ESTUDO DE CASO: TI DA AKAMAI

POR QUE A AKAMAI USA O **ENTERPRISE THREAT PROTECTOR**

ÍNDICE

RESUMO EXECUTIVO

Em março de 2017, a TI da Akamai implantou o Enterprise Threat Protector em suas redes corporativas com e sem fios.

Durante o período de março a maio, o Enterprise Threat Protector forneceu benefícios significativos e mensuráveis.

Eles incluem:

- Uma grande redução no volume de incidentes de malware identificados pela solução de proteção de ponto de extremidade existente: uma **redução de 54%** de março a abril e uma **redução de 37%** de março e maio.
- Uma redução no volume de eventos gerados pela solução de detecção avançada existente — uma **redução de 30%** de março a abril e uma **redução de 15%** de março a maio.
- Uma economia de tempo equivalente a **0,75 de um funcionário em tempo integral** (FTE) devido à redução de incidentes e alertas das soluções de detecção avançada e de ponto de extremidade existentes.

PROTEÇÃO DE PONTO DE EXTREMIDADE

A solução de proteção de ponto de extremidade que a Akamai implantou inclui recursos de detecção de malware e de prevenção contra invasão.

Incidentes de infecção por malware

As métricas de malware foram filtradas para excluir alertas de "adware" e de "softwares potencialmente indesejados", e concentram-se principalmente nas infecções por malware. O resultado obtido com a implantação do Enterprise Threat Protector foi uma redução de 54% na quantidade de incidentes de infecção por malware identificados de março (199) a abril (92), além de uma redução de 37% de março a maio (125).

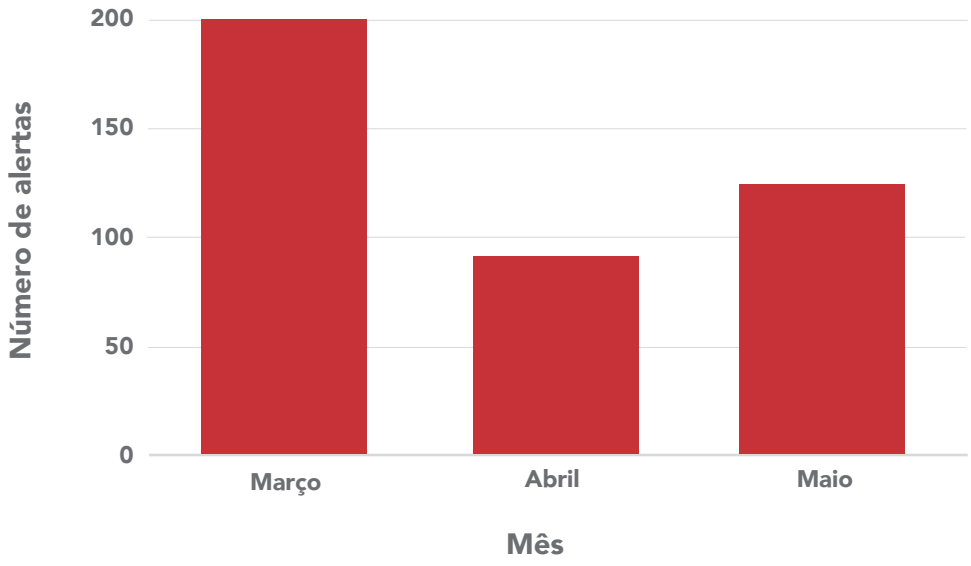

Figura 1 - Redução de incidentes por malware com a implantação do Enterprise Threat Protector

Alertas do Sistema de Prevenção Contra Invasão (IPS)

O número de alertas gerados pelo IPS de ponto de extremidade teve uma queda semelhante. A maioria dos alertas gerados veio em forma de torrents, mas houve uma diminuição considerável entre março e abril, seguido por mais uma redução em maio.

Figura 2 - Redução dos alertas do IPS (incluindo torrents) com o Enterprise Threat Protector implantado

A remoção completa de torrents dos alertas demonstra ainda uma redução significativa (27%) de março a abril e uma diminuição de aproximadamente 35% de março a maio.

Figura 3 - Redução dos alertas do IPS (excluindo torrents) com a implantação do Enterprise Threat Protector

Excluindo os torrents, o próximo número mais alto de alertas gerados pelo IPS foi para website, domínio ou URL malicioso, seguido de perto por ataque por Web e ataque por página da Web de verificação falsa.

Alerta	Alertas de março	Alertas de abril	Alertas de maio
Website, domínio ou URL malicioso	13	1	1
Ataque por Web e ataque por página da Web de verificação falsa	12	4	1

Tabela 1 - Redução nos Alertas de IPS com a implantação do Enterprise Threat Protector

DETECÇÃO AVANÇADA

A solução de detecção avançada que a Akamai implantou é um mecanismo de defesa complementar que fornece uma camada adicional de segurança. O número de alertas produzidos por esta solução é menor em volume, mas os alertas gerados por esta solução são muito mais significativos.

Como pode ser observado na Figura 4, o número de alertas gerados por esta solução também sofreu uma redução após a implantação do Enterprise Threat Protector.

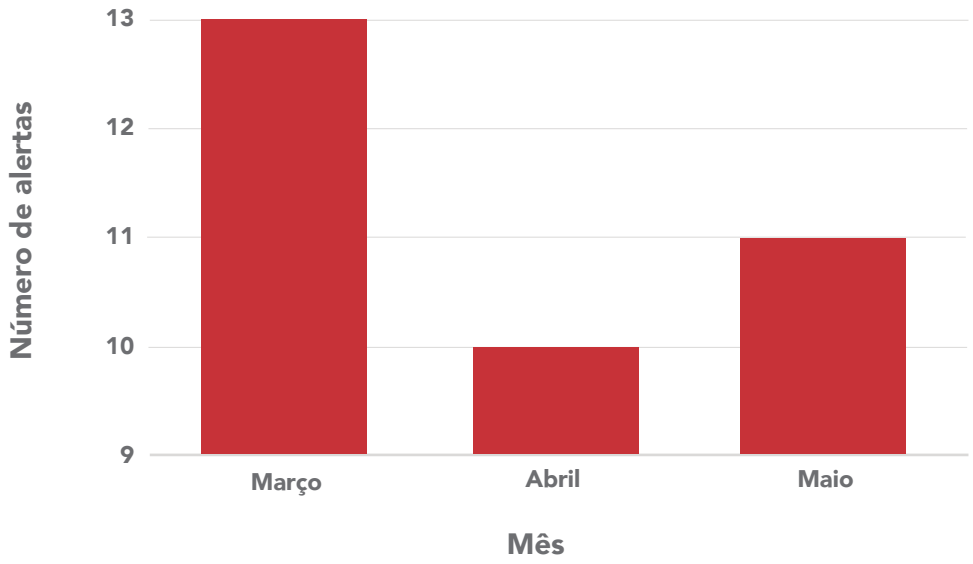

Figura 4 - Redução nos alertas de detecção antecipada com a implantação do Enterprise Threat Protector

ROI

Embora a redução na contagem de incidentes e alertas com a implantação do Enterprise Threat Protector seja evidente, o valor real parece estar no tempo economizado.

O "tempo economizado" foi calculado usando uma estimativa de tempo médio de resposta, o tempo de correção para incidentes de malware e o tempo para remover o software de torrent. Todas essas atividades são tarefas operacionais padrão a cada mês. Observe que houve também uma redução no número de torrents.

Mês	Contagem de usuários	IPs de torrent bloqueados
Março	56	2.089
Abril	48	1.100
Maio	40	1.546

Tabela 2 - Alertas do módulo do IPS

Para investigações de malware, foi utilizado um tempo calculado gasto por incidente para avaliação, resposta e correções.

Utilizando essas métricas, houve uma economia de tempo de aproximadamente **0,75 de um funcionário em tempo integral** (FTE) por mês com a implantação do Enterprise Threat Protector.

Combinando os módulos do IPS e de detecção de malware da proteção de ponto de extremidade, um tempo de resposta médio entre abril e junho foi calculado e comparado em relação ao mês de março anterior à implantação do Enterprise Threat Protector.

Os resultados foram:

- Uma economia estimada de **27 horas** no **módulo de detecção de malware**
- Uma economia estimada de **8 horas** no **módulo do IPS para resposta** a incidentes

Tempo de resposta economizado (em horas)	
Módulo de detecção de malware	27
Módulo do IPS	8
Total	**35**

Tabela 3 - Módulos de malware e IPS Alertas (economia no tempo de resposta com o Enterprise Threat Protector implantado)

Da mesma forma, levando em conta o tempo médio de correção por incidente mediante a resposta inicial, uma estimativa de **51 horas** do **módulo de detecção de malware** do ponto de extremidade e **24 horas** da hora/mês do analista no **módulo do IPS** foram economizadas.

Tempo de correção economizado (em horas)	
Módulo de detecção de malware	51
Módulo do IPS	24
Total	**75**

Tabela 4 - Módulos de malware e IPS Alertas (economia no tempo de correção com o Enterprise Threat Protector implantado)

Em geral, estima-se que aproximadamente **110 horas** foram economizadas por mês com a implantação do Enterprise Threat Protector.