



# Reimagining online security for federal agencies.

Do more than chase cyber threats and bad actors. Isolate users and data from malware, ransomware, spyware and zero-day attacks.

eBook



## For federal agencies, cybersecurity is non-negotiable.

There have been far too many high-profile security incidents at federal agencies in the past few years, and the numbers appear to be growing. These hacks put national security and global supply chains at risk.

Breaches have exposed an inordinate amount of personally identifiable information (PII), including Social Security Numbers, personal health records and other HIPAA-protected information. These hacks can leave citizens vulnerable to identity theft and personal attacks while also casting doubt on the integrity of government systems.

Too often, the security tools and protocols commonly used by agencies are simply unable to protect systems and data. Recent high-profile attacks, such as the September 2020 hack<sup>1</sup> that exploited a known VPN weakness to steal access credentials from multiple users at a federal agency, underscore the threat.

The Government Accountability Office has **emphasized steps** that should be taken by agencies to develop cybersecurity strategies, secure systems and protect critical infrastructure, privacy and sensitive data, including intellectual property and PII. Yet, despite civilian agencies **spending** more than \$8 billion per year on cybersecurity, the threats persist.

Phishing emails, malicious websites, and destructive code hidden in attachments are all used by bad actors as a way into government systems, allowing them to exfiltrate data or damage the ability of agencies to perform their missions. Zero-day attacks may be the most threatening, as the malicious code can lay dormant for months before causing damage or hijacking systems and data – and once you’ve detected them, it’s too late.

The question, then, remains: even with massive agency investments in security software and equipment: why are cyber attacks on the rise... and succeeding?<sup>2</sup>

## Combatting human nature.

It’s an undeniable fact: despite regular training<sup>3</sup> and frequent reminders<sup>4</sup>, users still click on links in phishing emails or visit websites that may be compromised. In fact, a study Menlo Security recently conducted with a federal customer found a disturbing trend – over a 90 day period, with results extrapolated to the entire user population, more than 100,000 dangerous URLs are being accessed per month by this agency’s personnel alone. Extend that risk across government, and it’s clear that current tools aren’t enough to prevent cyber threats to your data and systems.

<sup>1</sup> <https://www.nextgov.com/cybersecurity/2020/09/hackers-take-data-further-reconnaissance-breach-federal-agency/168791/>

<sup>2</sup> <https://www.latimes.com/politics/story/2020-08-28/federal-work-from-home-cybersecurity>

<sup>3</sup> <https://public.cyber.mil/training/phishing-awareness/>

<sup>4</sup> <https://www.cio.gov/assets/resources/telework-infographic.pdf>

## The COVID-19 effect: **more endpoints, more vulnerabilities.**

Across-the-board teleworking initiated in response to COVID-19 kept federal personnel productive, and accelerated IT modernization efforts across government. For some agencies, such as the Veteran's Administration,<sup>5</sup> digital transformation programs that were already underway helped them quickly pivot to "maximum telework."

But as the number of remote endpoints have grown, so have the security risks. Security teams have less visibility into teleworkers' systems, and home WiFi can be considerably less secure than an agency's onsite network.

In June, the Pandemic Response Accountability Committee reported concerns from both the Environmental Protection Agency and the National Reconnaissance Office about "inadvertent spills and disclosures of classified information by employees performing unclassified work at home."<sup>6</sup>

With the likelihood that telework will continue to a significant extent going forward, including more remote access to classified data, these conditions set the stage for ongoing assaults that put systems and personnel at risk.



<sup>5</sup> <https://governmentciomedia.com/va-digital-modernization-foundation-covid-19-response>

<sup>6</sup> [https://www.oversight.gov/sites/default/files/oig-reports/Top%20Challenges%20Facing%20Federal%20Agencies%20-%20COVID-19%20Emergency%20Relief%20and%20Response%20Efforts\\_1.pdf](https://www.oversight.gov/sites/default/files/oig-reports/Top%20Challenges%20Facing%20Federal%20Agencies%20-%20COVID-19%20Emergency%20Relief%20and%20Response%20Efforts_1.pdf)

## Spending more isn't the answer.

Agencies continue to invest substantially in endpoint protection, enterprise antivirus, intrusion detection and other technologies that simply don't address the basic issue: any time a user's system directly connects to a compromised or hostile one, there's a risk of downloading malicious code.

Using current security tools alone to protect systems and data across your network, including edge and IoT devices, doesn't provide protection because they are reactive; by design, they wait for an attack to happen or for a signature they recognize to appear.


At the same time, security has to support the mission, not slow it down. Cyber solutions need to be transparent in action, so users can do their jobs without the latency and system overhead imposed by multiple gates and processes. For government agencies, security must also enable IT modernization, especially the move to cloud and SaaS-based operations for scalability, predictable SLAs and cost-effectiveness.

---

Federal **cybersecurity funding** proposed in the President's FY 2021 budget:

# \$18.8 billion

on par with FY2020 estimates but more than **\$1.8 billion** over FY2019 actual spending.



Spending by agencies on **insider threat** solutions alone is expected to grow to more than **\$1.1 billion** in FY2021.



350,000

New **malware** and potentially  
unwanted applications daily

700 million

malware expected within 2020.



## To secure the network, **change the assumptions.**

Most cybersecurity products and services are built on the belief that stopping attacks is as simple as detecting them as they hit the perimeter of the network. But phishing emails rely on authorized users simply making a mistake that bypasses security protocols. Meanwhile, detection of malicious code is imperfect; you have to know what you're looking for to identify the attack. The on-prem products used by many agencies often fail for the simple reason that they aren't located where the users or data are — which is why additional products are needed to help mitigate the effects of something that slips through.

Since new malware variants emerge daily, most security products require constant patching and updating of attack signatures. This creates an unending circle of updates that can't solve the basic problem: authorized users linking to malicious software hidden on the web, in emails and in documents.

VPNs, which in theory should shield remote users from threats, aren't the answer, either. With COVID-19 driving exponentially more government users to telework, bad actors are taking advantage of weaknesses in certain VPNs to gain access to protected systems.<sup>7</sup> Again, the issue is that security products are taking a flawed approach, trying to detect and nullify attacks at the edge of the network while still allowing users to communicate, search and collaborate online.

<sup>7</sup> <https://us-cert.cisa.gov/ncas/alerts/aa20-099a>

## The costs of imperfect security go beyond lost data.

Most Security Operations Centers (SOCs) are overburdened: chasing false alarms takes time and resources, and reimaging systems after an attack could bring operations, both internal and citizen-facing, to a halt for hours or days... or longer. This affects everything from personnel costs (and burnout) to trust in public institutions, potentially derailing the mission.

Plus, regular cyber hygiene takes an inordinate amount of time and effort. It can also mean taking down systems that are supposed to be up and running 24/7, such as VPNs,<sup>8</sup> while updates are made.

Traditional security software also imposes a significant hardware cost. Some tools require regular hardware refreshes, which can be as costly – or more expensive – than the software itself. And the protection they deliver still leaves IT security

teams scrambling to assess every alert – including false positives, which can be caused by software bugs or unrecognized network traffic and misdirect personnel from actual threats.

Rather than continue to rely only on AV, anti-malware shields and intrusion detection tools to provide protection, what's needed is a way to isolate users from risky online resources – a solution that delivers 100% protection from malware, ransomware, spyware and zero-day attacks that stem from the most exploited vectors: phishing emails, malicious websites and infected downloads.

It's time to take a more direct approach: instead of defending the perimeter, relocate – and isolate – *the target*.



<sup>8</sup> <https://us-cert.cisa.gov/ncas/alerts/aa20-073a>

# True Zero Trust is more than authentication.

The concept of Zero Trust Architecture is absolutely valid, yet most “zero trust” models don’t quite live up to the name, especially when the resource being accessed is online. Current zero trust implementations can only limit access to resources; there’s still a direct connection between user devices and online data that could be exploited.

Isolation, on the other hand, creates a virtual “air gap” between the network end user and the online world. Instead of opening a website directly in a laptop’s web browser, a virtual machine in the cloud fetches and executes all content served from the target website. A sanitized version of the website is then sent to the end user – fully functional, with all malicious code removed.

Malware, if there is any, can only affect the disposable container, and the cloud platform can detect a phishing website, putting it into read-only mode and alerting the user. This is true zero trust security; by assuming no web resources can be trusted, users are in effect separated from all potential threats.



## FedRAMP® Authorized web isolation drives greater productivity.

With an isolation workflow, clicking on links in emails or navigating to websites can no longer allow malware to enter the network environment, there's no direct connection from site to user device. For users, the process is completely transparent, as there is no latency or performance degradation.

In fact, our FedRAMP Authorized isolation model can actually improve productivity. Networks have traditionally been designed to support both web and internal traffic, but web demand has grown extensively, thanks to the shift to SaaS apps and multimedia sites. Most bandwidth control techniques involved throttling performance for some users or uses. But, video sites, such as YouTube and Vimeo, and many news sites, such as CNN, serve up high-resolution content by default in order to provide the best experience, which intensifies bandwidth requirements.

By splitting web traffic off of the internal network and configuring the cloud security platform to display video resolution per agency policy (i.e., limiting the resolution automatically), the virtual sites can deliver content faster to the end-user device without a noticeable drop in quality. This also can mean that parts of the web, which may have once been unusable for federal personnel, are now accessible under a broader range of connectivity conditions.



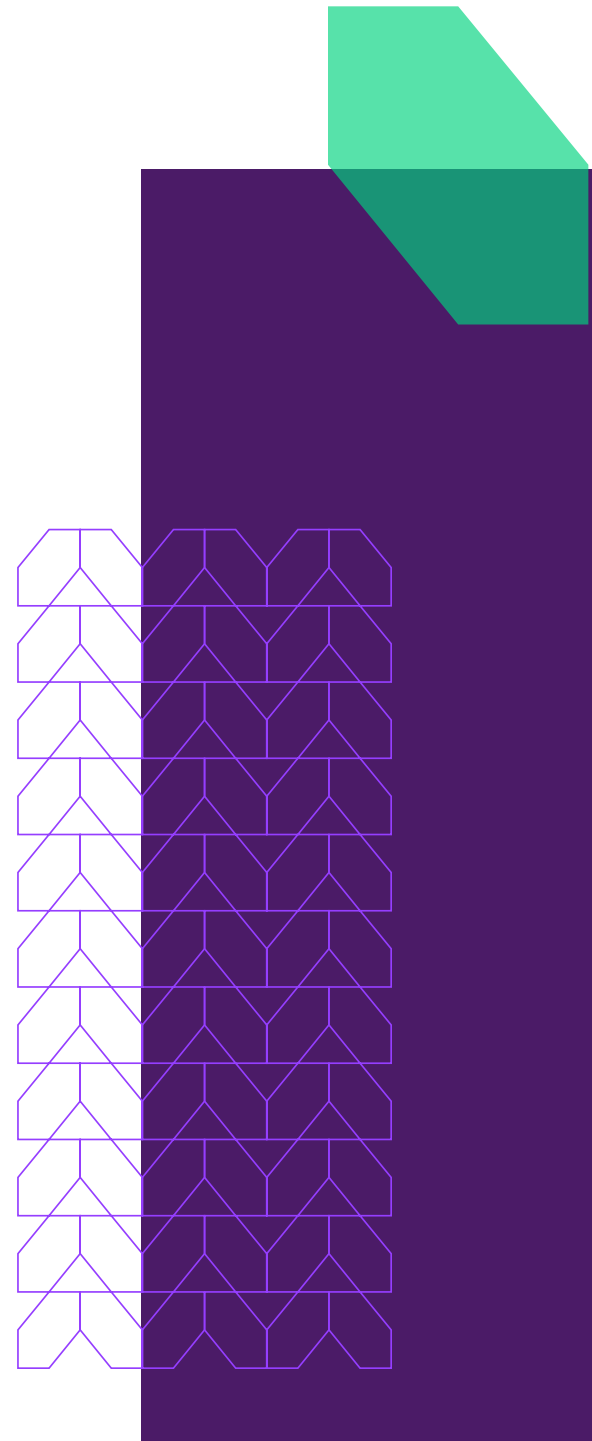
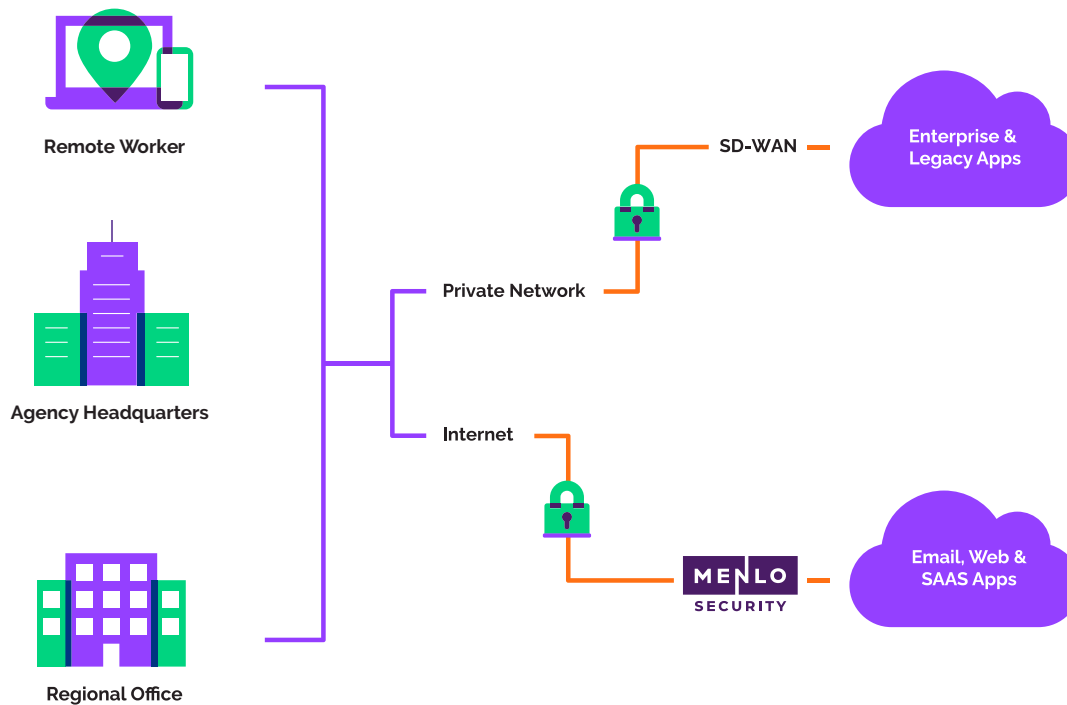


## Eliminating bottlenecks.

Productivity is directly tied to latency. In addition to variable connections over cellular or home Wi-Fi, VPNs can add overhead that slows down traffic. The impact is felt in slow file transfers, long waits for SaaS apps to respond and video conferencing that stutters and freezes.

These slowdowns also impact agency facilities, especially those in areas where Internet connectivity may be limited in terms of bandwidth.

Instead, the cloud-based isolation platform eliminates bottlenecks. Agencies can easily employ a split-tunnel VPN approach, which drives unclassified traffic directly to the cloud isolation platform, reducing bandwidth burdens. There's no longer a need to backhaul traffic through the government network or go through Internet Access Points (IAPs) or a Trusted Internet Connection (TIC) when dealing with unclassified information, moving the risk away from DoDIN or .gov networks.



## Part of your evolving security strategy.

The cloud isolation platform fully supports your IT transformation strategy, meshing easily with public, private and hybrid cloud environments. Rather than requiring you to “rip and replace,” cloud isolation can support your network today while helping you migrate to a more manageable, more secure future.

There are other advantages to this approach from an IT and security management standpoint:

### Centralized control

Security protocols can be applied to any or all users instantly, and web security can be enabled for hundreds of thousands of users in short order. Transparency and visibility into user connections and web behavior ensures that policies can be enforced.

### Near-instantaneous scalability

Because the functionality exists in the cloud, there's no need to install endpoint software on your personnel's devices. The platform can auto-scale as needed to support growing or variable requirements.

### Enhanced data loss protection capabilities

The cloud isolation model can also help protect against insider threats, both inadvertent and malicious. Data loss prevention (DLP) engines can only see so much; data can be hidden from the DLP stack through obfuscation techniques. But, cloud isolation provides 100% visibility into all data (files, post and put parameters, etc.) leaving the protected environment, providing an enhanced level of security in concert with your current DLP solution.

### Agency-wide visibility

Knowing what links users clicked on and where they go on the web can help you develop more effective cyber strategies. A simple, yet comprehensive dashboard can help you spot questionable activity and drill down into details.

### Anonymizing user identities

For government users, it's essential that they can use online resources without the owners of those sites knowing that the traffic originates with a federal agency. Shielding the source of the web request is crucial, as an adversary could use that information – i.e., the knowledge that someone at a specific agency is browsing a compromised site – to develop an attack. With cloud isolation, the source of the request is the virtual server, not the agency network, effectively hiding the originating IP address.

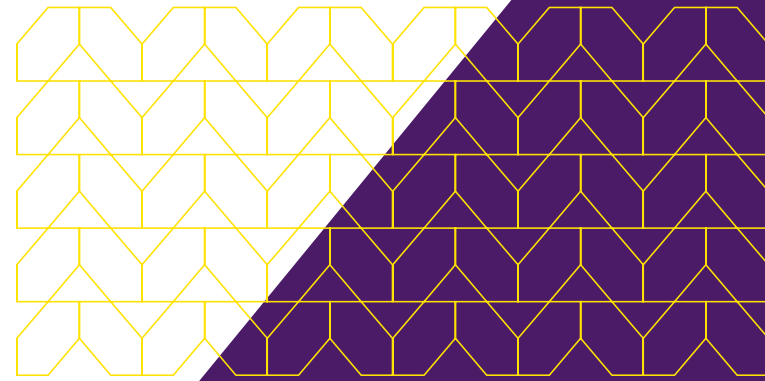
### Integration with existing infrastructure

A cloud-based isolation solution can augment current SD-WAN implementations; Internet traffic can be sent directly to the cloud service. Also, cloud isolation works with mobile device management (MDM) tools to ensure that smartphones and tablets are protected, fully supporting your remote work strategy.

## Supporting the mission, **anywhere work happens.**

For a remote workforce – whether teleworking, performing field data collection or performing maintenance on a flight line – high-speed, reliable access to data, apps and collaboration tools is a requirement. As already described, moving substantial parts of your network traffic away from TICs or IAPs can provide a huge benefit to bandwidth and throughput.

The secure cloud platform model works with your full portfolio of productivity and collaboration tools, including Microsoft 365, G Suite, Box, Salesforce and ServiceNow. SaaS apps now run in a virtual browser, just like websites, so documents can be opened and shared safely, even when they come from email attachments.

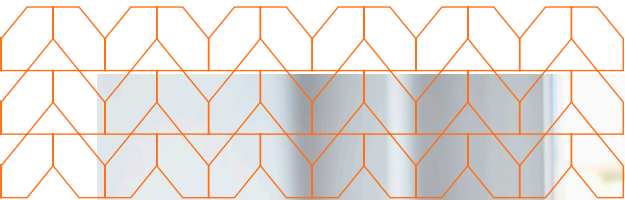


The isolation model provides **read-only access** to sensitive data, which eliminates the need for users to download documents approximately

**80 percent**

of the time





## **Productivity anywhere. Security everywhere.**

Current security measures simply aren't working. Instead of enabling greater productivity and confidence, they lead to an ever-escalating situation, where bad actors create new threats while security teams act to counter them as quickly as possible. Even if your security stack is 99.9 percent effective, it's that last tiny percentage that can leave your systems and data vulnerable.

Instead of keeping up with bad actors, leave them behind. The Menlo Security Cloud Platform, powered by the Isolation Core™, delivers uncompromising security against malware, ransomware and zero-day attacks. At the same time, you gain the real-world benefits of higher performance through bandwidth optimization, with simple-to-use yet comprehensive management controls.

By removing the issue of phishing emails and suspect websites, you can eliminate the vast majority of threats to essential systems and data. For users, the experience is transparent. For your agency, the Menlo Security Cloud Platform means keeping resources – and focus – where it belongs: on the mission.





# Stop ransomware, malware and zero days across your agency now.

Put an end to the threats posed by phishing and malicious websites while improving online performance for all users.

[menlosecurity.com/solutions/government](https://menlosecurity.com/solutions/government)

[www.menlosecurity.com](https://www.menlosecurity.com)

(650) 614 1705 | [ask@menlosecurity.com](mailto:ask@menlosecurity.com)



© 2021 Menlo Security, All Rights Reserved.

