Menlo Security

WHITE PAPER

Business Case for Internet Isolation

The Menlo Security Cloud Platform powered by Isolation helps eliminate the hidden high costs of detection-only cybersecurity approaches.

The nature of cyberattacks is changing. No longer are threat actors spending weeks probing network perimeters and trying to find a backdoor entry. Nor are they searching for unsecured and undersecured servers and network devices. Instead, threat actors today are overwhelmingly targeting the weakest link in the security apparatus: people. In fact, 99 percent of attacks in 2018 used email and web browser vulnarbilities as the primary attack vectors.[1]

As cyberattacks increase in frequency and sophistication, customers feel forced to deploy an array of solutions in the hope that a best-of-breed mindset will protect their network. Two of the most critical areas are email and web security. While the solutions that customers have deployed work well in their respective areas, the associated cost of operating and maintaining these solutions can be prohibitive.

Email- and web-based attacks are sophisticated, in that the attacker has spent time and effort to understand their victim and, in many cases, created custom ways to ensure that the user takes the call to action, resulting in compromise (credential theft, malicious download, watering-hole attack, etc.). The software, infrastructure, and skill set needed by cybercriminals to replicate and launch attacks at scale make the business of cyberattacks similar to that of Software-as-a-Service (SaaS) companies. The SaaS approach, as it has been adapted by cyberattackers, allows them to easily and continuously evolve their threats. In addition, attackers continue to improve their social engineering techniques to prey on people's emotions, curiosity, and insecurities. In fact, 12 percent of users will open a malicious email, and 4 percent will always click a link in a malicious email.[2]

Current Cybersecurity Solutions Are Ineffective

Current solutions are not keeping up with the changing nature of cyberattacks. Most enterprises continue to rely on security solutions

99%

Percentage of attacks in 2018 that used email as the primary attack vector

[1] Verizon. 2018 Data Breach Investigations Report (11th Edition)

[2] Ibid

grounded in outdated detect-and-respond tactics that still suffer from incidences of false negatives, which means that these organizations continue to be exposed to attacks. However, detection simply doesn't work when the emails themselves don't carry malware, or when the highly targeted nature of today's attacks results in little or no reputational information available to reference. As a result, threat actors are enjoying perhaps their most successful run in the history of hacking.

Current Cybersecurity Solutions Are "Almost" Secure

At the same time, cybersecurity solutions that rely on detect-and-respond tactics are costing enterprises tens of millions of dollars per year. The detect-and-respond approach is extremely labor intensive: Someone has to conduct thorough threat intelligence, respond to alerts, weed out false positives, conduct search-and-destroy tactics, reimage machines, and recategorize new and unknown websites. Cybersecurity professionals demand salaries averaging $175,000 per year in a highly competitive market, and they also require constant retraining and continuing education and certification.

4%

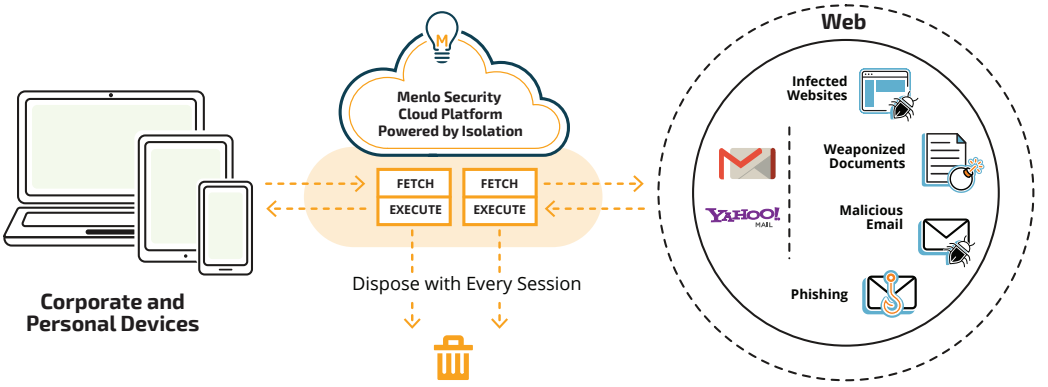
Percentage of Users Who Will Always Click a Link in a Malicious Email

The result is an ineffective and expensive enterprise cybersecurity strategy. Something has to change.

Internet Isolation Provides 100 Percent Protection

Internet isolation can change that dynamic by inserting a secure, logically air-gapped execution environment in the cloud between the user and potential sources of attacks. By executing sessions away from the endpoint and delivering only safely rendered information to devices, users are protected from malware and malicious activity. An Internet isolation gateway that focuses on both email- and web-based attacks is the only cybersecurity approach that can guarantee 100 percent protection.

The result is that malware cannot infect a device it cannot reach. Internet isolation eliminates the possibility of malware reaching user devices via compromised



or malicious websites, email, or documents. This approach is not detection or classification; rather, the user's web session and all active content (e.g., Java, Flash, etc.)—whether it's good or bad—is fully executed and contained in a remote web browser in the cloud. Only safe, malware-free information is mirrored to the user's endpoint device. No active content—including any potential malware—is able to escape the environment, because it has no path to reach an endpoint.

The result is a completely safe web and email experience without having to block any websites or legitimate content in the interest of security. Administrators can open up more of the Internet to their users while simultaneously eliminating the risk of attacks.

4.5 Billion

Data Records That Were Compromised in the First Half of 2018

Comparing the Hard and Soft Costs of Detect and Respond Versus Internet Isolation

It's clear that Internet isolation is more effective than detect-and-respond security strategies: Internet isolation simply treats all content as risky, preventing any code—malicious or not—from reaching the endpoint. But Internet isolation is also more efficient, eliminating many of the bottlenecks and inefficiencies associated with traditional cybersecurity strategies.

The following pages detail cybersecurity costs and show how Internet isolation reduces an organization's financial risk:

Malware Containment

Why It's Expensive

Uncategorized sites present a dilemma for many enterprises. One of our customers, a large Fortune 50 financial services organization, did research into the source of all malware and found that more than 60 percent of infections were from uncategorized sites. Allowing users to visit uncategorized sites is a business imperative, yet it introduces significant risk and financial burden to the organization. The average enterprise spends more than 600 hours each week on malware containment. Considering that the average hourly cost of a security operations center (SOC) engineer is $82, the cost comes to more than $2.5 million annually.

How Isolation Eliminates That Expense

Isolation prevents all web content—including content from uncategorized sites—from ever reaching the endpoint. With an isolation solution in place, malware infection from these sites is virtually impossible, eliminating the need for time-consuming and expensive malware containment activities.

More Than

600

HOURS/WEEK

Spent on Malware Containment Can Cost the Average Enterprise

More Than

$2.5

MILLION ANNUALLY

Reimage Machines

Why It's Expensive

Given the difficulty that traditional detect-and-respond solutions have with identifying and stopping advanced malware, some enterprises elect to just reimage and restore systems every night or week. A large service provider in Asia that we work with utilized this approach because they no longer had confidence in their traditional antivirus solutions. An internal analysis showed that reimaging just eight devices per week cost $3–$4 million per year—not including productivity loss resulting from the planned downtime.

How Isolation Eliminates That Expense

Isolation eliminates the possibility of infected endpoints, effectively eliminating the need to sanitize machines on a regular schedule. It also reduces the urgency around patching machines for every browser and plug-in vulnerability—an added cost savings.

Reimaging Just

8 DEVICES PER WEEK

Can Cost

$3M-$4M ANNUALLY

Not Including Productivity Loss Caused by Downtime

False Positives

Why It's Expensive

According to the Ponemon Institute, two-thirds of the time spent by security staff responding to malware alerts is the result of faulty intelligence and false positives, costing organizations an average of $1.27 million annually[3]. In addition, all this manual labor and chasing after false alerts is costing enterprises more than just time and money. It's affecting the morale of their employees. The average tenure of SOC engineers is roughly one year, mainly because of alert fatigue. Recruiting costs are high because it's difficult to find qualified SOC engineers in a highly competitive job market. Given a 25 percent recruiting cost of a $170,000 base salary and a conservative 40 percent turnover rate on a five-person team yields $85,000 a year. Add time spent by existing employees to train new colleagues, and cumulatively, the cost of churn in the security space can be $170,000 per year for a five-person team.

How Isolation Eliminates That Expense

Isolation stops threats before an attack reaches the network perimeter, when an alert would be generated. No contact. No alert. No false positives. No fire drills. No chasing after ghosts. No alert fatigue. Lower turnover.

TURNOVER RATE

Caused by Alert Fatigue Can Cost

$170K PER YEAR

For a Five-Person Team

[3] 2018 Cost of Data Breach Study: Impact of Business Continuity Management by Ponemon Institute

An "Almost" Secure Cybersecurity Strategy Is Cost Prohibitive

The soft costs of an unsuccessful cybersecurity strategy can be burdensome. Infections need to be fixed and holes need to be patched. Fines and audits can be costly as well—especially with the rollout of GDPR in the EU and similar regulations that are sure to be enacted in other parts of the world. In addition, the loss of public trust, the burden of informing customers and shareholders of breaches, and the cost of lost business can be devastating to a company's bottom line. Often, victims of large data breaches aren't able to come back from the hit at all.

Unfortunately, traditional detect-and-respond cybersecurity strategies are highly ineffective and inefficient—costing enterprises tens of millions of dollars each year in containment, management, hiring, help desk, and PR costs.

Internet isolation eliminates much of the financial burden associated with cybersecurity—giving organizations a way to improve their security posture and reallocate budget to other, more strategic IT costs.

To learn more, visit menlosecurity.com/resources or get in touch via ask@menlosecurity.com to see how you can use isolation to stop email- and web-based attacks.

About Menlo Security

Menlo Security protects organizations from cyberattacks by eliminating the threat of malware from the web, documents, and email. Menlo Security has helped hundreds of Global 2000 companies and major government agencies achieve Secure Cloud Transformation. The company's Cloud Security Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. The company was named a Visionary in the Gartner Magic Quadrant for the Secure Web Gateway.

Contact us
menlosecurity.com
(650) 614-1705
ask@menlosecurity.com