CASO REAL: EQUIPO DE TI DE AKAMAI

POR QUÉ AKAMAI UTILIZA **ENTERPRISE THREAT PROTECTOR**

TABLA DE CONTENIDO

RESUMEN EJECUTIVO

En marzo de 2017, el equipo de TI de Akamai implementó Enterprise Threat Protector en la red inalámbrica y cableada corporativa de Akamai.

Durante el periodo comprendido entre marzo y mayo, Enterprise Threat Protector proporcionó importantes beneficios cuantificables.

Se incluyen los siguientes:

- Una gran disminución del volumen de incidentes de malware identificados por la anterior solución de protección de puntos finales: una **reducción del 54 %** en el periodo comprendido entre marzo y abril, y una **reducción del 37 %** desde marzo hasta mayo.
- Una disminución del volumen de eventos generados por la anterior solución de detección avanzada: una **reducción del 30 %** de marzo a abril y una **reducción del 15 %** desde marzo hasta mayo.
- Un ahorro de tiempo equivalente a **0,75 empleados a tiempo completo** debido a la disminución de incidentes y alertas con respecto a las anteriores soluciones de puntos finales y detección avanzada.

PROTECCIÓN DE PUNTOS FINALES

La solución de protección de puntos finales que Akamai ha implementado incluye capacidades de detección de malware y prevención de intrusiones.

Incidentes de infección por malware

Se filtraron las métricas de malware con el fin de excluir las alertas de "adware" y "software potencialmente no deseado" y poder centrarse principalmente en las infecciones por malware. El resultado, tras la implementación de Enterprise Threat Protector, fue una disminución del 54 % en el número de incidentes de infección por malware identificados desde marzo (199) hasta abril (92), y una reducción del 37 % de marzo a mayo (125).

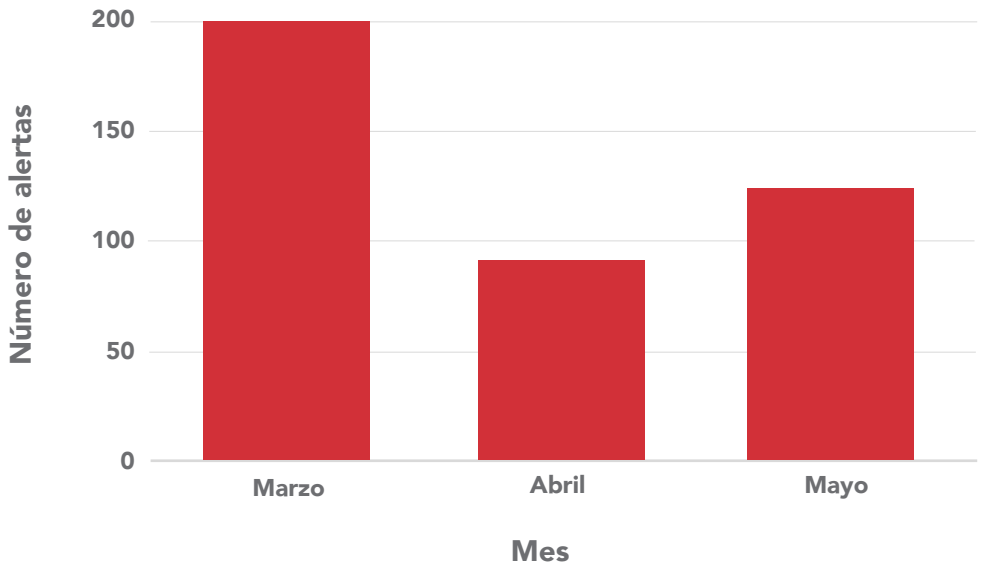

Figura 1: Reducción del número de incidentes de malware con la implementación de Enterprise Threat Protector

Alertas del sistema de prevención de intrusos (IPS)

El número de alertas generadas por el IPS de punto final mostró un descenso similar. La mayoría de las alertas generadas llegó en forma de torrents, pero hubo una notable disminución de marzo a abril y, a continuación, de nuevo, hasta mayo.

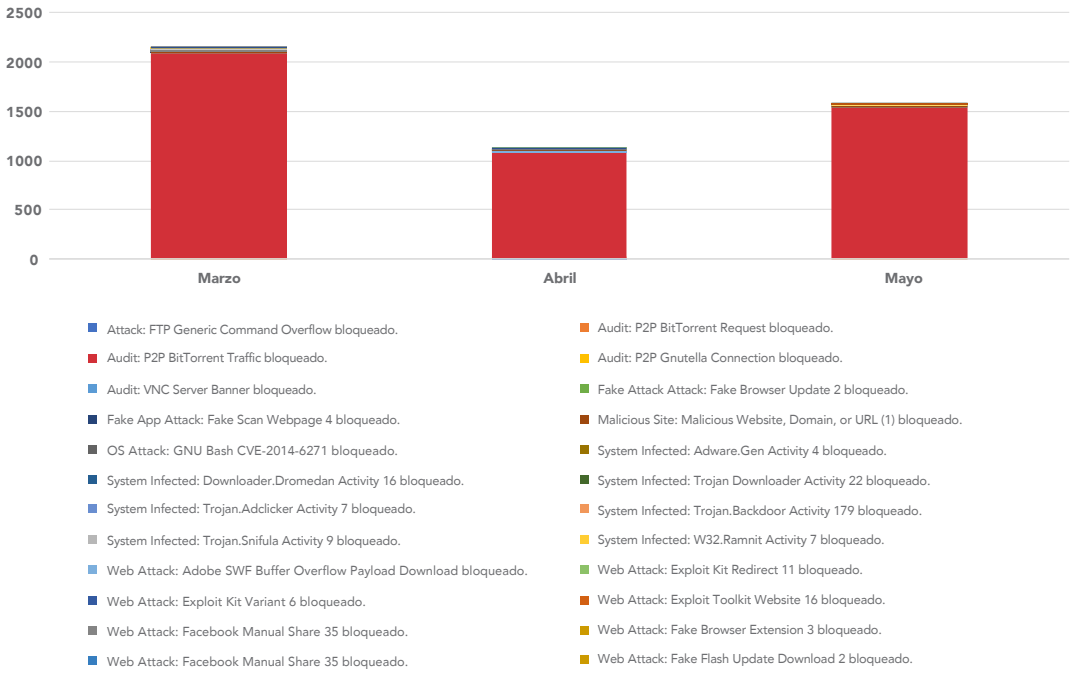

Figura 2: Reducción del número de alertas de IPS (incluidos los torrents) con la implementación de Enterprise Threat Protector

Al extraer por completo los torrents de las alertas, todavía se muestra una reducción considerable (27 %) de marzo a abril y una disminución de, aproximadamente, el 35 % de marzo a mayo.

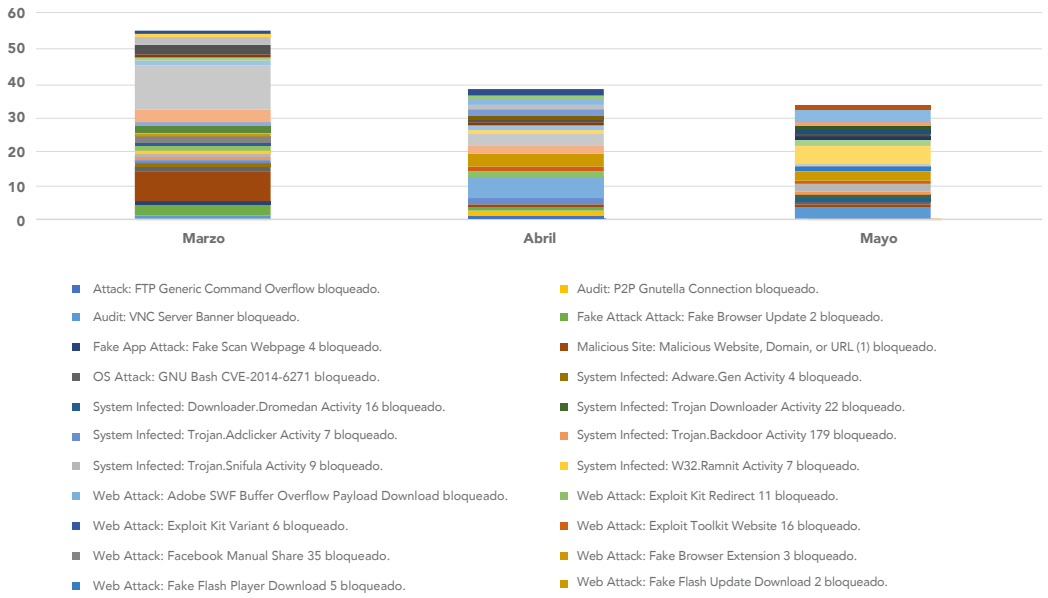

Figura 3: Reducción del número de alertas de IPS (excluidos los torrents) con la implementación de Enterprise Threat Protector

Si se excluyen los torrents, el siguiente número más alto de alertas generadas por el IPS corresponde a sitios web, dominios o URL maliciosos, seguidos de cerca por ataques web y ataques de páginas web de análisis falsos.

Alerta	Alertas de marzo	Alertas de abril	Alertas de mayo
Sitio web, dominio o URL maliciosos	13	1	1
Ataque web y ataque de página web de análisis falso	12	4	1

Tabla 1: Reducción del número de alertas de IPS con la implementación de Enterprise Threat Protector

DETECCIÓN AVANZADA

La solución de detección avanzada que ha implementado Akamai es un mecanismo de defensa complementario que proporciona una capa adicional de seguridad. El número de alertas generadas por esta solución tiene un volumen menor, pero las alertas generadas son mucho más significativas.

Como se puede observar en la figura 4, el número de alertas generadas por esta solución también disminuyó tras la implementación de Enterprise Threat Protector.

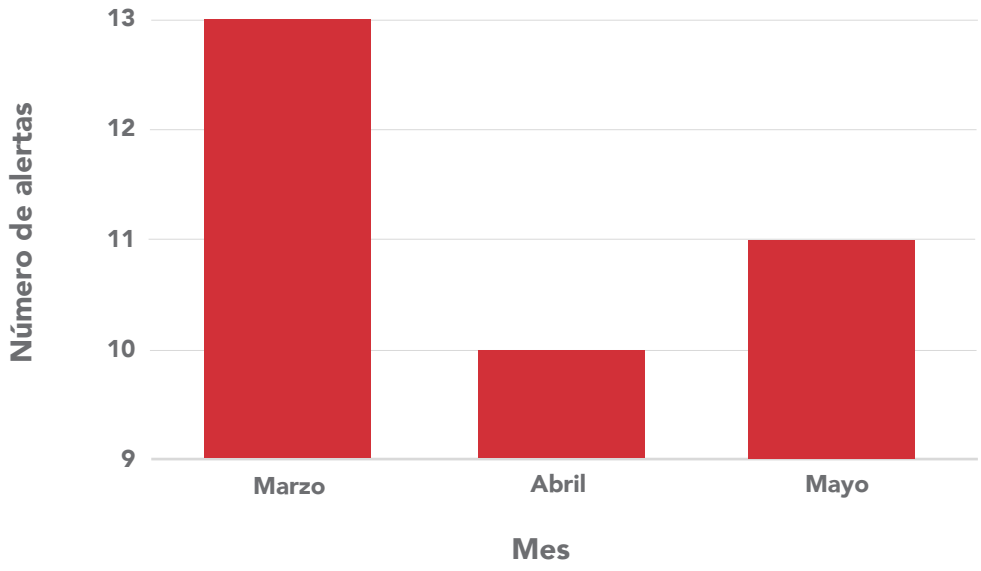

Figura 4: Reducción del número de alertas de detección avanzada con la implementación de Enterprise Threat Protector

RETORNO DE LA INVERSIÓN

Aunque la reducción del número de incidentes y alertas con la implementación de Enterprise Threat Protector es evidente, su valor real parece ser el tiempo ahorrado.

El "tiempo ahorrado" se calculó utilizando una estimación del tiempo medio de respuesta, el tiempo de corrección de incidentes de malware y el tiempo de eliminación del software de torrents. Todas estas actividades son tareas operativas estándar mensuales. Hay que tener en cuenta que también hubo una disminución en el número de torrents.

Mes	Número de usuarios	IP de torrents bloqueadas
Marzo	56	2089
Abril	48	1100
Mayo	40	1546

Tabla 2: Alertas del módulo de IPS

Para realizar el estudio sobre malware, se utilizó un cálculo del tiempo empleado en investigar, responder y corregir cada incidente.

Mediante el uso de estas métricas, la implementación de Enterprise Threat Protector registró un ahorro de tiempo equivalente a, aproximadamente, **0,75 empleados a tiempo completo** al mes.

Al combinar los módulos de malware e IPS del sistema de protección de puntos finales, se calculó un tiempo medio de respuesta entre abril y junio, y se comparó con el mes de marzo, antes de implementar Enterprise Threat Protector.

Los resultados fueron los siguientes:

- Un ahorro estimado de **27 horas** en el **módulo de detección de malware.**
- Un ahorro estimado de **8 horas** en el **módulo de IPS para la respuesta** a incidentes.

Ahorro de tiempo de respuesta (en horas)	
Módulo de malware	27
Módulo de IPS	8
Total	**35**

Tabla 3: Alertas del módulo de malware e IPS (ahorro en el tiempo de respuesta con la implementación de Enterprise Threat Protector)

Del mismo modo, teniendo en cuenta el tiempo medio de corrección por incidente tras la respuesta inicial, se calcula un ahorro de **51 horas** en el **módulo de malware** de punto final y **24 horas** de tiempo de análisis al mes en el **módulo de IPS**.

Ahorro de tiempo de corrección (en horas)	
Módulo de malware	51
Módulo de IPS	24
Total	**75**

Tabla 4: Alertas del módulo de malware e IPS (ahorro en el tiempo de corrección con la implementación de Enterprise Threat Protector)

En general, se calcula un ahorro aproximado de **110 horas** al mes gracias a la implementación de Enterprise Threat Protector.