

First responders stand guard, ready to serve the community, 24/7. You know who else works around the clock? Cybercriminals. That's why public safety agencies need fast, reliable and secure communications for mission-critical services.



The stakes couldn't be higher.

85%

of Public Sector respondents surveyed agree that a security breach of their organization could endanger lives, especially if critical or emergency services go down.¹



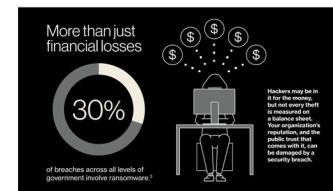
Cyberattacks can come from anywhere, with the potential to cause communication outages and dispatch failures.

53%

of critical infrastructure respondents have experienced significant mobile- or Internet of Things (IoT) device-related security incidents leading to data loss or system downtime.²



Cybersecurity breaches on public safety information systems can result in delays to critical response times and inaccurate information.



Common vulnerabilities and exploits



Unsecured devices

- Personal devices used for work
- Outdated software
- Weak passwords
- No encryption
- Potentially vulnerable IoT devices (body-worn cameras, drones, smart vehicles, etc.)

Weak networks

- Unsecured Wi-Fi
- Outdated network infrastructure
- No segmentation

Human factors

- Phishing attacks
- Social engineering
- Insider threats
- No security awareness training

The building blocks of security

To help protect your organization and its assets, potential threats are addressed with our security solutions, including:

- Verizon Mobile Device Management**
Centralized management helps improve security by enabling data erasure, password enforcement, app management, location tracking and data encryption.
- Cyber Risk Programs**
Evidence-based risk assessments are designed to measure the effectiveness of your cybersecurity risk controls.
- Rapid Response Retainer**
Stay ahead of cyberthreats by preparing for security incidents before they happen through risk assessment and response planning.
- Verizon Zero Trust Dynamic Access**
Harden your security by subjecting all users and devices, regardless of their locations within the network, to rigorous authentication and authorization procedures.
- Verizon Private Wireless Network**
A dedicated, secure wireless network helps provide greater control, reliability and security for public safety communications and data transmission.

Verizon is the #1 network choice in public safety.⁶ More than 40,000 public safety agencies rely on Verizon Frontline and its mission-critical solutions.

#1

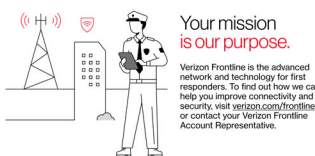
Why Verizon

17+ years of deep analysis of cybersecurity breach and incident trends with the Verizon Data Breach Investigation Report

3.5M security alerts monitored annually (approximate)

20T signals analyzed annually for malicious security activity (approximate)

Powered by America's most extensive data network⁷ in public safety, experience is invaluable. Our team has more than three decades of experience in threat intelligence and cybersecurity as well as experience protecting networks, infrastructure, data and people from threat actors.



Your mission is our purpose.

Verizon Frontline is the advanced network and technology for first responders. To find out how we can help you improve connectivity and security, visit verizon.com/frontline or contact your Verizon Frontline Account Representative.

1. Verizon Data Breach Investigation Report, March 2018
2. Verizon Data Breach Investigation Report, March 2018
3. Verizon Data Breach Investigation Report, March 2018
4. Verizon Data Breach Investigation Report, March 2018
5. Verizon Data Breach Investigation Report, March 2018
6. Verizon Data Breach Investigation Report, March 2018
7. Verizon Data Breach Investigation Report, March 2018