# GOVERNMENT ENDPOINT

**SPOTLIGHTS**

**Industry**
Government

**Use Case**

Protect Windows-based endpoints (e.g., desktops, servers, workstations, Windows CE devices) from zero-day malware and exploits.

**Business Benefits**

- Kill zone at the endpoint for exploits to protect against targeted government attacks at all endpoints
- Compensation to slow patch cycles and end-of-life (EoL) product transitions
- Overcome insufficiency in today's antivirus solutions in protecting government endpoints

**Business Drivers**

- **Governments are among the most highly targeted networks.** Use to protect government systems (e.g., servers, workstations, virtual desktops) from exploits for zero-day vulnerabilities, APTs, and never-before-seen malware.
- **Slow government patch cycles.** Use as a compensating solution to patch management.
- **Highly sensitive SCADA controls in military and energy operations.** Protect key ICS/SCADA systems from attacks.
- **Mobile government workers – afield, afloat and airborne.** Control executable use from mobile media (e.g. USB, CD-ROM drives) where such media is not controlled in government installations.
- **Compliance to specific government mandates.**
- **Endpoint threat prevention as part of modernized defense in depth.**

**Business Problem**

As we know, governments globally are among the most highly targeted networks. From political campaigns to government personnel to intelligence and troop planning, government data is of great interest to nation-states and others for a variety of reasons. Accessing sensitive government data means accessing the assets that can connect to it or house that data. Servers, workstations, virtual desktops and other devices can all suffer from vulnerable operating systems and applications – a way in for a would-be attacker. New exploits to take advantage of a vulnerability and new malware appear daily, and slow government patch cycles make this even more concerning.

New attack tactics also appear regularly to circumvent security controls. Antivirus technology or similarly outdated processes simply cannot protect government assets any longer from today's swiftly changing threat environment.

In addition to the sensitive assets that access and house sensitive data, ICS/SCADA devices that control sensitive government processes from energy systems to military transportation, navigation, fueling and weapons systems are also lucrative targets. Rather than confidentiality, the focus of these systems is on their integrity and availability – ensuring they are functional, accurate and available to the services that rely on them.

Government employees and contractors, like their commercial counterparts, are also now more mobile than ever – afield, afloat and airborne. Government policy-makers want ongoing access to their constituents, and government wants to be nimbler and accessible from more locations to provide timelier – and smarter – services. This means security is necessary for mobile devices often more easily targeted than those in government installations.

Finally, as often happens in bureaucratic processes, security mandates and regulations tend to fall behind the curve of the threat environment. Government agencies are then left to mark compliance check boxes that don't sufficiently protect their organizations. If they settle for this low level of protection, they could be blamed for a significant breach of sensitive government data or operations.

**Traditional Approaches**

When government agencies have tried to address their endpoint security requirements in the past, they had few choices other than antivirus protection. As we know, antivirus technology became outdated with the advent of online forums to buy/trade malware and

malicious services which made it easier to change malware and harder for static analysis operations such as antivirus technology to keep up. Antivirus technology was fine for those agencies who only wanted to meet a minimum standard – that is, to check a box for compliance and not actually defend their assets from today's threats. In addition to these challenges, traditional endpoint technology enjoys no communication with, much less automation from, other network sensors of their threat findings and protections. As a result, network and endpoint security capabilities have remained separated, siloed efforts without the leverage that government agencies should enjoy with the modernized machine learning and automation capabilities available today.

More recently, anti-exploit technology has become available but, unfortunately, not for large-scale enterprise deployments as is the case in most government networks.

### Palo Alto Networks Approach

To ensure governments have a realistic approach to cyber risk reduction and threat prevention that's adapted to today's threat conditions, Palo Alto Networks enables several things to happen on a government network:

- **Visibility** – Understand what's already on your network to plan an effective strategy of what to allow and disallow that both works for your end-user needs and also effectively protects your assets and operations;
- **Reduce the attack surface across killzones at every stage of the cyberattack lifecycle** – In numerous successful attacks against governments worldwide, adversaries have used each stage of the cyberattack lifecycle to successfully gain further access to the government's network [Figure 1]. Governments must think in the context of the entire lifecycle if they hope to prevent successful attacks.

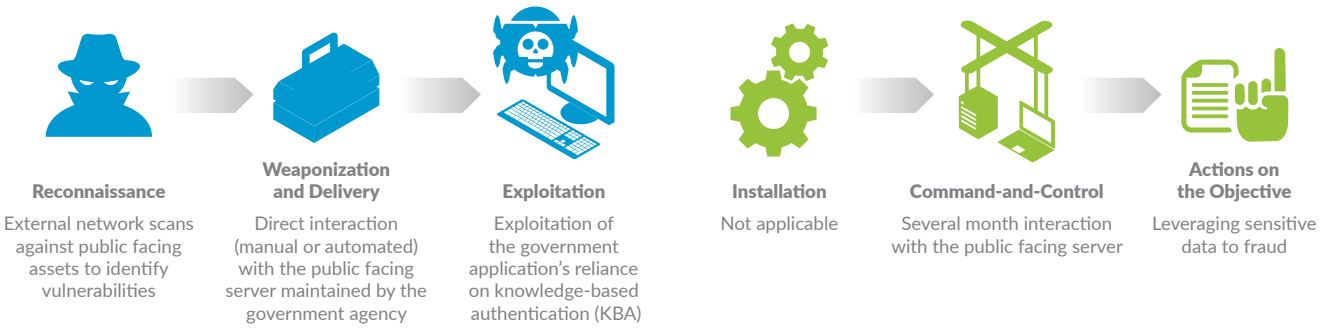



**Figure 1:** Government attack showing each stage of the cyberattack lifecycle used by the attacker

With the WildFire™ malware analysis environment communicating with all of the security capabilities on the pre-emptive Palo Alto Networks sensors (physical or virtual appliances), an attacker can use each piece of malware once, at most, anywhere in the world, and only has seconds to carry out an attack before WildFire renders it entirely ineffective. The platform approach, where each capability automatically reprograms itself to convert what's learned into automatic prevention, all but eliminates the opportunity for an attacker to use unknown and advanced malware to infect a system.

- Enforcement of whitelisting across the network, contextually, based on the users and user groups' needs, at each zone. This means at the perimeter, at the endpoint, at the data center edge, in the cloud, and between VMs.
- Establishment of "Zero Trust" policies for user groups, such as the warfighter vs. the administrator, the flag officers vs. the enlisted soldiers, the field agents vs. the Human Resources department, etc. based on role, department or other delineation while blocking known malicious DNS, URLs and files. To further reduce the surface area of attack, you can also control on the endpoint where executables can be run from – from attached media or external devices, out of the temp folder, etc. (For the endpoint, you can use Traps to set such Restriction Rules.)
- Blocking of known malware and malicious links in email, malicious URLs, and malicious DNS.
    - Decryption of any encrypted network traffic for inspection that meets your criteria for doing so.
    - File analysis on all new and unidentified files on the network – immediately submitting these files to the WildFire malware analysis environment – on-site/on-premises or in the Palo Alto Networks Threat Intelligence Cloud – to identify, analyze and automate protections on all pre-emptive network sensors for those rendered malicious (i.e., zero-day malware).

Beyond all of the above network threat prevention automation from the platform network sensors, the endpoint solution (Traps) automates a multi-method approach to prevention:

- **Exploit** prevention of attempts to compromise vulnerable assets and sharing with the network for further threat prevention at the pre-emptive network sensors. By "trapping" exploit techniques, it can thwart a successful breach of the endpoint. See Exploit Protection Rules.
- **Malware** detection and prevention: Any executable file a user or endpoint tries to open triggers a series of potential actions to render a verdict to allow or disallow a file to execute. Regardless of the ultimate verdict, administrators always have the final say in what is or is not allowed to run in their environment.

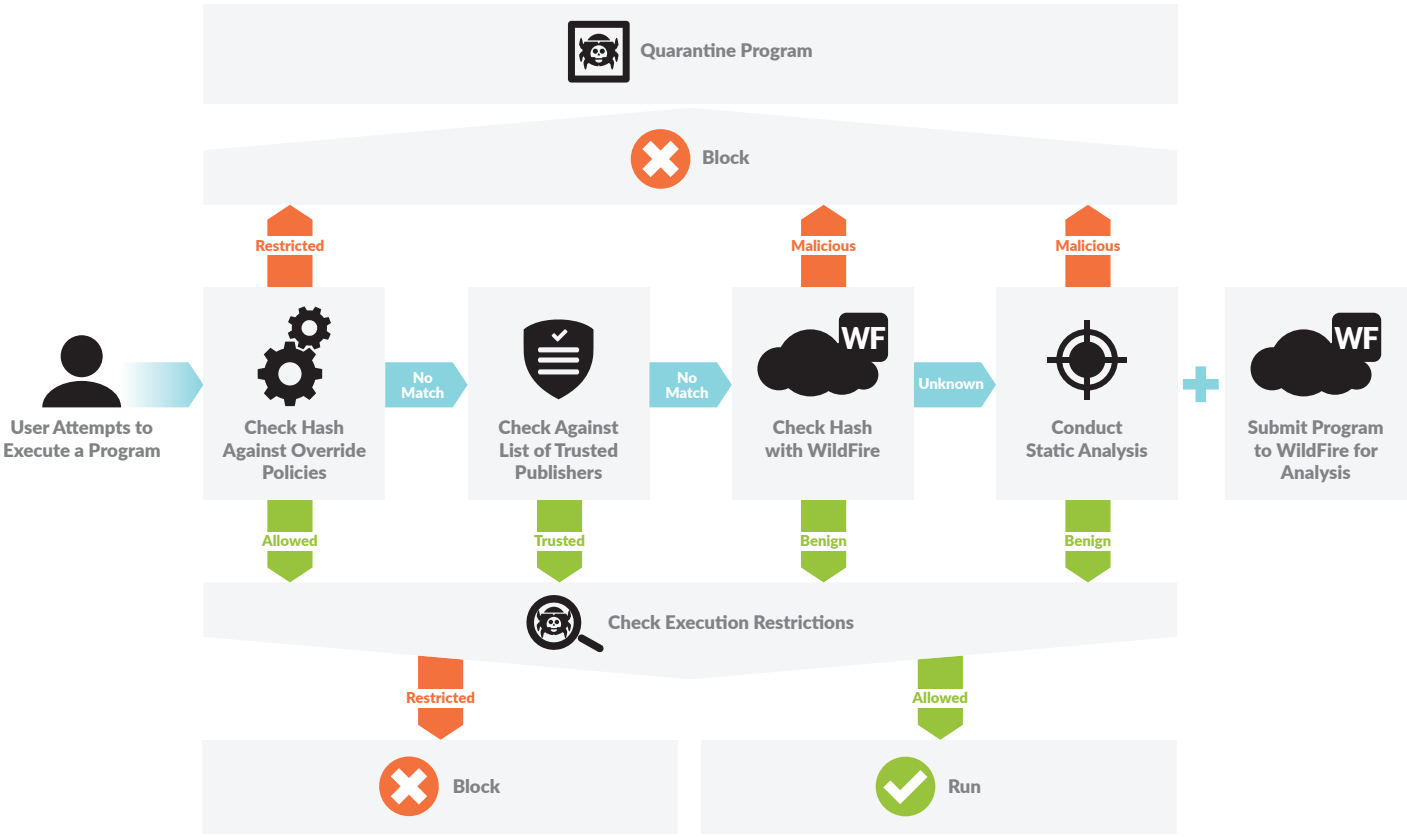



**Figure 2:** Traps handling of files a user or devices attempt to execute

- Before files are further analyzed, two things can happen:
  - Admin override policies and other policy restrictions can determine actions on the file. Examples of policy restrictions include:
    - Block unsigned executables.
    - Block executables launched from specific network locations or devices.
      Any file blocked in this way triggers a security event alert to the ESM and can be configured to alert/educate the end user.

    And/or

  - A Trusted Publisher list can be checked to determine an appropriate action. Files signed by "Trusted Publishers" can be approved to run. These files are also submitted to WildFire for analysis. [Trusted Publisher lists are maintained by Palo Alto Networks and updated in Content updates similar to those for the next-generation security platform.] Files with unknown publishers continue to hash checking as described below.

File hashes are also checked for malware status in the local agent cache; then if unknown, in the Endpoint Security Manager (ESM) server (database) cache; then if still unknown, in the WildFire malware analysis environment – for a verdict. See Malware Protection Rules. For "malicious" verdicts, Traps automatically reprograms itself to prevent the execution of that file from that moment on. The actual flow for all of this is depicted in Figure 2.

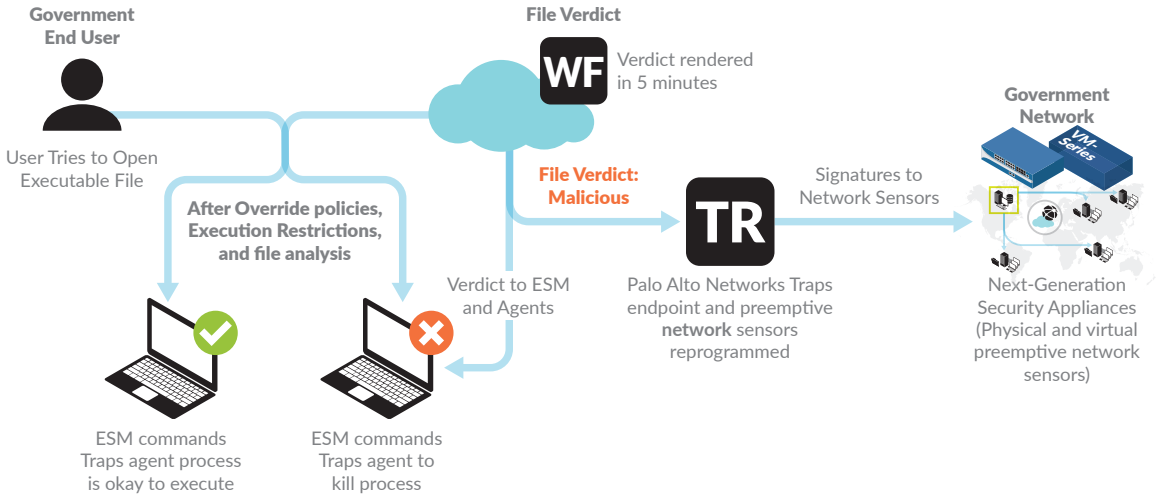



**Figure 3:** How Traps benefits the rest of the network

Any files whose hash ultimately returns an "unknown" verdict, after all checks above, can automatically be sent to WildFire for further analysis. While awaiting a WildFire decision, a file is also run through static analysis on the endpoint for a potential decision. (Admins can configure which files to send for analysis. An administrator can also determine, through policy, whether to run the file while awaiting the verdict for no connection, unknown verdicts and malicious verdicts.)

WildFire renders malware decisions in ~300 seconds and provides feedback to Traps (to the agent through the ESM) and, for malware, provides signatures to all pre-emptive network sensors. [Refer to Enable WildFire.] This holistic endpoint-to-network approach benefits the entire network. (Figure 3).

**Note:** The frequency of WildFire verdict updates for all Traps caches, how far back to look for changes, and file sizes for submitting files, are all configurable.

For any government agency that wishes to store forensics on endpoint security events – including files accessed, modules loaded into memory, URIs accessed, and ancestors of the process that triggered the security event – for further analysis, you can configure what data to collect and other rules for doing so. [Refer to Define Forensics Collection Preferences.]

And it can do all of the above in an enterprise-class deployment like the one described below.

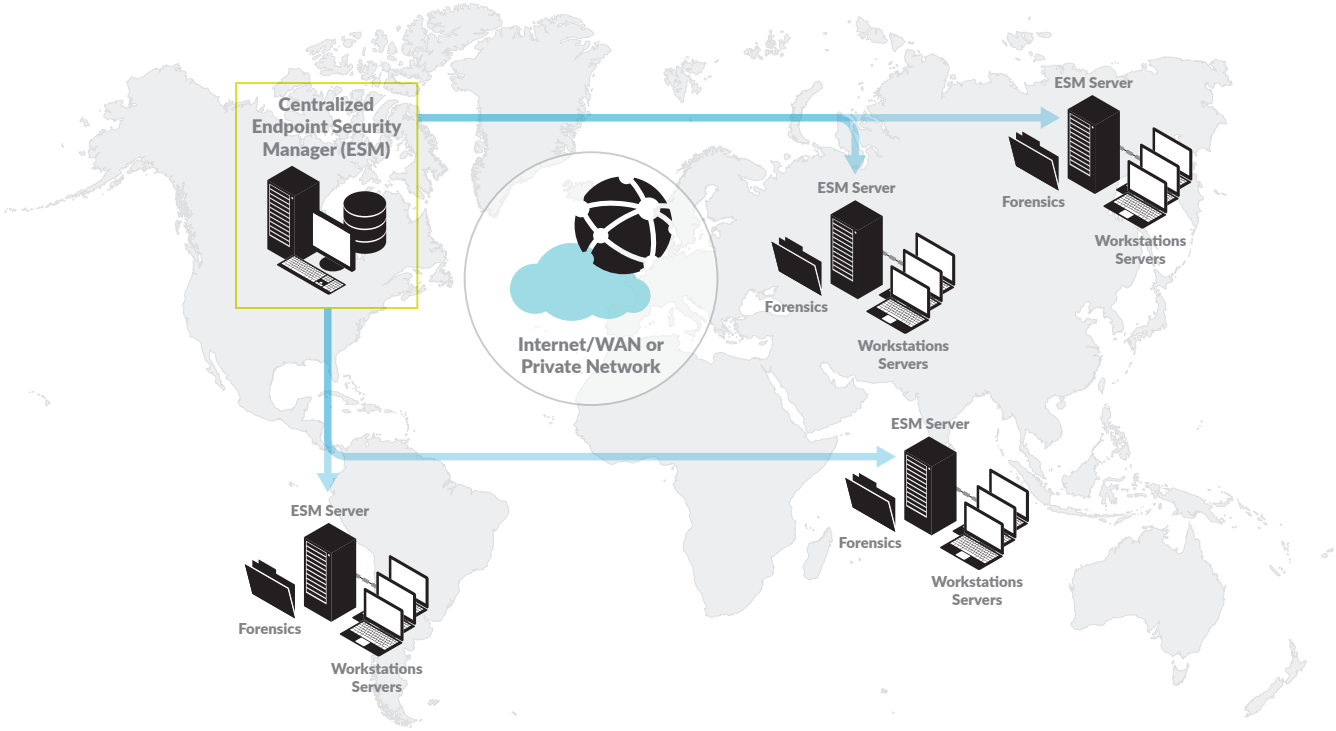
### Example Government Deployment

A government agency deployed Traps in a large, geo-dispersed installation of thousands of sensitive workstations, consisting of laptops and desktops and approximately a thousand servers. Today, it is managed by one centralized management platform and will likely evolve to a hub and spoke model in which separate management stations at the disparate geographies manage a subset of devices to ensure both the greatest security and privacy associated with the local environment and the fastest throughput to its protected assets downstream.

This government agency shared the same business challenges and drivers noted above. The agency had indeed modernized its approach to protecting its assets, which is commendable, by using an anti-exploit technology. As noted, with the swiftly changing threat environment, it's critical to apply more modernized security controls and processes to government assets. However, while good at its function, it was unfortunately not capable of the enterprise-level management and scale for a government network of this size.

Similar to other compliance mandates in the government and commercial sectors, this agency was subject to sub-par requirements within a security mandate insufficient for the modern threat environment. To its credit, the agency chose to focus instead on protecting its network – not settling for checking a compliance box.

Given the sensitive nature of this deployment, the below architecture reflects what a Traps deployment over similar network conditions might entail but does not represent this particular government agency deployment.




This deployment scenario supports up to 40,000 Traps agents (10,000 per ESM server) in a multi-site environment that consists of the following components:

- One dedicated database server
- One ESM console in the same location as the database for managing the security policy and Traps agents
- One ESM server for every 10,000 Traps agents (for example, 25,000 Traps agents requires three ESM servers)
- One forensic folder for each ESM server that is accessible by all endpoints for storing real-time forensic details about security events
- (Optional) Load balancer for distributing traffic across ESM servers
- (Optional) External logging platform, such as a SIEM or syslog
- (Optional) WildFire integration

In this example, the sites above each need to support up to 10,000 Traps agents. To support this scenario, each site contains an ESM server that retrieves the security policy from the database located in headquarters. The agents connect to the Endpoint Security Manager using their local ESM server, the primary server, and use the ESM servers at other sites as secondary servers.

**Note:** Other deployment scenarios – including multi-ESMs in multiple locations and stand-alone site deployments – can also be used.

Required products:

- Traps agent
- Endpoint Security Manager (ESM) – the Traps management server

Deployment guidance:

- Prerequisites to Install the ESM Console
- Prerequisites to Install the ESM Server
- Prerequisites to Install the Database
- Traps Deployment Scenarios

Deployment assumptions:

- **System backups** – The machine(s) in question have a current backup in the event of system corruption during installation.
- **Installation day/time** – Care should be taken to perform installation when necessary personnel are available to assist, in the event that installation does not proceed as planned. If installation occurs from a remote site, secure someone on-site to assist in installation and recovery efforts.
- **Back-out plan** – There is a well-documented back-out plan in the event that installation does not proceed as planned.
- **Production cycle** – The implementer is fully aware of the production cycle and status of the system prior to installation. Care should be taken so that installation does not adversely affect production.
- **Remote installation** – The location of installation should be taken into consideration, especially if it's remote. If installation does not proceed as planned, local personnel may be required to assist with installation or recovery efforts.
- **System integrity validation** – The implementer has a well-documented process to determine if the system is operating within acceptable parameters both prior to and post installation.

## Additional Palo Alto Networks Resources

This particular government agency uses a full-time Resident Engineer, and chose an Enterprise License Agreement, which was the most cost-effective approach for its use of other Palo Alto Networks appliances serving different functions on the network. Such services are described below. In addition, please refer to all online Traps technical documentation at the links above and below.

### *Services to Assist Customers With Their Deployment*

#### Support

Palo Alto Networks Customer Support offers multiple Support packages: Standard, Premium and Premium Plus. We continue to innovate by automating the discovery of related cases to increase productivity and get you to a resolution faster. You can also opt for your own Technical Account Manager, as an optional, subscription-based extension of Premium Support. Premium Plus provides both a designated technical support engineer and technical account manager, who will learn and understand your deployment at both a technical and business level. This in-depth understanding accelerates incident resolution.

#### Consulting

Palo Alto Networks Consulting Services provide access to specialized talent knowledgeable in ensuring the safe enablement of applications. By matching talent to task, we can deliver the right expertise at the right time, dedicated to your success.

- **Resident Engineer:** The Resident Engineers provide on-site product expertise and are uniquely qualified to advise how to get the most out of your next-generation platform.

#### Education

Training from a Palo Alto Networks Authorized Training Center delivers the knowledge and expertise to prepare you to help protect our way of life in the digital age. Our trusted security certifications give you the Next-Generation Security Platform knowledge necessary to prevent successful cyberattacks and safely enable applications.

## Next Steps

Government endpoints are a critical path to sensitive government data and are central to government operations. Malicious, unauthorized changes and access to these systems can have a significant impact on an agency's operations and, potentially, that of the country. They can be protected against today's swiftly changing threat environment in a manner that is minimally disruptive to government operations and meets the productivity needs of the end user – whether military soldier, airman, sailor or government civilian.

For further information and experience with the product:

- Register for an Ultimate Test Drive for Traps
- Download the Traps 3.4 Administrator's Guide