Menlo Security

WHITE PAPER

The Hidden Cost of Web Security

A Menlo Security Business Whitepaper

August 2016

With more that 500 million malware variants in existence, and popular sites allowing content from vulnerable background sites, users can contract malware without even clicking.

Introduction

Today's security administrators find themselves in a no-win situation as they work to implement and enforce web security policies with secure web gateway (SWG) appliances and cloud-based services. SWG policies are largely based on websites' categories, such as news, entertainment, weather, social media, etc. But what if a site is unknown to the SWG, and does not fall into a known category? Administrators can either be lenient in allowing access to these uncategorized sites, increasing malware risk, or deny access to such sites and deprive employees of information and data they may need. There are hidden costs to both approaches. This paper examines these costs, and details how an alternative solution based on isolation can eliminate undesirable tradeoffs.

Uncategorized Sites, Allow or Deny?

The threat of contracting malware from the web is very real. With more that 500 million malware variants in existence[1], and popular sites allowing content from vulnerable background sites, users can contract malware without even clicking. Because it is so easy to propagate, malware has played a critical role in most of the high-profile breaches in recent times. The costs of these breaches is often in the millions, and can potentially even reach the billions, so businesses have been forced to adopt increasingly strict web security policies relying primarily on traditional secure web gateways.

Unfortunately, secure web gateways can only protect against what they know. These devices rely largely on two data points: site reputation, and site category, such as news, entertainment, weather, social media, etc. As such, there is a gap in security when the device fails to recognize a site or its category. In these situations, administrators are faced with two decisions: either allow access to uncategorized sites and face a high malware risk, or deny access and deprive employees of information and data they may need. There can be negative ramifications for either policy. On the following pages are real-world examples.

[1] *AV Test: The Independent IT-Security Institute*

According to the Ponemon Institute, two-thirds of the time spent by security staff responding to malware alerts is wasted because of faulty intelligence

The Problems with Allowing Uncategorized Sites

- **Risk** – The risk of malware from allowing access to uncategorized sites it significant. A large Fortune 50 financial services institution tasked their security research team to analyze the sources of malware infections for 3 months. Their internal report showed that >60% of the infections were from uncategorized sites. These infections are costly given that a large enterprise can spend an average of almost 600 hours each week on malware containment.[2] Considering $82 per SOC-engineer-hour X 52 weeks X 600 hours per week, that's more than $2.5M annually.
- **Cost of Sanitizing Infected Machines** – Sanitizing infected machines can also be costly. A large service provider in Asia was forced to re-image devices every week because they no longer believed they could successfully disinfect machines using traditional antivirus solutions. An internal analysis showed that this practice cost them $3-4M per year in IT and productivity loss.
- **SOC Costs** – Allowing uncategorized sites means more security alerts. In Japan, and most regulated industries across the globe, every alert from every security product has to be fully analyzed for possible endpoint compromise. According to the Ponemon Institute[2], two-thirds of the time spent by security staff responding to malware alerts is wasted because of faulty intelligence. It costs organizations an average of $1.27 million annually in time wasted responding to erroneous or inaccurate malware alerts.
- **SOC Turnover** – The average employment term of SOC engineers is roughly a year, after which they resign due to alert-fatigue. Recruiting costs in this area are high, as it is increasingly difficult to hire qualified SOC engineers. This is because fresh graduates are more compelled to build apps rather than learn security and forensics, a career path with a steep learning curve and a high-degree of expertise required to make sense of the complexities. A 25%-of-$170,000-base-salary recruiting cost, times a conservative 40% turnover rate within a 5-person team, yields $85,000 per year. If you consider the opportunity cost of two existing SOC engineers spending 25% of their time training two new employees, the cost is an additional $85,000 per year. Combine these, and the total annual turnover cost is $170,000.

[2] *The Cost of Malware Containment, Ponemon Institute, January, 2015*

Allowing uncategorized sites puts your organization at greater risk, while denying these sites creates user and administrator frustration.

The Problems with Denying Uncategorized Sites

- **Number of Trouble Tickets** – Denying uncategorized sites creates an overwhelming number of recategorization requests. For a global investment firm, the number of tickets to re-categorize per day was approximately 2000 across 250,000 employees. Greater than 75% of these requests were non-work related such as veterinarian research, schools, soccer little league, etc. With more than 5 dedicated people parsing through the requests, the issue was frustrating and expensive, costing approximately $850,000 per year.

- **Recategorization Experts** – Recategorization is a manual process. A European insurance provider and a large Japanese manufacturer were inundated with such requests when they began blocking access to uncategorized sites. The issue was compounded by the fact that their secure web gateway could not help them to determine the security posture of the sites in question. The organizations had 16 and 5 security analysts respectively dedicated to analyzing sites before recategorization. Another global financial services firm had a staff of 20 around the world to, in their own words, "recreate the Yahoo index". With a conservative SOC staff of 5, this team cost an enterprise $850,000 annually.

As these examples demonstrate, there are significant tradeoffs with both approaches. Allowing uncategorized sites puts your organization at greater risk, while denying these sites creates user and administrator frustration. Both generate millions in additional costs. A new approach is needed.

Isolation eliminates the possibility of malware reaching user devices via compromised or malicious websites

A New Approach, Isolation

A new approach to preventing malware uses isolation, which inserts a secure, trusted execution environment, or isolation platform, between the user and potential sources of attacks. By executing sessions away from the endpoint and delivering only safe rendering information to devices, users are protected from malware and malicious activity.

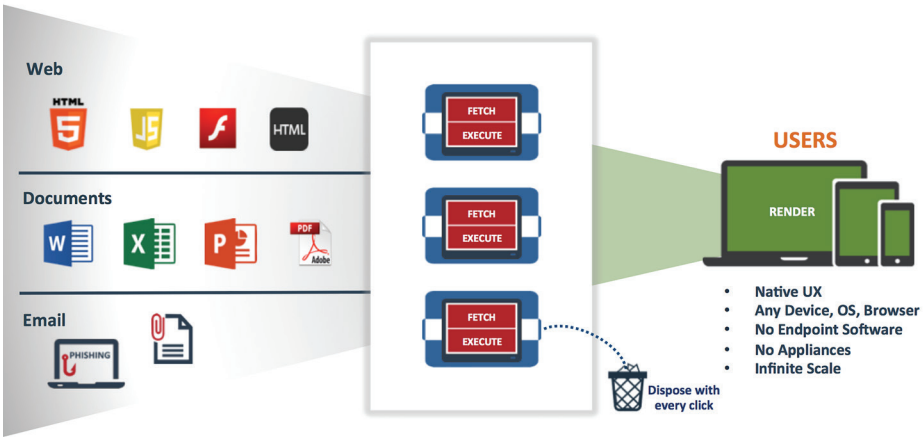

Figure 1: The isolation approach eliminates malware and its effects across the most critical threat vectors

Isolation eliminates the possibility of malware reaching user devices via compromised or malicious websites, email or documents. This is not detection or classification, rather the user's Web session and all active content (e.g. Java, Flash, etc.), whether good or bad, is fully executed and contained in the isolation platform. Only safe, malware-free rendering information is delivered to the user's endpoint. No active content—including any potential malware—leaves the platform. As such, malware has no path to reach an endpoint, so websites and legitimate content needn't be blocked in the interest of security. Administrators can open up more of the Internet to their users while simultaneously eliminating the risk of attacks.

With isolation, administrators are able safely allow access to uncategorized sites and eliminate the frustrating security vs. cost tradeoffs of the past:

- **Risk** – No active web content reaches the end-point, thus uncategorized sites present zero risk.
- **Cost of Sanitizing Infected Machines** – Isolation eliminates the web as a malware threat vector, drastically reducing number of machines to be reimaged. Reduces the urgency around patching machines for every browser and plug-in vulnerability.
- **SOC Costs** – Isolation stops threats before they are detected by traditional solutions, eliminating erroneous or inaccurate malware alerts

- **SOC Turnover** – Alert fatigue is minimized along with SOC staff turnover
- **Number of Trouble Tickets** – Employees are more productive and are now free to safely explore the web without submitting recategorization requests
- **Recategorization Experts** – By eliminating recategorization requests, the need for expensive experts is eliminated.

Conclusion

The hidden costs of web security vary for each deployment, but for an organization of several thousand employees, we have seen isolation customers derive material savings in several areas:

- The salaries of several security engineers who can be repurposed to higher value tasks.
- A reduction in training and recruiting costs for new engineers that accompanies reduced turnover.
- Savings from the reduction of re-imaging infected machines, etc.

Although web security administrators have traditionally been faced with no-win policy decisions, new isolation technology enables them to maintain strict security policies without sacrificing end-user satisfaction. By eliminating undesirable risk vs. usability tradeoffs, IT teams will not only make their organizations more secure, they can also drastically reduce the hidden costs of web security.

For more information visit menlosecurity.com

Menlo Security

934 Santa Cruz Avenue
Menlo Park, CA 94025
Tel: 650 614 1795
info@menlosecurity.com