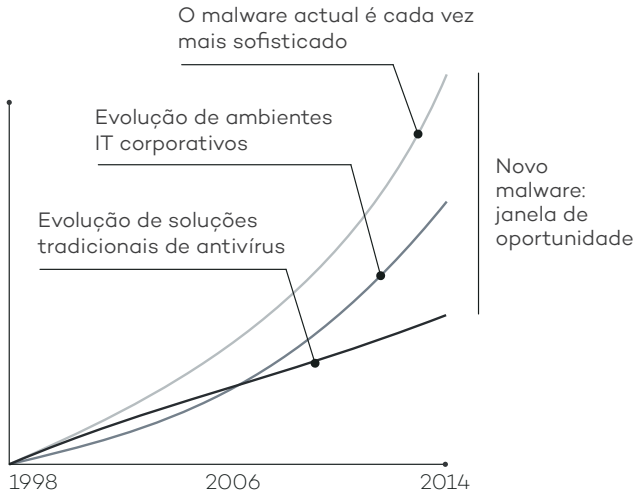
Adaptive Defense 360

Visibilidade Ilimitada, Controle Absoluto

DEFESA COMPLETA DE ENDPOINTS INTEGRANDO PROTEÇÃO, DETECÇÃO, RESPOSTA E REPARAÇÃO NUMA SÓ SOLUÇÃO

Defender os endpoints de ataques é difícil. A proteção deve incluir uma grande variedade de defesas, incluindo antivírus/anti-malware tradicionais, firewall pessoal, filtros de e-mail e internet e controle de dispositivos. Além disso, qualquer defesa deve fornecer salvaguardas adicionais contra ataques direcionados e de dia-zero difíceis de detectar. Até agora, o departamento de IT precisou de comprar e fazer a manutenção de vários produtos diferentes de fornecedores diferentes para defender o endpoint.

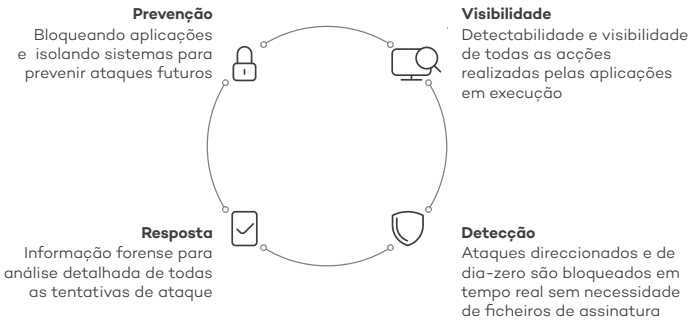
O Adaptive Defense 360 é o primeiro e único produto a oferecer uma combinação das funcionalidades de Protecção de Endpoints (EPP) e Detecção e Resposta de Endpoints (EDR) numa só solução. O Adaptive Defense 360 também automatiza funcionalidades reduzindo a carga de trabalho do departamento de IT. O Adaptive Defense 360 começa com a melhor solução EPP da Panda que inclui segurança simples e centralizada, soluções de reparação, monitorização e relatórios em tempo real, proteção baseada no perfil, controle de dispositivos centralizado, monitoramento e filtragem Web.



No entanto, esse é apenas o início. O malware e o ambiente de segurança IT sofreram mudanças decisivas tanto em termos de volume como de sofisticação. Com mais de 200.000 novos vírus surgindo diariamente e com o aumento da sofisticação das técnicas para penetrar defesas e esconder malware, as redes corporativas estão mais vulneráveis do que nunca a ataques direcionados e de dia-zero.

Soluções de Protecção de Endpoints tradicionais são eficientes no bloqueio de malware conhecido usando técnicas de detecção baseadas em ficheiros de assinatura e algoritmos heurísticos. No entanto, não há defesa contra ataques direccionados e de dia-zero, que se aproveitam da "janela de oportunidade para malware", o espaço de tempo entre o aparecimento de novo malware e a emissão do antídoto por parte de empresas de segurança. Há um espaço crescente que é explorado pelos hackers para colocarem vírus, ransomware, trojans e outros tipos de malware em redes corporativas. Estas ameaças cada vez mais comuns conseguem encriptar documentos confidenciais e exigir um resgate ou apenas extrair dados sensíveis para espionagem industrial.

O Adaptive Defense é a solução da Panda para este tipo de ataques. O Adaptive Defense fornece um serviço EDR que consegue classificar com precisão todas as aplicações em execução numa organização, apenas permitindo que sejam executados os programas legítimos. As funcionalidades EDR do Panda Adaptive Defense 360 contam com um modelo de segurança baseado em três princípios: monitorização contínua de aplicações nos computadores e servidores de uma empresa, classificação automática com utilização de machine learning na nossa plataforma Big Data na cloud e, finalmente, como opção, os nossos técnicos especialistas analisam essas aplicações que não foram classificadas automaticamente, de forma a terem a certeza do comportamento de tudo o que opera nos sistemas da empresa.



Estas funcionalidades estão agora combinadas com a melhor solução EPP da Panda, fechando o ciclo da protecção adaptativa de malware, que agora inclui prevenção, detecção, análise forense e reparação automatizadas.

A única solução que garante a segurança de todas as aplicações em utilização

PROTECÇÃO ROBUSTA E COMPLETA

O Panda Adaptive Defense 360 oferece dois modos de funcionamento:

- O modo **Standard** permite executar todas as aplicações classificadas como goodware e todas as aplicações que ainda não foram validadas pelo sistema automático da Panda Security.
- O modo **Extended** permite unicamente a execução de goodware. Esta é a fórmula ideal para empresas conseguirem máxima segurança sem qualquer risco associado.

INFORMAÇÃO FORENSE

- Gráficos com a execução de eventos fornecem uma perspectiva mais clara sobre os eventos causados por malware.
- Obtenha informação visual através de mapas geográficos com as zonas mais afetadas por malware, ficheiros criados e muito mais.
- Identifique software instalado na sua rede que contenha vulnerabilidades já conhecidas.

PROTEÇÃO PARA SISTEMAS OPERATIVOS E APLICAÇÕES VULNERÁVEIS

Sistemas como o Windows XP, já descontinuados pelo fabricante e aos quais não são feitas atualizações, são o alvo preferencial para ataques de dia-zero e de next-generation

Além disso, vulnerabilidades em aplicações como Java, Adobe, Microsoft Office e browsers são aproveitadas por 90% dos malwares.

O módulo de proteção contra vulnerabilidades do Adaptive Defense 360 utiliza regras contextuais e comportamentais que asseguram às empresas o nível de segurança mesmo quando os sistemas operativos não se encontram atualizados.

FUNCIONALIDADES EPP TOTAIS

O Adaptive Defense 360 integra o Panda Endpoint Protection Plus, a mais sofisticada solução EPP da Panda Security, e que fornece funcionalidades EPP completas, incluindo:

- Ações de reparação
- Controle de dispositivos centralizado: previne a entrada de malware e a perda de dados ao bloquear tipos de dispositivos
- Monitoramento e filtragem Web
- Antivírus e anti-spam para servidores exchange
- Firewall para endpoints, e muitas outras...

INFORMAÇÃO CONTÍNUA SOBRE O ESTADO DE TODOS OS TERMINAIS DA REDE

Obtenha alertas imediatos no momento em que o malware é identificado na rede, com relatórios intuitivos que identificam a origem das ameaças, os equipamentos infectados e as ações realizada por estes códigos maliciosos.

Receba relatórios via e-mail sobre a atividade diária de todo o serviço.

INTEGRAÇÃO SIEM

O Adaptive Defense 360 pode ser integrado com soluções SIEM que fornecem informação detalhada sobre a atividade de todas as aplicações ativas no sistema operativo.

Para clientes sem SIEM, o Adaptive Defense 360 pode incluir o seu próprio sistema para armazenamento e gestão de eventos de segurança e respectiva análise em tempo real.

SERVIÇO 100% GERIDO

Esqueça a necessidade de investimento em pessoal técnico especializado para lidar com ficheiros suspeitos ou em quarentena e desinfecção e restauro de sistemas infectados. O Adaptive Defense 360 classifica todas as aplicações automaticamente graças ao processo machine learning nos nossos ambientes Big Data sob supervisão contínua dos especialistas da PandaLabs.

REQUISITOS TÉCNICOS

Console Web

- Conexão à internet
- Internet Explorer 10
- Microsoft Edge
- Firefox (última versão)
- Google Chrome (última versão)

Agente

- Sistemas operativos (postos de trabalho): Windows XP SP2 e posteriores (Vista, Windows 7, 8, 8.1 e 10)
- Sistemas operativos (servidores): Windows Server 2003 / 2008 / 2012 / 2016
- Conexão à Internet (direta ou através de uma proxy)

Parcialmente suportado (apenas EPP):

- Linux, MAC OS X e Android

www.fcbrasil.com.br
(21) 4063-7703
(21) 4063-4840
(21) 4003-8776
vendas@fcbrasil.com.br