A guide to zero trust for government agencies

How to design and implement a zero-trust approach with HP Wolf Security[1]

This guide discusses solutions that can enhance your existing hardware and security portfolio, designed with zero-trust principles that deliver endpoint security for federal, state, and local agencies.

As governments increasingly rely on their networks and the data they collect, they become steadily more attractive targets for cybercriminals—both internal and external. A zero-trust approach to endpoint security is one of the most strategic investments any agency can adopt, serving to secure all users, devices, and applications.

Background

The concept of zero trust is based on the principle that external and internal threats exist on a network at all times. It is a way to make timely decisions against cyberthreats using device and user identities, firmware and software configuration, and broader contextual information.

A number of federal mandates and resources encourage agencies at all levels of government to modernize their cybersecurity posture using zero trust, including:

- U.S. National Cybersecurity Strategy,[2] which places greater responsibility for cybersecurity on federal contractors, technology companies, and critical infrastructure owners and operators
- Department of Defense Zero Trust Strategy and Roadmap[3]
- U.S. Government Accountability Office description of zero trust architecture[4]
- Infrastructure Investment and Jobs Act of 2021, which included $1 billion for state and local agencies to shore up cybersecurity over four years[5]

Zero trust applied at the source

Many, if not most, agencies rely on multiple generations of IT assets spread across physical, virtual, and cloud environments. From regional plans to constituent records to infrastructure blueprints, governments create and maintain highly valuable information.

Cyberattacks against governments jumped 95% in the second half of 2022 compared to the same period in 2021,[6] and phishing attacks—where bad actors try to get users to click on malicious links that bypass security—have reached all-time highs.[7] That means governments adjusting to hybrid work models can no longer rely on firewalls to protect themselves. Instead, they need to protect endpoints.

Government agencies often house extremely sensitive data in secure facilities. The sad fact, though, is that security is breached and data is stolen every day. Many breaches can be triggered by a single end-user mistake, like clicking on a phishing link, with significant consequences.

Attacks can compromise anything from personally identifiable financial and health data to national security information or other data that safeguards the integrity of government institutions.

Maintaining workflow while tightening security

It is impractical to isolate people from the data they need to do their jobs and serve the public; people are, after all, human, and they make mistakes. But by the same token, a transition to a zero-trust model must ensure no degradation of an agency's security posture. Every zero-trust journey is unique, and no two agencies will implement it the same way.

HP Wolf Security can help agencies manage security risks posed by hybrid work. It offers a product portfolio designed with zero-trust principles to protect against phishing, malware, and ransomware attacks. HP makes PC and printer security simple and flexible to strengthen protection for governments, their workers, and the citizens who depend on them, with no special knowledge or actions required by end users. HP commercial PCs and printers are secured with HP Wolf Security[8] at every level, from factory services to apps and data, creating a secure foundation that protects against cyberthreats.

Our approach to this challenge is simple: We apply zero-trust techniques on every potentially risky activity on your employees' computers, focusing on the highest-risk actions:

- Opening email attachments like PDF files, spreadsheets, presentations, or word processing documents
- Web browsing and clicking web links in chat clients
- Opening files on USB devices

Security through the PC network

HP Sure Click Enterprise[9] is a transparent added layer to your existing security solutions. It applies zero-trust principles to endpoint security to stop even undetectable threats. When and if a breach occurs, Sure Click Enterprise helps IT teams identify it quickly, limit its impact, and rapidly recover affected systems, data, or devices. Using defense-grade hardware-enforced isolation and containment technology, Sure Click Enterprise helps government agencies stay ahead of continuous attacks and threats from bad actors.

As the flagship offering in this HP Wolf Enterprise Security portfolio, Sure Click Enterprise is the key element of our zero-trust strategy. Sure Click Enterprise places each user task (such as opening an email attachment) into an isolated, hardware-enforced micro-virtual machine (micro VM). This prevents malware from escaping the task it arrived in, so it can't infect the user's computer or anything else on the network. When the process is complete, the micro VM is destroyed, along with the malware.

User productivity remains unaffected, because users don't have to do anything different. They don't have to change daily behaviors to trigger the threat containment feature. They are free to read, edit, save, and print documents as usual without being disrupted.

HP takes the zero-trust approach one step further by leveraging the advanced security capabilities built into all modern PC hardware.

Endpoint security software that lacks hardware enforcement is always susceptible to being defeated through compromise of the operating system or underlying infrastructure. But Sure Click Enterprise uses the security hardware assist in today's Intel® and AMD CPUs to create the micro VMs and establish per-task micro-segmentation.

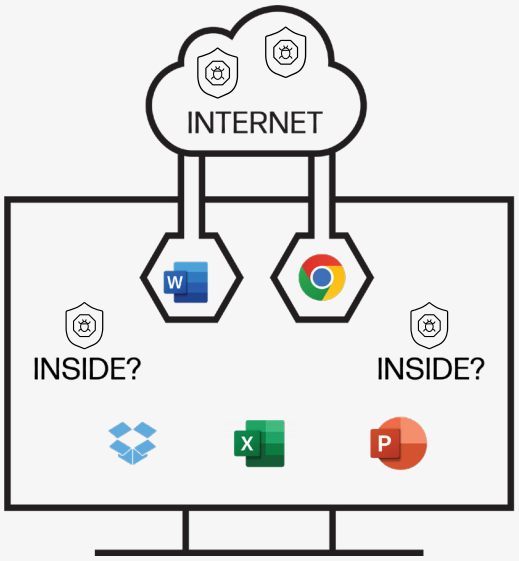
Applying zero-trust principles to the entire stack creates a threat-prevention model that is far harder to subvert. Federal IT teams receive actionable threat intelligence to help strengthen the agency's security posture and reduce the negative impacts of breaches.

HP Wolf Security applies zero-trust principles to create a more secure network and reinforce best practices, such as defense-in-depth, across the entire product portfolio to help enhance resiliency, limit exposure, and minimize the damage caused by a cyberattack.

Relieve overworked federal IT teams with endpoint-enforced zero trust

A sound zero-trust approach is one that combines efficiency with effectiveness. Unlike alternative solutions, neither HP Sure Click Enterprise nor HP Sure Access Enterprise[10] requires constant updates to stay relevant. Both products are equally effective at defeating zero-day attacks, and neither needs to be customized based on application usage.

Threat prevention from HP Wolf Security, based on zero-trust principles, vastly reduces the pressure on security operation centers (SOCs) and incident response, because most malware is eliminated before it can infect even a single device. That translates into fewer alerts requiring investigation, less device remediation, and higher user productivity.



Application isolation secures high-value protected applications from the rest of the environment.

As government cybersecurity teams grapple with talent shortages, they need solutions that help them do more with less. Security must be enabled at multiple levels with automatic updates that don't require fully staffed teams to continually monitor and manage security. Limited time and budgets can be reallocated away from detection and response to further optimize a hybrid work environment and help your agency stay flexible and resilient.

Summary

Government agencies rely heavily on in-person connections. But with 69% of public servants now working remotely at least part of the time,[11] a zero-trust approach has become a key component in today's environment.

HP Wolf Security uniquely delivers on a zero-trust approach by applying threat prevention at the source and putting protection on the endpoint. Federal IT teams don't need to worry if their user is remote or in the office, or if the data they access is in your data center or the cloud. Hackers and threat actors are stopped in their tracks in a way that eliminates the need to remediate the user's PC.

HP Wolf Security should be a key component of a robust IT security architecture for government agencies and their workers, so they can stay safe themselves, operate at scale, and strengthen protection for the citizens who depend on them.

LEARN MORE AT HP.COM/WOLF

HP WOLF SECURITY

[1] HP Wolf Enterprise Security is an optional service and may include offerings such as HP Sure Click Enterprise and HP Sure Access Enterprise. HP Sure Click Enterprise requires Windows 8 or 10 and Microsoft Internet Explorer, Google Chrome, Chromium or Firefox are supported. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files, when Microsoft Office or Adobe Acrobat are installed. HP Sure Access Enterprise requires Windows 10 Pro or Enterprise. HP services are governed by the applicable HP terms and conditions of service provided or indicated to Customer at the time of purchase. Customer may have additional statutory rights according to applicable local laws, and such rights are not in any way affected by the HP terms and conditions of service or the HP Limited Warranty provided with your HP Product. For full system requirements, please visit www.hpdaas.com/requirements

[2] Covington, "March 2023 Developments Under President Biden's Cybersecurity Executive Order," April 28, 2023, https://www.insidegovernmentcontracts.com/2023/04/march-2023-developments-under-president-bidens-cybersecurity-executive-order/

[3] U.S. Department of Defense, "Department of Defense Releases Zero Trust Strategy and Roadmap," November 22, 2022, https://www.defense.gov/News/Releases/Release/Article/3225919/department-of-defense-releases-zero-trust-strategy-and-roadmap/

[4] U.S. Government Accountability Office, "Science & Tech Spotlight: Zero Trust Architecture," November 18, 2022. https://www.gao.gov/products/gao-23-106065#:~:text=Zero%20trust%20architecture%20(ZTA)%20is,once%20they%20are%20granted%20access

[5] Cybersecurity & Infrastructure Security Agency, "State and Local Cybersecurity Grant Program," September 16, 2022, https://www.cisa.gov/state-and-local-cybersecurity-grant-program

[6] CloudSEK, "Unprecedented Increase in Cyber Attacks Targeting Government Entities in 2022," December 30, 2022, https://www.cloudsek.com/whitepapers-reports/unprecedented-increase-in-cyber-attacks-targeting-government-entities-in-2022

[7] Help Net Security, "Phishing reaches all-time high in early 2022," June 15, 2022, https://www.helpnetsecurity.com/2022/06/15/2022-total-phishing-attacks

[8] HP Wolf Security for Business requires Windows 10 or 11 Pro and higher, includes various HP security features and is available on HP Pro, Elite, RPOS and Workstation products. See product details for included security features.

[9] HP Sure Click Enterprise requires Windows 10 and Microsoft Internet Explorer, Edge, Google Chrome, Chromium or Firefox are supported. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files, when Microsoft Office or Adobe Acrobat are installed.

[10] HP Sure Access Enterprise is sold separately. For full system requirements, please visit System Requirements for HP Sure Access Enterprise for details.

[11] U.S. Office of Personnel Management, "2022 Federal Employee Viewpoint Survey Results," November 30, 2022, https://www.opm.gov/fevs/reports/governmentwide-reports/governmentwide-reports/governmentwide-management-report/2022/2022-governmentwide-management-report.pdf

4AA8-2450ENW, Rev 1, July 2023