Enterprise Security Platform for State, Local, and Provincial Governments

STATE AND LOCAL GOVERNMENT CHALLENGES AND INITIATIVES:

- New demands placed on networks not built to withstand modern threats
- IT teams must deliver new services without additional budgets to support them
- Each new initiative increases the amount of work required in order to maintain visibility across siloed security systems
- Every network has unique requirements and configurations, and are usually managed by a distributed IT organization
- Networks serve a broad range of people, with varied access rights, all of whom control their own devices and apps

SUPPORTING AND SECURING MODERN CITY, STATE AND PROVINCIAL GOVERNMENT NETWORKS

Today, the drive to "Smart government" is changing the dynamic of government services and networks. IT teams who run government networks must support new initiatives that generate revenue, provide connectivity to utilities and other critical infrastructure, supply connectivity for libraries, government offices, transportation agencies and schools. Some of these programs include:

New applications or services

- Public demand is driving the need for new online services: Smart Safety, Smart Utility, Smart Transport and other Smart City or Government services require mobile-enabling government networks. Paying parking tickets or taxes, arranging transportation, checking utility usage, access to GIS/mapping data or other public records creates more efficiency but requires a new approach. IT teams must respond accordingly with specialized networks designed for high availability, commerce, etc.

Wi-Fi deployments

- IT organizations no longer have to just think about networks that support specific buildings or departments. They must provide Wi-Fi coverage to adequately accommodate entire cities—with a varied set of users who all have different devices, use cases and limited understanding of the risks they can pose.

Data Center consolidation and/or virtualization

- IT teams must consolidate and simplify their data center architecture, between the data center and the various networks it supports. While this allows for scalability and cost efficiencies, it also adds complexity to the security and governance aspects of supporting a variety of users and applications to whom they provide network access, with customizable security permissions and access privileges.

More citizen interaction through Social Media engagement

- Governments, such as law enforcement organizations, are engaging every day citizens using social media like never before. At the same time, government services are being delivered to the public online to offload manual/face-to-face processes: emergency notifications, voting updates, and other initiatives. Yet allowing this engagement also exposes networks to unknown malware and malicious access, which can often be hard to detect.

New threats

- With the growing interest in hacktivism, with attackers making political statements by attacking government services, as well as other forms of threats, government security teams must be more vigilant than ever. They must ensure not only the protection of sensitive data, but the resilience of government networks meant to serve the public.

paloalto networks

While IT teams may have security solutions in place, they typically have a silo'd set of tools, each providing a different security function which is uncorrelated from the others. The teams typically lack user-specific and application visibility of what is running or being used on their networks. Each of these networks have unique requirements and configurations, and are usually managed by a distributed IT organization. What's more, these networks serve a broad range of people, many of whom are the general public who use their own devices and applications when accessing their services.

Some of the challenges IT teams face include:

- Fighting hacktivism, zero day threats or malware with manual, unscalable approaches that can't stand up to the new wave of threats
- Protecting government services and citizen data while opening networks to enable greater citizen engagement and mobile applications to improve efficiency
- Serving many different users or constituent needs, requiring sufficient access controls to limit extraneous and internal attack vectors
- Managing disjointed, distributed network and endpoint security
- Protecting critical infrastructure, often running control systems protocols, that was not built to withstand modern attacks
- Protecting unpatched commercial-off-the shelf (COTS) systems from known cyber-threats and reducing downtime due to cyber-incidents or patching

THE PALO ALTO NETWORKS® ENTERPRISE SECURITY PLATFORM

To address these challenges and effectively secure critical government services and infrastructure, a disruptive, comprehensive approach—a platform approach—is necessary. Palo Alto Networks Enterprise Security Platform eliminates complexities involved with point products—firewall, IPS, IDS, URL filtering, endpoint antivirus, and more. The platform realizes this vision of comprehensive security by integrating the power of three core elements:

- The next generation firewall with its innovative layer-7 classification engine not only provides granular traffic visibility even to ICS protocols, applications, and users, but as the enforcing device allows users to segment their network using intuitive government service- or user-specific policies that reduce the attack footprint. It further secures the allowed traffic by natively blocking known threats, including both IT and control systems exploits, viruses and spyware and by sandboxing unknown threats which are quickly analyzed and stopped with automatically generated protections. Security can also be extended to virtual and mobile environments which are increasingly being deployed to improve efficiencies.

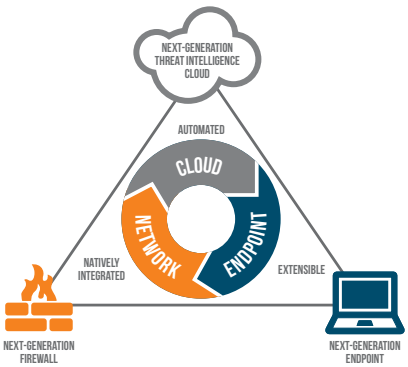

Figure 1: Palo Alto Networks Next-Generation Enterprise Security Platform.

- The advanced endpoint prevention, Traps, ensures that the point of entry for most advanced threats, the host, is secure. It uses a disruptive approach to prevention, stopping the underlying techniques used by exploits and malware in their attack chain. This is unlike the ineffective and burdensome approach used by traditional endpoint solutions which only look at the ever growing repository of known signatures, strings, and behaviors to try to deter zero-day attacks.
- The threat intelligence cloud analyzes and correlates intelligence from all platform security functions—URL Filtering, mobile security, IPS/threat prevention and the virtual execution engine or sandbox, WildFire™—and validated community input. WildFire immediately discovers previously unknown malware and communicates the results to the platform to automatically generate signatures. All threat intelligence is distributed to the network and endpoints to ensure they are protected. Known, zero-day and advanced attacks, including APTs, can all be prevented from endpoint to data center. This is all done automatically, reducing operational burden and shortening an organization's response time.

HOW GOVERNMENTS BENEFIT FROM THE PLATFORM

Palo Alto Networks Enterprise Security Platform provides a unified approach to securing and managing city, state and provincial networks. We make it easier for IT teams to:

Adopt a platform approach

- Regardless of traditional services to SmartGov innovations, detect, analyze and prevent threats across both known and unknown threats, including APTs, from one consolidated platform. Security for these swiftly changing networks includes all core security functions in one platform: IPS/IDS, mobile device management, URL filtering, anti-malware, anti-virus and threat intelligence.
- Unify security policy and enforcement capabilities across Internet edge, data center, mobile devices and endpoints—regardless of how far-reaching the city, state or provincial employee or initiative.

Secure user, application and Internet access

- Allow a diverse set of users—law enforcement to tax services to traffic control to citizen—with mobile computing, data center virtualization, and mobile-enabled services with comprehensive threat prevention capabilities that offer complete identification and blocking of known and unknown malware and zero-day threats.

1 Gartner Group Magic Quadrant 'leader' for Enterprise Firewalls 2014 and several years in a row.

- Powerful and easy-to-implement access control policies that are based on applications and users, rather than port and protocol so approved URLs and applications are allowed, while all else is blocked including unapproved, problematic file-sharing, and risky peer-to-peer apps
- Instead of the traditional "'allow all or block all" approach, IT teams can also deploy flexible, policy-based control (based on groups of users, applications, categories of URLs, customized white or blacklists created from local lookups of the most frequently accessed URLs and a cloud-based database of the latest URLs) with application visibility and URL filtering

Ensure high quality of service

- Allocate bandwidth usage based on application, user, content, or a combination of the three so real-time or high-priority traffic, such as emergency alerts or law enforcement communications, has priority over best-effort or low-priority traffic, preventing non-essential applications from monopolizing critical bandwidth

Threat mitigation and forensics

- Next generation cyber security including sandboxing, IDS/IPS, firewall, URL filtering, and anti-malware protections, in ONE platform
- A unique approach incorporates threat intelligence about new software vulnerabilities, bad IP addresses, suspect URLs, malicious files and emerging malware tactics into actionable firewall and endpoint prevention.
- Rich forensics and logging within PAN-OS™, Panorama and WildFire for rare after-the-fact investigations

Simplify cross-departmental administration

- Our ability to centrally manage all security appliances and key security functions streamlines the deployment of configurations and policies and simplifies the collection and analysis of logs from multiple locations

RESPOND TO YOUR GOVERNMENT SECURITY NEEDS

Take action today and find out what protocols, applications and risks exist in your state, local or provincial government network. The Palo Alto Networks Enterprise Security Platform provides the scalability and performance needed to address the most diverse and complex network demands with the security and visibility required to stand up to today's threat landscape. With more than 19,000 customers in over 120 countries across multiple industries, more than 75 of the Fortune 100 and the most advanced governments rely on Palo Alto Networks to improve their cybersecurity posture. Sign up for a free **Application and Visibility Risk Report** for your city, state or provincial network. This free and non-disruptive process will help you discover unknowns on your network and where you are most at risk.

paloalto networks®
the enterprise security company™

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com