PROTECTING PUBLIC SAFETY AND FIRST RESPONDER SYSTEMS

EXECUTIVE SUMMARY

Public safety networks typically must incorporate a diverse array of disparate technologies. This may include mobile devices, wireless cameras and sensors deployed in the field, workstations, on-premises databases, cloud-based services and applications, and communications systems. By their nature, these kinds of networks that combine high degrees of complexity and mobile connectivity can be difficult to secure. The Fortinet Security Fabric integrates key solutions for protection that meet the critical networking needs of first responders. These include endpoint protection, access point security, device controls, and end-to-end sharing of threat intelligence for automated threat responses.

> **"… I believe that cyber threats collectively now exceed the danger of physical attacks against us. This is a major sea change for my department, and for our country's security."[1]**
>
> *-Kirstjen M. Nielsen,*
> *United States Secretary of Homeland Security*

PUBLIC SAFETY'S CYBERSECURITY PROBLEM

The public safety sector (such as state and local policing, firefighters, paramedics, and emergency responders to natural disasters) relies on technology in life-or-death circumstances every hour of every day. On top of typical office functions, these networks must also support the intense demands of emergency response operations—instant, coordinated communications between teams, central command posts, and outside agencies—in order to provide situational awareness during a crisis. Field-deployed surveillance and sensor systems also connect and wirelessly share continuous data with public safety networks. Connections must be fast, robust, and reliable. And most importantly, they must be secure.

A report from the U.S. Department of Homeland Security revealed that 32 of 33 tested public safety applications have security holes that could let nefarious actors slip in to access a smartphone's camera, contacts, audio recording, SMS messaging, and hard-coded credentials.[2] And on top of their inherent vulnerabilities, public safety networks are also a prime target for cyber criminals, hacktivists, and nation-state attacks.

As cyber threats of all varieties increase in volume and sophistication, this increases the dangers to the state, county, and local systems that help ensure the safety of citizens.

Take for instance the ransomware attack that brought Atlanta municipal government services and programs to a halt in March 2018, or the one last year in Dallas where hackers gained the ability to set off tornado sirens in the middle of the night.[3]

WHAT TO LOOK FOR IN A SOLUTION

Public safety's specific intersection of endpoints, communications, surveillance devices, and wireless sensors, and a regular need to collaborate with other services and outside agencies, creates a complex system that introduces many cybersecurity risks to these organizations. There are several key criteria to look for in a security architecture that can support the unique needs of regional public safety institutions.

1. END-TO-END NETWORK PROTECTION

Complexity, mobility, and new technologies like cloud applications and Internet of Things (IoT) devices all expand the attack surface of networks and introduce new vulnerabilities. Security leaders can no longer count on an amalgamation of isolated point solutions to protect their organizations. Public safety networks need an integrated security architecture that connects and shares threat intelligence across all solutions deployed among the organization. Integration unlocks automation—providing instantaneous responses to potential threats, which shrink the window from detection to containment.

2. ENDPOINT SECURITY

Endpoint devices represent some of the most common targets for cyberattacks. If a vulnerable laptop or smartphone is compromised by malware in the field, that infection can rapidly spread to the rest of the organization upon reconnecting to the network. Fifty-three percent of organizations reported an increase in malware-infected endpoints last year.[4]

Security leaders must harden their endpoints and ensure proper hygiene by identifying, installing, and configuring effective security solutions. Endpoint security should provide risk-based visibility of all devices that connect to the network, granular controls, and automated responses and workflows that enable faster detection of potential and better overall protection.

3. SECURE ACCESS

First responders need fast and reliable device connectivity in the field for real-time data and communications. Priority access to networks is not only a top concern for first responders but also a necessity during an emergency. At the same time, the organization's IT team needs reduced complexity of network, application, and device management.

Protecting access points requires scanning for malware, checking endpoint integrity, and controlling application usage. And the solution must not only be secure but also easy to manage.

In a recent study, 97% of risk management professionals indicate that a breach via unsecured IoT devices could be catastrophic for their organization.[5] To protect headless connected devices, such as cameras, sensors, or IoT products, organizations must be able to see where each device is, what it does, and how it connects to other devices across the network topology.

THE FORTINET SOLUTION

Fortinet's end-to-end security strategy addresses the key problems of public safety networks. It is designed to help organizations adapt to evolving network demands and address the full spectrum of challenges that they currently face from both sophisticated threats and rapid infrastructural changes.

THE FORTINET SECURITY FABRIC

Our **Security Fabric** offers an integrated architecture that connects and coordinates solutions, shares threat intelligence in real time, and enables automated responses to potential threats across the full breadth of the organization. It provides an architectural approach to security that lets organizations weave together all of their discrete security solutions into an integrated whole. This, in turn, helps public safety leaders ensure that their ever-expanding network attack surface is protected—from the command center to connected first responders in the field.

ENDPOINT PROTECTION

Fortinet's endpoint security provides risk-based visibility, compliance control, vulnerability management, and automation. It proactively defends endpoints with pattern-based anti-malware technology, behavior-based exploit protection, web filtering, and an application firewall.

Our **FortiClient** solution establishes risk awareness by sharing real-time endpoint telemetry with other solutions across the broader Security Fabric architecture. This includes device information, user identities, protection status, unpatched vulnerabilities, and endpoint events. Integration between FortiClient and FortiGate NGFWs enables enforcement of compliance control, so that only devices that meet security standards can access the network and applications.

FortiClient's vulnerability management capabilities prioritize critical exposures and include remediation options such as automatic patching of software/operating systems. This helps eliminate defensive gaps while reducing the churn of manual processes for under-resourced IT teams.

SECURE UNIFIED ACCESS AND FORTINAC

Fortinet's Secure Unified Access solution provides comprehensive security for local area network (LAN) infrastructures, delivering flexible security with end-to-end enforcement. It tightly integrates our **FortiGate** NGFWs with **FortiSwitch** devices and **FortiAP** wireless access points to enable a common security policy that extends firewall protection out to the network edge. Together, FortiGate and FortiNAC can perform traffic shaping to prioritize first responder access on priority networks during emergencies.

Our **FortiNAC** network access control (NAC) solution provides real-time visibility via a live inventory of all devices connected to the network. FortiNAC offers an easy-to-use, one-step solution specifically designed to close security gaps resulting from absent or outdated access controls. It enables network lockdown, simplifying IoT device onboarding and management, while filling a crucial defensive gap by controlling device access.

KEEPING FIRST RESPONDERS SAFE FROM CYBER THREATS

With mobile and IoT devices continuing to be a top risk exposure for organizations, Fortinet's deep integration between endpoint security and network security can solidify public safety defenses. This helps to protect critical data, applications, and services running on the network. At the same time, our Security Fabric also helps maximize institutional resources by streamlining operations, simplifying management, and reducing total cost of ownership (TCO). Fortinet provides powerful, scalable, reliable, and highly secure solutions that meet the intensely demanding requirements of protecting public safety networks.

[1] "Secretary Kirstjen M. Nielsen's National Cybersecurity Summit Keynote Speech," U.S. Department of Homeland Security, July 31, 2018.

[2] Tom Sullivan, "New cybersecurity threats unwrapped: Hidden Cobra, public safety apps, Western Digital My Cloud," Healthcare IT News, December 28, 2017.

[3] Alan Blinder and Nicole Perlroth, "A Cyberattack Hobbles Atlanta, and Security Experts Shudder," The New York Times, March 27, 2018.

[4] "The Cost of Insecure Endpoints," Ponemon Institute, June 2017.

[5] "Second Annual Study on The Internet of Things (IoT): A New Era of Third-Party Risk," Ponemon Institute, March 2018.