Menlo Security

BUSINESS CASE FOR WEB ISOLATION

Eliminate the hidden high costs of detection-only cybersecurity approaches

WHITE PAPER

OVERVIEW

A Changing Threat Landscape Requires a New Approach to Cybersecurity

The nature of cyberattacks is changing. No longer are threat actors spending weeks probing network perimeters trying to find a backdoor entry. Nor are they searching for unsecured and undersecured servers and network devices. No, threat actors today are overwhelmingly targeting the weakest link in the security apparatus: people. In fact, 95 percent of attacks in 2017 used email as the primary attack vector.[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]

95%
OF ATTACKS IN 2017
used email as the primary attack vector

4%
OF USERS WILL ALWAYS CLICK A LINK
in a malicious email

4.5
BILLION DATA RECORDS
were compromised in the first half of 2018

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

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 Most enterprises continue to rely on security solutions grounded in outdated detect-and-respond tactics that still suffer from incidences of false negatives, which means that these organizations continue to be exposed to attacks.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. According to Gemalto, 4.5 billion data records were compromised in the first half of 2018.

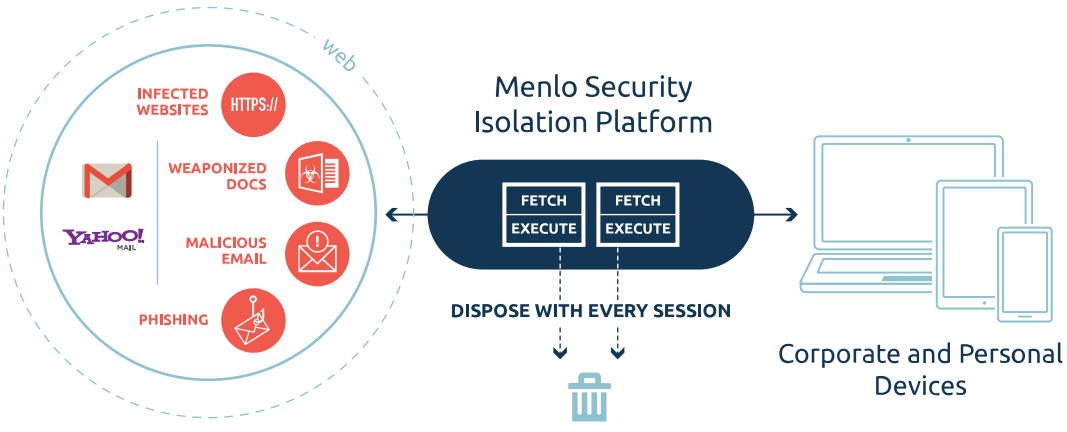
Current Cybersecurity Solutions Are Inefficient

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.

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

Web Isolation Provides 100 Percent Protection

Isolation can change that dynamic. Isolation cybersecurity solutions insert a secure, logically air-gapped execution environment—or isolation platform—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. Isolation is the only cybersecurity approach that can guarantee 100 percent protection.



The result is that malware cannot infect a device it cannot reach. 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 the isolation platform. 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 platform, because it has no path to reach an endpoint. The result is a completely safe web 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.

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

It's clear that isolation is more effective than detect-and-respond security strategies: Isolation simply treats all content as risky, preventing any code—malicious or not—from reaching the endpoint. But 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 isolation reduces an organization's financial risk:

MALWARE CONTAINMENT

WHY 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 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 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

$3-4 MILLION ANNUALLY

NOT INCLUDING PRODUCTIVITY LOSS DUE TO DOWNTIME

MALWARE FALSE POSITIVES

WHY 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. In addition, all this manual labor and chasing after false alerts is costing enterprises more than just time. 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 costs $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. Little turnover.

TURNOVER RATE

DUE TO ALERT FATIGUE CAN COST

$170K PER YEAR

FOR A FIVE-PERSON TEAM

HELP DESK COSTS

WHY EXPENSIVE:

Given the risk, some enterprises simply ramp up their blocked content policies, figuring that a hardened security posture will protect them in the long run. It might, but there's a productivity trade-off. Users who can't access the websites they need aren't able to conduct their responsibilities adequately. They can file a help desk ticket to gain access to the site in question, but that cost really starts to add up. Several of our customers tried this approach, and quickly realized that this frustrating and expensive process was cost prohibitive. For one customer in the financial services space, the number of recategorization tickets exploded to nearly 2,000 per day across 250,000 employees—requiring a dedicated team of five help desk administrators that cost the company $850,000 per year.

HOW ISOLATION ELIMINATES THAT EXPENSE:

Isolation doesn't discriminate between uncategorized and categorized sites, or between good content or bad. It treats all web traffic as risky, preventing any code from reaching end users while giving them the freedom to access any site they want—as long as the content doesn't conflict with the company's acceptable use policies. There's no loss of productivity, no need to recategorize sites, and no additional burden on the help desk staff.

NEARLY

2,000

RECATEGORIZATION TICKETS PER DAY

ACROSS 250,000 EMPLOYEES
COST THE COMPANY

$850K

PER YEAR

FOR A DEDICATED
TEAM OF FIVE HELP DESK
ADMINISTRATORS

Conclusion

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.

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.

Menlo Security

About Menlo Security

Menlo Security protects organizations from cyber-attacks by seeking to eliminate the threat of malware from the web, documents, and email. Our cloud-based Isolation Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. Menlo Security is trusted by major global businesses, including Fortune 500 companies and financial services institutions.

2300 Geng Rd., Ste. 200

Palo Alto, CA 94303

Tel: 650 614 1705

info@menlosecurity.com

menlosecurity.com