com a reputação de arquivo e recursos de sandbox de arquivos. Ele bloqueia automaticamente arquivos mal-intencionados e aplica as políticas definidas pelo administrador, de acordo com a reputação conhecida de um arquivo. Ele também analisa de acordo os arquivos desconhecidos que passam pela rede e atualiza as informações sobre ameaças. Esses recursos ajudam os analistas de segurança a priorizarem as ameaças a serem investigadas.

Depois: abranger, conter, corrigir

O CTA e o AMP permitem a análise e a correção contínuas na crítica fase “posterior” ao ciclo do ataque. O CTA oferece a análise do comportamento da rede em tempo real para ajudar a identificar algum comportamento anormal na rede. Enquanto isso, a retrospecção do arquivo do AMP aborda o problema de arquivos mal-intencionados que passam pelas defesas de perímetro. Os recursos de relatório ativos do AMP oferecem visibilidade em relação à reputação e ao comportamento dos arquivos que entraram na rede. As equipes de segurança podem identificar e avaliar mais facilmente a abrangência do ataque e corrigi-lo com rapidez.

A aprendizagem automática que ocorre com o CTA e o AMP na fase “posterior” é utilizada, então, para aprimorar os recursos de detecção em tempo quase real que o Cloud Web Security Premium aplica durante um ataque.

Para obter mais informações

Para saber mais sobre o Cisco Cloud Web Security Essentials e o Cloud Web Security Premium, acesse http://www.cisco.com/go/cws.

Para obter mais informações sobre o CTA, acesse http://www.cisco.com/go/cognitive.

Para obter mais detalhes sobre o AMP, acessehttp://www.cisco.com/go/amp.

Sede - América
Cisco Systems. Inc.
San Jose. CA

Sede - Ásia e Pacífico
Cisco Systems (USA) Pte. Ltda.
Cingapura

Sede - Europa
Cisco Systems International BV Amsterdam.
Países Baixos

A Cisco possui mais de 200 escritórios no mundo todo. Os endereços, números de telefones e fax estão disponíveis no site **www.cisco.com/go/offices**.

Impresso nos Estados Unidos C11-734836-00 06/15