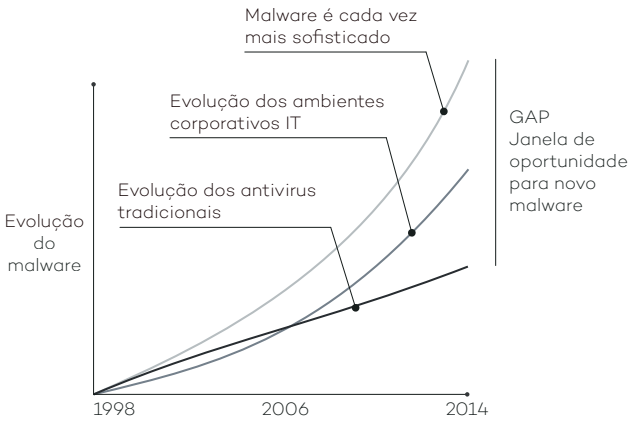
Adaptive Defense

Feche a janela de oportunidade das ameaças direcionadas

A SUA REDE ESTÁ PROTEGIDA CONTRA ATAQUES DIRECCIONADOS OU DE "DIA ZERO"?

O panorama do malware e segurança informática sofreu grandes mudanças em termos de volume e sofisticação. Registou um aumento exponencial no número de vírus em circulação (cerca de 300.000 novos vírus por dia), e novas técnicas para passar a defesa das redes. Esconder malware e permitir que estas aplicações maliciosas permaneçam nos sistemas por longos períodos de tempo, é o novo objectivo.



Em paralelo os ambientes corporativos tornaram-se mais complexos, tornando a gestão mais difícil e os sistemas mais vulneráveis.

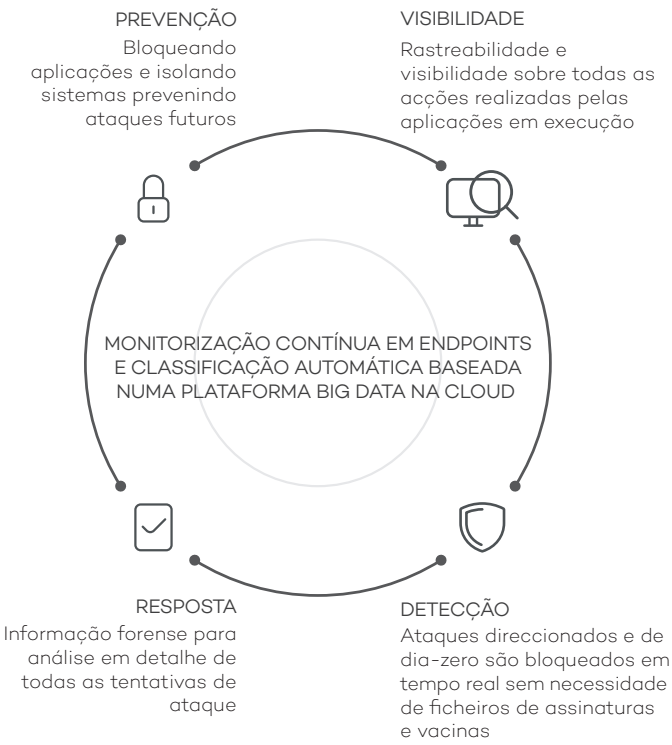
Ainda assim, os sistemas de antivírus tradicionais estão um passo atrás da realidade. A sua evolução linear continua a basear-se em detecções reactivas e as suas técnicas de detecção assentam em algoritmos e sistemas de heurística. Isto resulta por vezes em falta de precisão na detecção fazendo com que algum malware passe despercebido ou em alguns casos sejam gerados falsos positivos.

Esta discrepância gera o que é apelidado de janela de oportunidade para malware: o período de tempo entre o aparecimento de um novo vírus e o lançamento de uma vacina por parte das empresas de segurança. Esta diferença temporal é aproveitada por hackers para lançar novos vírus, ransomware, trojans e outro tipo de malware para as redes corporativas. Estas novas ameaças podem encriptar redes inteiras e pedir resgaste pelos dados cifrados. Em alternativa podem simplesmente recolher informação sensível com o propósito de espionagem industrial.

Governos, banca e outras grandes organizações sofrem com estes tipo de ataques que os antivírus tradicionais não têm capacidade para lidar em tempo útil. Pesquisas internas realizadas sobre milhões de assinaturas e sobre as melhores soluções antivírus, revelam que 18% do malware não é detectado nas primeiras 24horas depois de ser lançado e mesmo após 3 meses 2% deste malware continua por detectar.

A solução para esta situação é o **Adaptive Defense**: um serviço que classifica todas as aplicações que são executadas num determinado ambiente e onde só são autorizados programas legítimos.

Este é o resultado de 5 anos de desenvolvimento de um novo **modelo de segurança** baseado em 3 princípios: monitorização contínua de aplicações em endpoints e servidores, classificação automática inteligente baseada numa plataforma Big Data na Cloud e finalmente numa equipa técnica especializada e focada na análise de aplicações que não foram classificadas automaticamente, certificando-se do comportamento de tudo o que é executado nestes ambientes.



A ÚNICA SOLUÇÃO QUE GARANTE A SEGURANÇA DE TODAS AS APLICAÇÕES EM EXECUÇÃO

GARANTIA DE PROTECÇÃO ROBUSTA A COMPLETA

O Panda Adaptive Defense oferece dois modos de funcionamento:

- Modo **Standard** permite executar todas as aplicações classificadas como goodware e todas as restantes ainda por validar pelo sistema automático da Panda Security.
- No modo **Extended** é permitida unicamente a execução de goodware. Esta é a fórmula ideal para as empresas conseguirem máxima segurança sem qualquer risco associado.

INFORMAÇÃO FORENSE

- Gráficos com a execução de eventos fornecem uma perspetiva mais clara sobre eventos causados por malware.
- Obtenha informação visual através de mapas geográficos com as zonas mais afectadas por malware.
- Identifique software instalado na sua rede que contenha vulnerabilidades já conhecidas.

COMPATIVEL COM SOLUÇÕES ANTIVIRUS TRADICIONAIS

O **Adaptive Defense** pode coexistir com os antivírus tradicionais e assumir a função de ferramenta corporativa capaz de bloquear todos os tipos de malware, incluindo ataques direccionados e de dia-zero que as soluções tradicionais não conseguem detectar.

PROTECÇÃO CONTRA VULNERABILIDADES DE SISTEMAS OPERATIVOS E OUTRAS APLICAÇÕES

Sistemas como o Windows XP, já descontinuados pelo fabricante, estão sem actualizações e portanto são o alvo preferencial para novos ataques de dia-zero e outros.

Para além disso, vulnerabilidades em aplicações como o Java, Adobe, Microsoft Office e browser são aproveitadas por mais de 90% de todo o malware.

O módulo de protecção contra vulnerabilidades do Adaptive Defense utiliza regras comportamentais e de contexto que asseguram às empresas o nível de segurança desejado e que permite execução das operações com total protecção mesmo que as diferentes aplicações não disponham das mais recentes actualizações.

INFORMAÇÃO CONTÍNUA SOBRE O ESTADO DA REDE

- Obtenha alertas imediatos no momento que o malware é detectado com relatórios intuitivos que identificam a origem das ameaças, os equipamentos afectados e as diferentes acções executadas por estes códigos maliciosos.
- Receba relatórios via e-mail com o resumo diário de todo o serviço.

INCLUI SIEM

O Adaptive Defense integra com soluções SIEM que providenciam informação detalhada sobre a actividade de todas as aplicações a correr no sistema operativo.

Para cliente sem SIEM, o Adaptive Defense inclui o seu próprio sistema para armazenamento e gestão de eventos e respectiva análise em tempo real.

SERVIÇO 100% GERIDO

Esqueça a necessidade de investimento em pessoal técnico para lidar com ficheiros suspeitos ou em quarentena e restauro de sistemas infectados. O Adaptive Defense classifica todas as aplicações automaticamente graças a um sistema que verifica em tempo real todos os processos em execução.

REQUISITOS TÉCNICOS

Consola Web

- Ligação à Internet
- Internet Explorer 7.0 ou superior
- Firefox 3.0 ou superior
- Google Chrome 2.0 ou superior

Agente

- Sistemas operativos para postos de trabalho: Windows XP SP2 ou superior (Vista, Windows 7, 8 e 8.1)
- Sistemas operativos de servidor: Windows Server 2003, 2008 e 2012
- Ligação à Internet