CASE STUDY: AKAMAI IT

WHY AKAMAI USES **ENTERPRISE THREAT PROTECTOR**

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In March 2017, Akamai IT deployed Enterprise Threat Protector on Akamai's corporate wired and wireless network.

During the period March to May, Enterprise Threat Protector delivered significant and quantifiable benefits.

These include:

- A large decrease in the volume of malware incidents identified by the existing endpoint protection solution — a **54% reduction** from March to April and a **37% reduction** from March to May.
- A decrease in the volume of events generated by the existing advanced detection solution — a **30% reduction** from March to April and a **15% reduction** from March to May.
- The equivalent of **0.75 of a full-time employee** (FTE) in time saved due to the reduction of incidents and alerts from the existing endpoint and advanced detection solutions.

ENDPOINT PROTECTION

The endpoint protection solution that Akamai has deployed includes malware detection and intrusion prevention capabilities.

Malware Infection Incidents

The malware metrics were filtered to exclude "adware" and "potentially unwanted software" alerts, and to focus primarily on malware infections. The result with Enterprise Threat Protector deployed was a 54% decrease in the amount of malware infection incidents identified from March (199) to April (92), and a 37% decrease from March to May (125).

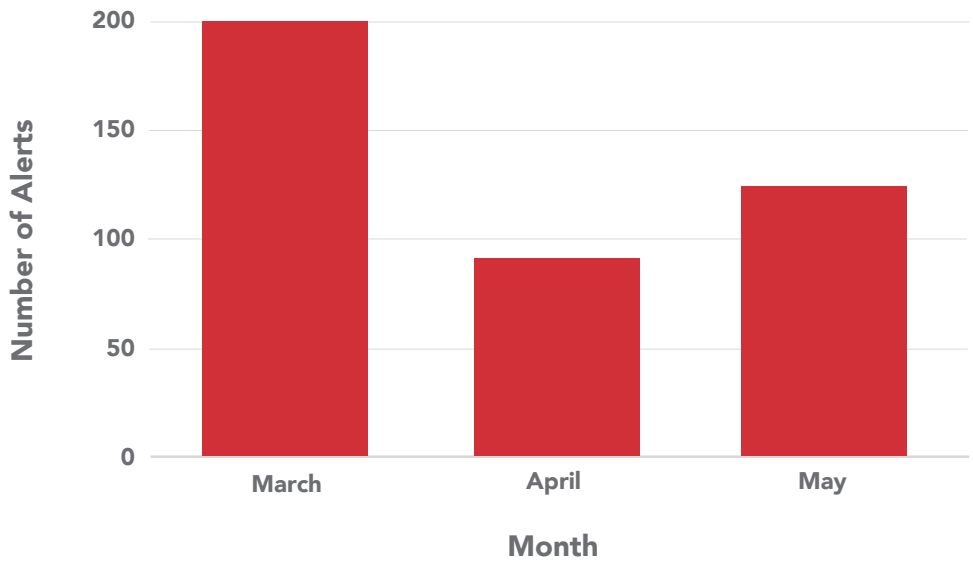

Figure 1 – Malware Incident Reduction with Enterprise Threat Protector Deployed

Intrusion Prevention System (IPS) Alerts

The number of alerts generated by the endpoint IPS sees a similar drop-off. The majority of alerts generated came in the form of torrents, but there was a noticeable decrease from March to April, and then again to May.

Figure 2 – IPS Alert Reduction (Including Torrents) with Enterprise Threat Protector Deployed

Removing torrents completely from the alerts still shows a significant reduction (27%) from March to April and decreasing approximately 35% from March to May.

Figure 3 – IPS Alert Reduction (Excluding Torrents) with Enterprise Threat Protector Deployed

Excluding torrents, the next highest number of alerts generated by the IPS were for malicious website, domain, or URL, followed closely by web attack and fake scan web page attack.

Alert	March Alerts	April Alerts	May Alerts
Malicious website, domain, or URL	13	1	1
Web attack and fake scan web page attack	12	4	1

Table 1 – Reduction in IPS Alerts with Enterprise Threat Protector Deployed

ADVANCED DETECTION

The advanced detection solution that Akamai has deployed is a supplementary defense mechanism that provides an additional layer of security. The number of alerts produced by this solution is smaller in volume, but alerts generated by this solution are much more significant.

As can be seen in Figure 4, the number of alerts generated by this solution also saw a decrease after Enterprise Threat Protector was deployed.

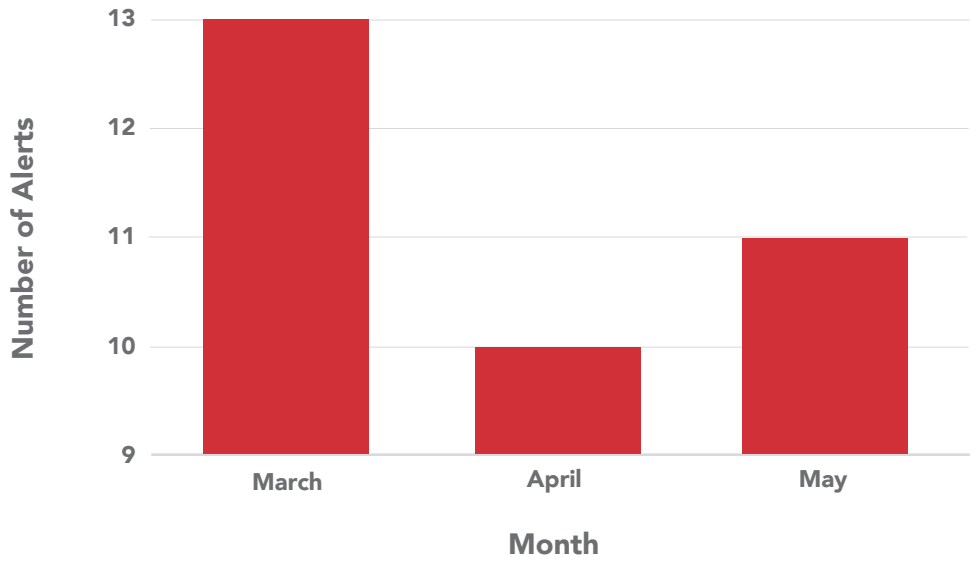

Figure 4 – Advance Detection Alert Reduction with Enterprise Threat Protector Deployed

ROI

While the reduction in incident and alert count with Enterprise Threat Protector deployed is apparent, the real value appears to be in time saved.

"Time saved" was calculated using an estimated average response time, the remediation time for malware incidents, and the time to remove torrent software. All of these activities are standard operational tasks every month. Note that there was also a decrease in the number of torrents.

Month	User count	Torrent IPs blocked
March	56	2,089
April	48	1,100
May	40	1,546

Table 2 – IPS Module Alerts

For malware investigations, a calculated time spent per incident for investigation, response, and remediations was used.

Utilizing these metrics, with Enterprise Threat Protector deployed there was an approximate time saved of **0.75 full-time employee** (FTE) per month.

Combining the malware and IPS modules from the endpoint protection, an average response time between April and June was calculated and compared against March before Enterprise Threat Protector was deployed.

The results were:

- An estimated savings of **27 hours** in the **malware detection module**
- An estimated savings of **8 hours** in the **IPS module for responding** to incidents

Response time saved (in hours)	
Malware module	27
IPS module	8
Total	**35**

Table 3 – Malware and IPS Module Alerts (Savings in Response Time with Enterprise Threat Protector Deployed)

Similarly, factoring in the average remediation time per incident upon initial response, an estimated **51 hours** from the endpoint **malware module** and **24 hours** of analyst time/month in the **IPS module** was saved.

Remediation time saved (in hours)	
Malware module	51
IPS module	24
Total	**75**

Table 4 – Malware and IPS Module Alerts (Savings in Remediation Time with Enterprise Threat Protector Deployed)

Overall, it is estimated that approximately **110 hours** were saved per month with Enterprise Threat Protector deployed.