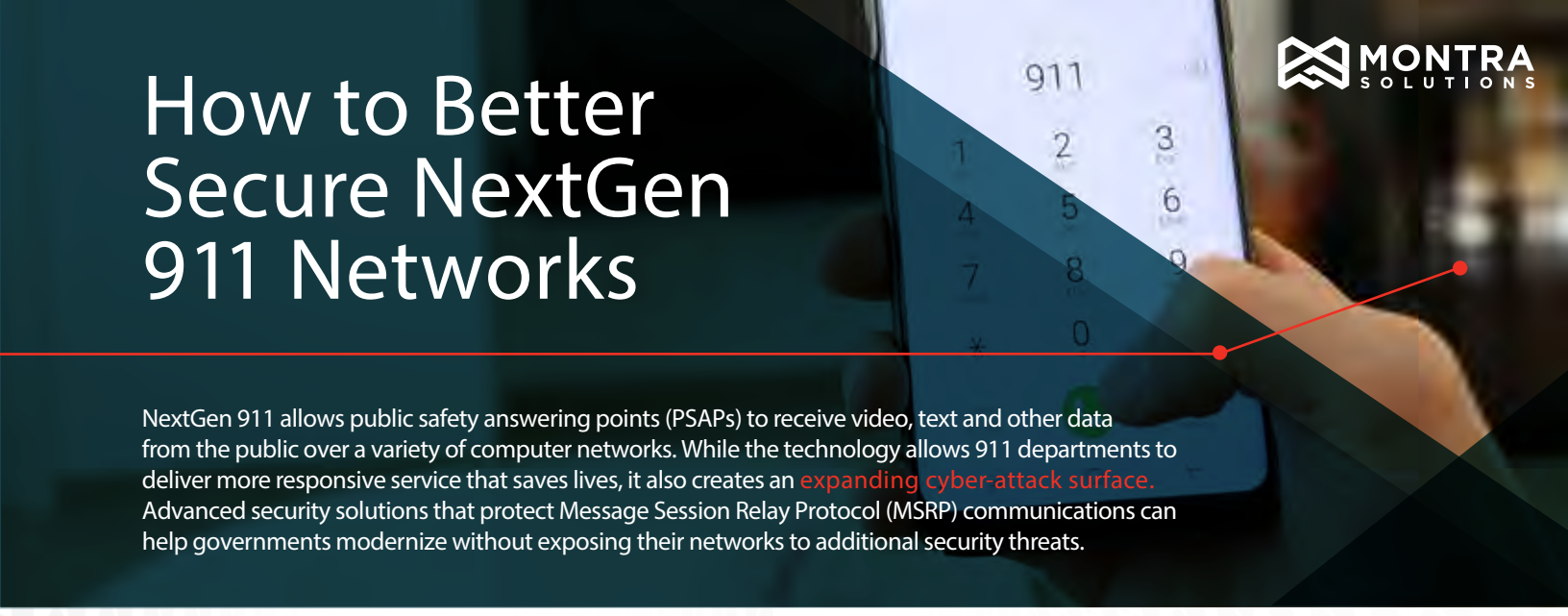
How to Better Secure NextGen 911 Networks



NextGen 911 allows public safety answering points (PSAPs) to receive video, text and other data from the public over a variety of computer networks. While the technology allows 911 departments to deliver more responsive service that saves lives, it also creates an expanding cyber-attack surface. Advanced security solutions that protect Message Session Relay Protocol (MSRP) communications can help governments modernize without exposing their networks to additional security threats.

PSAPs Face Greater Cyber Threats

More than 40 attacks in the last three years have targeted 911 dispatch centers.

A ransomware attack in Henry County, Tenn., shut down the dispatch system for the 911 call center with hackers demanding **$2,000 in Bitcoin.**

The city of Baltimore's 911 system was hacked, causing a disruption that forced call center staff to **manually manage calls.**

These attacks could increase as traditional 911 networks transition to NextGen 911, which enables interconnection among a range of public and private networks, including:

Wireless | Internet | Phone

These interconnections create an expanding attack surface.

Today , 2,200 partially implemented NexGen 911 systems can accept text messages.

Top Threats for NextGen 911 Networks

- **Distributed denial-of-service attacks**
  Traffic, sometimes created by a botnet, that overwhelms a website or an online service
- **Malware**
  Code developed by cyber attackers, designed to cause extensive damage to data and systems or to gain unauthorized access to a network
- **Ransomware**
  A type of malware designed to deny access to a computer system or data until a ransom is paid
- **Spoofing**
  An unauthorized device that disguises itself as an authorized device
- **Swatting**
  Manipulation of IP-based calls to make authorities think these calls are coming from locations where serious crimes have occurred

The Problem

A Message Session Relay Protocol (MSRP) facilitates large-scale instant messaging — including **transferring large files such as video and images** — within NextGen 911 systems.

But many Text Control Centers (TCCs) do not perform security inspections on MSRP even though they can contain malicious URLs, malware attachments and other security threats.

TCCs must perform security inspection on MSRP messages before they are processed by the NextGen 911 system.

However, most point solutions on the market do not have this capability.

How to Better Secure PSAPs

Public safety agencies need an MSRP protocol decoder, an advanced security solution that analyzes text messages and attachments as they are flowing from the TCC into the PSAP.

Key Considerations:

- Seek the help of a security-focused technology provider that understands your organization's IT infrastructure.
- Implement a platform (rather than point solutions) that provides a security strategy with products that work together and offer automation via artificial intelligence.
- Make sure the enterprise security platform provides end-to-end visibility and has features like MSRP protection and proactive detection and prevention response capabilities mapped to standards like NIST.

For more information, visit www.fortinet.com

MONTRA SOLUTIONS Learn about Montra IT Services at montra.io/contact-us

PRODUCED BY: government technology

Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education.
www.govtech.com

FOR: FORTINET

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network—today and into the future.
www.fortinet.com