The federal agency guide to navigating the top 3 cloud security risks

eBook

FedRAMP

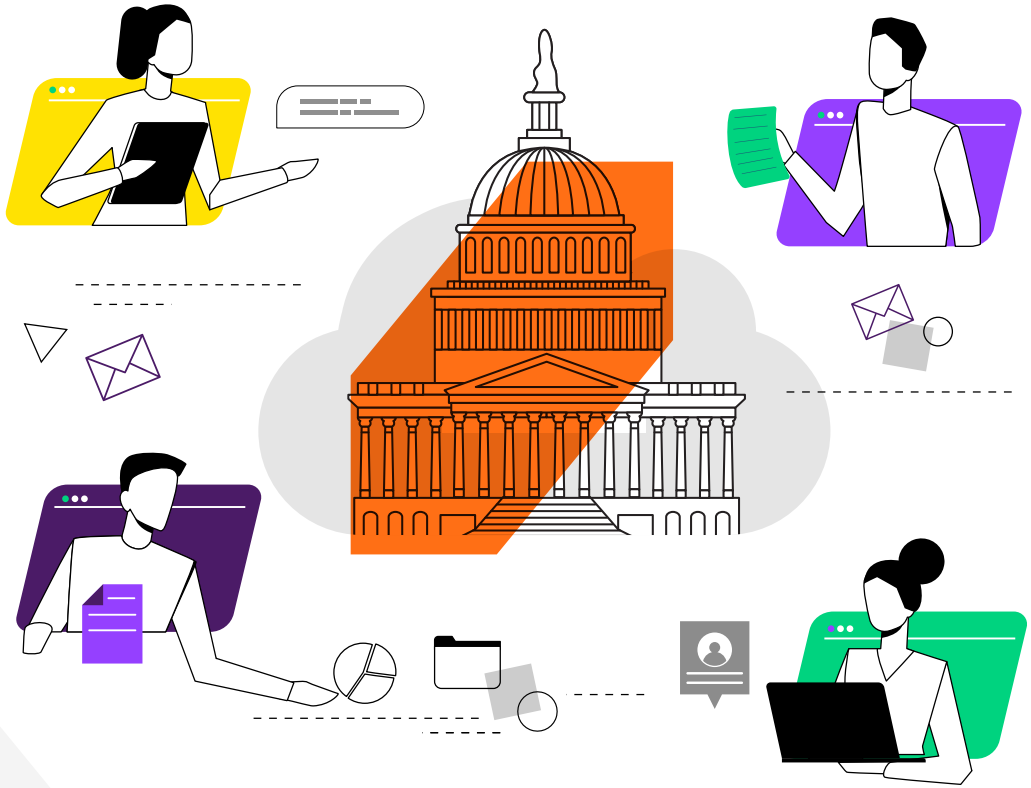
MENLO SECURITY

Contents

Today's tumultuous threat landscape

Worldwide crisis forever changed the way federal agencies view the cloud. IT leaders rushed to support remote work and massive surges in demand by becoming "cloud first" organizations virtually overnight.

Next, the job became bolstering security to keep users — and data — safe in a volatile cloud threat landscape.



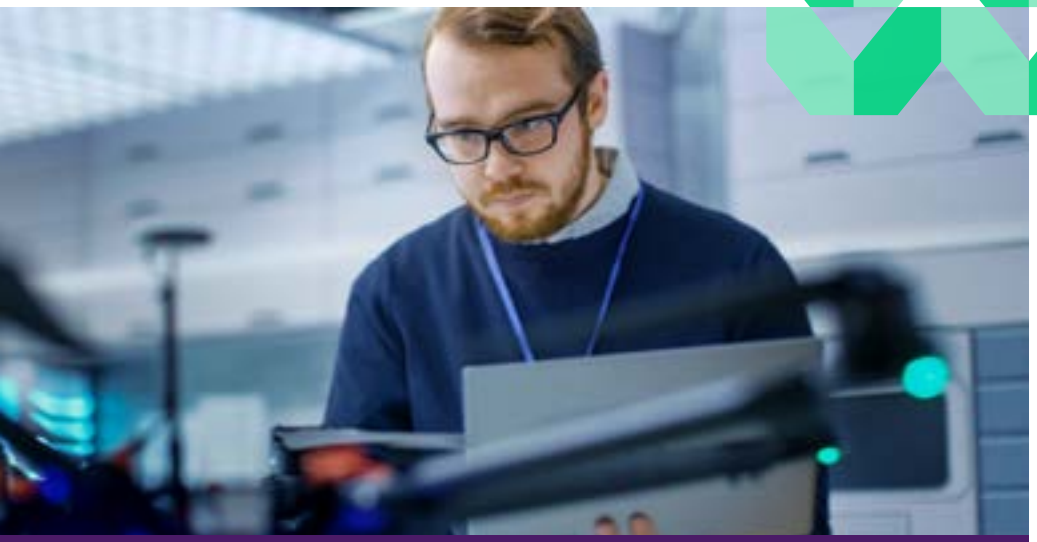
Agency attacks on the rise

With a hybrid workforce and dynamic attack surface, governments are being targeted like never before. A CloudSek report found the number of attacks targeting the government sector increased 95% worldwide in the second half of 2022 compared to the same period in 2021.

The flexibility and scalability of cloud allowed governments to meet the urgent challenges of the pandemic, such as massive surges in demand for services or the sudden shift to remote work. Governments at all levels made considerable investments in cloud, but now they face difficult choices about how to maintain, develop, and build upon cloud investments.

— Deloitte[1]

1 https://www2.deloitte.com/us/en/insights/industry/public-sector/public-sector-cloud-adoption.html



55%

of organizations encounter advanced web threats at least 1x a month

20%

face at least one each week

Menlo Security *State of Threat Prevention* report

The crisis was temporary. The change feels permanent.

After tasting the scale and agility of cloud technologies, agencies opted to stick with it — if they can find a viable balance between convenience and exposure to risk. Challenges they face in securing today's multi-cloud environments include:

Evolving beyond VPNs

With large numbers of users connecting from everywhere, Virtual Private Networks (VPNs) feel less safe and even less practical than they did before. Backhauling traffic to centralized systems adds significantly to cost, detracts from the user experience (UX), and creates new vulnerabilities for bad actors to exploit.

75% of work taking place in browsers – the new #1 threat vector

Today's workforce relies on browsers to access the cloud, SaaS-based applications, collaboration tools, and other critical resources 24/7. Security controls built for the office provide limited visibility into browser-based threats, making it easy for attackers to drop malware with payloads that compromise endpoints.

Emerging evasive threats

As we'll see in Section 4, today's attacks use sophisticated techniques to sail past traditional security stacks undetected.

What happens now?

In this eBook we'll explore how a modern approach to cybersecurity protects federal agencies from three devastating cloud attacks on the rise today as operations stay rooted in browsers, and the cloud.

Modern threats raise the stakes for cloud security

Digitalization would have happened anyway, just not this fast. Accelerating global support for remote work — and emphasizing speed above security in the beginning — paved the way for threat actors to get creative about attacking the cloud. And they are.

What causes most cloud breaches?

Common enablers of cloud-based attacks include:

- **File-based malware** delivered during file-syncing
- **Leaked credentials and overly permissive** IAM policies
- **Vulnerabilities in APIs** or weak vulnerability management
- **Misconfigurations** in cloud services and storage buckets

Most threats share two things in common.

- They involve the human element.
- Legacy security systems won't prevent or detect them until it's too late — and *that's* the real problem.

Spending more is not the answer

IT continues to invest in endpoint protection, anti-virus solutions, intrusion detection systems (IDS), and perimeter technologies that don't keep users safe online and in multi-cloud environments. While the *2022 Cyberthreat Defense Report* shows typical IT security budgets grew 5% last year, losses resulting from cyberattacks rose as well. No net gain.

Detect-and-respond strategies give attackers the edge

Defenders of data owned by government agencies can't afford to wait for attacks to happen. Rapid detection proves essential, but over-reliance on detection and response keeps defenders in a reactive mode.

A better strategy? Complementing modern detection capabilities with preventive strategies that stop new threats from entering environments through the cloud in the first place.

Don't go it alone

Fortunately, thought leaders aiming to modernize the government's IT infrastructure have laid out guidelines for strengthening security and compliance as you go. We'll list the most important next, then move on to see how you can avoid today's riskiest cloud-based attacks.

95%

Increase in the number of attacks targeting the government sector in 2H 2022 compared 2H 2021 (CloudSek)

$1.8B

Annual spending for vendor-furnished cloud computing goods and services by FY 2024 (Deltek)

The clock is ticking on Zero Trust

Making security flexible and dynamic enough to protect a distributed workforce in perpetuity is a big lift for IT. With more data finding its home in the cloud, leading cybersecurity strategists are weighing in about when, where, and how they should go about it:

- In 2019, the Department of Defense (DoD) launched the Cybersecurity Maturity Model Certification (CMMC) to strengthen assessments of federal contractors that handle Controlled Unclassified Information (CUI).
- In 2021, The Biden administration's Executive Order 14028, "Improving the Nation's Cybersecurity" set the stage for rapid modernization to defend against malware, phishing, nation states, and other attacks.
- The Office of Management and Budget (OMB) followed with a migration path requiring agencies to hit certain milestones by EOY 2024.
- In 2022, the Cybersecurity and Infrastructure Security Agency (CISA), US Digital Service, and Federal Risk Authorization Management Program (FedRAMP) collaborated to define the nation's Cloud Security Technical Reference Architecture (TRA) for protecting data throughout migration.

Change isn't easy . . .

Nearly 60%

of federal officials say rebuilding or replacing existing legacy infrastructure is a primary challenge to implementing Zero Trust.

48%

say their agencies lack sufficient IT staff expertise.

Read the full blog

"As agencies move into the cloud, their assets cannot be protected by this 'castle and moat' paradigm. Agencies will likely operate in a multi-cloud environment where they have varied levels of control over perimeters."

— (CISA TRA)

The core requirement?

Adopt the principles of a Zero Trust security architecture, fast. Use the guidance — and pressure — from regulators to take the first steps on your Zero Trust journey using new implementation models and fundamentally different approaches.

Innovative strategies emerge

Zero Trust aligns with a preventive, versus reactive approach. In 2020, the Defense Information Systems Agency (DISA) took the lead by making cloud-based Internet Isolation (CBII) a cornerstone of plans to secure the DOD's workforce of 3.5 million.

CBII became DISA's first Other Transaction Authority (OTA) to reach production, and it worked as expected. According to Laurel Ashley, CBII Program Manager at DISA, "It has been very effective in terms of identifying malicious content and keeping the DODIN [Department of Defense Information Network] and users protected when threat actors on websites are encountered."

But first . . .

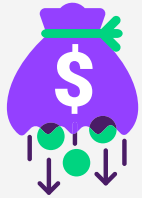
We'll take a closer look at CBII again after looking at three of today's top cloud security risks – ransomware, evasive attacks, and supply chain attacks.

9%

Hacktivist activity accounted for incidents reported in the government sector (CSO)

6%

Reported incidents attributed to LockBit and other ransomware groups (CSO)



$2.07M

Average cost of attacks against the public sector in 2022, up 7.25% vs. 2021 (IBM)

Cloud Risk #1: Ransomware

According to Sophos', *The State of Ransomware in State and Local Government 2022*, 72% of state and local government organizations attacked by ransomware had their data encrypted — 7% higher than the cross-sector average, and just 20% stopped the attack before data could be encrypted (vs. cross-sector average 31%).

Emisoft research shows upwards of 25% of attacks in 2022 resulted in known data breaches with some agencies choosing to pay the ransom.

Modern attacks have changed

Ransomware of old mostly encrypted the data on local machines and held it hostage. In this scenario, backing up critical files and systems to the cloud was a key part of the defense strategy. Why pay a ransom when you can just download a copy from the cloud within a day or two?

Now, instead of just encrypting files on local systems, ransomware attacks steal or threaten and expose data. Scare tactics might include threatening to damage public trust in an agency's reputation by "leaking" that a breach has occurred on social media. In this scenario, the cloud becomes part of the problem.

Cloud-based ransomware attacks

The cloud represents both a target and modern delivery mechanism for today's malware and ransomware attacks. This new generation of exploits compromises

data housed in cloud storage services or as it moves to and from the cloud.

Tried-and-true tactics for deploying malware still work. For example, the notorious Petya attack that began exploiting Windows-based systems in 2016 began with phishing emails that contained bogus Dropbox links. Instead of relevant attachments, clicking the link exposed users to cloud-based executables that infected local systems.

Evolving tactics and techniques in the cloud

As we've seen, the most common method of spreading attacks to the cloud occurs when compromised endpoints sync data with cloud storage services. Modern campaigns also leverage malware to cash in on the common causes of attack cited earlier: application vulnerabilities, misconfigurations, weak credentials and APIs, overprovisioned access, and human error. Ransomware research from Emertec shows misconfigured identities, publicly exposed machines, third-parties, and compromised access keys also add risk.

Sophisticated ransomware designers produce variants that bypass cloud protections to reach as many systems as possible. Other campaigns phish individual users and extract or encrypt cloud data or target specific cloud providers to find vulnerabilities or brute-force their way through the login process.

However, it happens, experts warn . . .

Do NOT pay the ransom

To discourage payment, and ransomware attacks themselves, authorities set new proposed regulations in motion. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) required CISA to develop and implement regulations requiring covered entities to report covered cyber incidents and ransomware payments to CISA.

According to a Gartner® Press Release, "Through 2025, 30% of nation states willpass legislation that regulates ransomware payments, fines and negotiations, up from less than 1% in 2021."[2]

Gartner Press Release, Gartner Unveils the Top Eight Cybersecurity Predictions for 2022-23, June 21, 2022, https://www.gartner.com/en/newsroom/press-releases/2022-06-21-gartner-unveils-the-top-eight-cybersecurity-predictio

Cloud Risk #2: Evasive browser threats

As defenders race to monitor and close every door, attackers find new ways to sneak in a window. The latest class of sophisticated threats uses evasive tactics and techniques to gain initial access to endpoints via the cloud.

Their plan? To get around Secure Web Gateways (SWGs), agencies' primary tool for deflecting web-based threats, and either steal sensitive data or detonate malicious payloads.

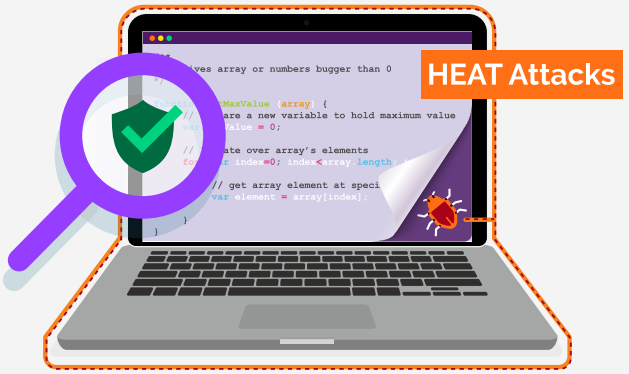
Threat actors are leveraging Highly Evasive Adaptive Threats (HEAT) to exploit web browsers. By employing various evasive techniques, these HEAT attacks are able to easily bypass multiple layers of detection across common security technology in use today.

We're not "just browsing" . . .

When desktops first got connected to the Internet, PCs and OSs were the primary targets of cyberattacks. The meteoric rise of SaaS changed all that.

SaaS raised the stakes for security strategies like Defense in Depth (DID) that secure networks — with firewalls, Secure Web Gateways (SWGs), intrusion prevention systems (IPS), etc. — and endpoints (with AV, EDR, etc.). Now, for the first time, and perhaps above all else, security needs to protect the browser.

Attacks arrive at the browser poised to "land and expand" so malware can corrupt user endpoints instantaneously. Evasive attacks slip past the radar of monitoring tools and deliver their malicious payloads within seconds of an initial breach. By the time detection and response-based systems mobilize, it's already too late.



224%
Increase in HEAT attacks during 2H 2021

50+%
of HEAT attacks come from categorized web sites

69%
Malicious attacks prevented by the Menlo Cloud showed HEAT characteristics

50%
Malicious URLs analyzed by Menlo Labs leveraged HEAT techniques

70%
increase in LURE attacks in 2022

How it works

HEAT attacks leverage various techniques to evade detection-based security technology, including:

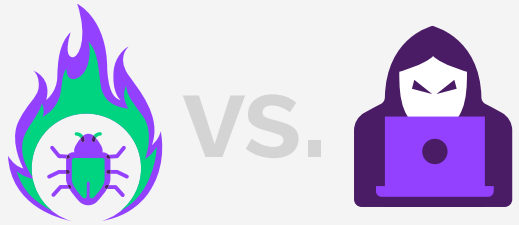
- **MFA bypass:** Phishers and other bad actors circumvent multi-factor authentication (MFA) to compromise credentials (a leading cause of breaches) and steal data. Tactics include MFA fatigue (flooding users with requests until they give in and approve), token theft, and machine-in-the-middle (MITM) campaigns that direct users to fake login pages where hackers steal credentials.
- **HTML smuggling:** Attackers "smuggle" and encode malicious scripts within HTML attachments or webpages that deposit malware.
- **SEO poisoning:** Or "search poisoning attacks" in which sponsored links lure users to malicious sites that infect visitors with malware or phish them for sensitive information.
- **Password-protected file attacks:** Emails attract users to open malicious documents by including passwords within the email, thus evading traditional anti-malware detection.

Most HEAT attacks target the weakest link in the chain — users — hoping they'll click or download the wrong thing and rely on IT's lack of visibility since traditional defenses won't recognize behaviors as malicious. Along with SWGs and Secure Email Gateways (SEGs), HEAT attacks completely bypass detection-based security technology including:

- URL filtering
- Anti-virus / anti-malware engines and sandboxes
- Network and HTTP content inspections
- Malicious link analysis
- Offline domain analysis
- Indicator of compromise (IOC) feeds

Attacks on the rise

Evasive threats are proliferating rapidly, replacing other go-to threat levers used by sophisticated threat actor groups to deliver malware. Rather than react, the sensitive IT environments used in national security and public services must adopt new cyber defense strategies to prevent evasive attacks from succeeding.



HEAT vs. APT

Highly Evasive Adaptive Threats and advanced persistent threats (APTs) can be seen as two very different-looking sides of the same coin. HEAT attacks are used to gain initial access into a network. Only then can an APT be deployed. The evasive attack gets threat actors in the door, the APT makes its way toward the target.

And risk isn't all . . .

Evasive attacks don't just confront security analysts with a new nemesis. Compromising browsers slows down the online experience making users, especially those working remotely, less productive on the web. And even less happy.

Evasive threats turbo-charge ransomware

The simultaneous rise of evasive attacks and ransomware is no coincidence. Remote work and the ongoing migration of many applications to Software as a Service (SaaS) platforms increase users' reliance on browsers. With many spending up to 75% of their time working in browsers,[3] ransomware gangs like LockBit enjoy new opportunity to peddle more malware while flying under the radar of existing security tools.

Again, the ideal defense keeps tricky new threats from gaining access to networks and corrupting endpoints in the first place.

Implementing Zero Trust with Menlo Security Cloud Platform

Converged cloud native services delivered at scale

3 https://cloud.google.com/blog/products/chrome-enterprise/chrome-is-helping-it-teams-support-cloud-first-workforce

The DoD Defends Against HEAT Attacks

In 2020, By Light Professional IT Services tapped Menlo for its best in industry Isolation platform, and was awarded a $198.9M Other Transaction Agreement (OTA) by the US Department of Defense to design and implement change to browser isolation technology able to contain evasive threats within 5 years.

The platform stands to protect:

3.5M users

against evasive attacks while improving UX and slashing VPN traffic by

44%

for estimated total cost-savings of

$300M

Cloud Risk #3: Third-party/supply chain attacks

Nothing spotlights the value of a Zero Trust risk posture like third-party attacks. A high percentage of campaigns aimed at the government use trusted partners and providers to target agencies and critical infrastructure.

Even with rigorous vetting and certification processes, vendors with weaker security controls can still become agency partners. Email service providers, collaboration tools like Slack or Zoom, SaaS and eCommerce offerings, and other suppliers all look like third-party threat vectors to attackers.

Risk gets amplified in the cloud

Enhanced data interoperability, though practical, raises agencies' risk of suffering third-party breaches even higher. Migrating data from legacy systems to cloud service offerings creates a sprawling, multi-tiered supply chain too vast to watch over as more partners than ever have access to federal assets.

Disparate security practices create blind spots and inconsistencies that create dangerous complexity. Risk grows exponentially, cyber hygiene practices vary and no one organization patrols the entire border to catch threat actors on the lookout for misconfigurations and unpatched vulnerabilities.

Attacks scale in size and scope

According to IBM's *2022 Cost of a Data Breach Report*:

19%

of breaches were caused by compromised supply chain.

$4.46M

The average cost third-party breaches was 2.5% greater than the overall average.

26 days

Third-party breaches took longer to find and contain.

Identity as the new perimeter

Like evasive attacks, perimeter-based strategies fail to detect third-party attacks because trusted suppliers aren't technically "intruders." Because people, machines, and cloud providers all may use digital identity to access resources, maintaining lists of providers or CSP-managed accounts gets challenging. Hence the recent assertion by vendors and industry analysts that "identity is the new perimeter."

Adhere to standards for partnering in the cloud

With supply chain attacks taking down critical infrastructure, agencies need strategies, tools, and guidelines for staying out of the headlines. At the start of 2023, the FedRAMP Authorization Act passed making it easier for agencies to certify vendors, but also calling for creation of a Secure Cloud Advisory Committee. This group made up of vendors, federal agencies, and members of CISA plans to drive stronger adoption of secure cloud capabilities and reduce dependence on outmoded practices.

The magnitude of breaches like the 2019 attack on the SolarWinds ecosystem also led authorities to update guidelines for partnering with government agencies in the cloud. In 2021, the Department of Justice issued the Civil Cyber-Fraud Initiative to hold federal contractors to higher standards. The directive promises to identify aspects of suppliers' cybersecurity defenses that may be lacking or outdated.

Practice least privilege access

The combination of high volumes of identities and the intricacies of their permissions makes it nearly impossible to avoid errors and oversights in IAM. Intentionally or unintentionally, permissions become over-privileged, or temporary access is granted that never gets shut down.

Least-privilege access establishes a Zero Trust posture for onboarding third-party providers. The basic idea is to grant third parties only the access and rights — read, edit, publish, etc.— needed to fulfill agreed-upon roles.

Isolate risk from third parties

Cloud-based isolation, the new best practice mentioned earlier, keeps second-hand risk from third parties and other advanced cloud threats from leaving the cloud. Let's take a look . . .

A new security best practice: Isolate threats in the cloud

Security should go unnoticed, protecting workers without stifling productivity. Remote Browser Isolation (RBI), often referred to as browser isolation, lets users work in browsers safely without fear of threats reaching endpoints. Content — good and bad — is presumed malicious and stays in the cloud until proven safe.

How Change to browser isolation works

With more work taking place in browsers, and more browsing happening in the cloud, a browser isolation platform acts as a middleman to protect endpoints from malware. Layered on top of existing security stacks, the platform keeps online threats from downloading onto an agency's network, even as users browse non-government sites. The process also isolates users to keep human error from adding new vulnerabilities.

A safe space to verify threats

Instead of users connecting directly to sites, browser isolation inserts a cloud-based intermediary between endpoints and servers. The intermediary interacts with the server and delivers screenshots or mirrored versions to users so they can do what they need to do in a safe environment without exposing endpoints to malware.

A win for IT

Isolating threats in the cloud:

1. Prevents initial access
2. Adds an additional, protective security layer
3. Modernizes security architectures
4. Scales seamlessly across the globe
5. Preserves the native user experience

Up to 50% of HEAT attacks observed come from uncategorized websites. That means attackers are successfully exploiting the shortcomings of URL categorization to compromise sites and/or buying domains used to execute new techniques.

DoD avoids future spending

"Over time, as the department leverages more cloud services, services need to go off DoD networks more often, those capacity requirements increase, adding to the cost of the upgrade. CBII, by translating the web browser experience off of the desktop and into a cloud, relieves a lot of that bandwidth requirement and therefore allows us to not operate or increase the capabilities at the same rate we otherwise would have.

Thus the $300M in cost avoidance."[4]

—DISA Comptroller
Christopher Barnhurst

4 https://breakingdefense.com/2020/11/disa-cloud-based-browsing-will-save-300m/

Browser isolation streamlines use of expensive bandwidth for massive savings on backhauling VPN traffic from remote work, or for processing by centralized tools. The right solution eliminates up to 90% of alerts — a major productivity enhancer for IT — and buys leaders time. With users protected as they browse the cloud, IT can build agile, dynamic security infrastructures in its own time.

Isolation and prevention: the first steps toward Zero Trust

Web isolation lets federal agencies address the first milestone in the MITRE ATT&CK framework: initial access. Turning away adversaries in the cloud prevents them from lying in wait and moving laterally through a network tagging high-profile targets. Browser isolation scales across multi-cloud environments protecting users on distributed laptops, mobile devices, SaaS platforms, and other vulnerable endpoints.

CBII makes the browser a safe space

90%
fewer alerts

50%
lead times reduced

Open up access without risk

Stopping cloud threats before they stop work

The ultimate prevention: keep threats from leaving the cloud

Letting attacks strike your network before you take action isn't "prevention." Instead of waiting to detect and remediate — which only works inside your environment — Menlo Security takes a uniquely preventive approach that keeps ransomware and evasive threats from ever gaining a foothold.

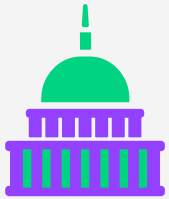
Isolation-powered cloud security

Zero Trust cloud-based isolation provides 100% protection, removing malware from web and email systems without special software or plugins. Menlo's Fedramp® Authorized Cloud Security Platform powered by an Isolation Core™ sequesters known and unknown threats to allow users to work safely in browsers and cloud-based environments.

The result? No risk to endpoints with no drag on workflows.

Automated and invisible to users

The only solution to deliver on the promise of cloud security, Menlo's Cloud Security Platform mitigates evasive threats that deliver malware while users work online to keep operations moving forward. Automated, preventive security takes place in the background, invisible to users and without burdening IT.



60+

Menlo Security Federal Government and Mission Partners

"If threats can't get in, they aren't really threats."

Keep ransomware, evasive, and third-party attacks from ever reaching your endpoints.

About Menlo Security

Menlo Security protects organizations from cyberattacks by eliminating the threat of malware from the web, documents, and email. It focuses on protecting the single biggest productivity driver for knowledge workers — the web browser.

Menlo's Cloud Security Platform prevents threats from entering an organization and secures data and application access in a single, global cloud-based offering. Our Elastic Isolation Core™ creates separation between the user, content and applications where security, policy and visibility are applied. With deep visibility inside the browser, adaptive policy enables the prevention of threats before they happen, as opposed to detecting and responding, organizations eliminate all threats, including Highly Evasive Adaptive Threats (HEAT) across web, email, SaaS applications and private applications.

HEATcheck

Menlo Security provides a lightweight penetration assessment to help organizations better understand any susceptibility to various HEAT attacks. The assessment leverages various real-world HEAT attacks currently being used by threat actors, safely allowing organizations to deduce their exposure. Menlo's HEATcheck tool does not deliver actual malicious content.

Get in touch with us.

Contact us today to learn if your organization is currently susceptible to these top web threats, but most importantly, how you can make them never happen in the first place.

www.menlosecurity.com

(650) 614 1705 | ask@menlosecurity.com

MENLO SECURITY