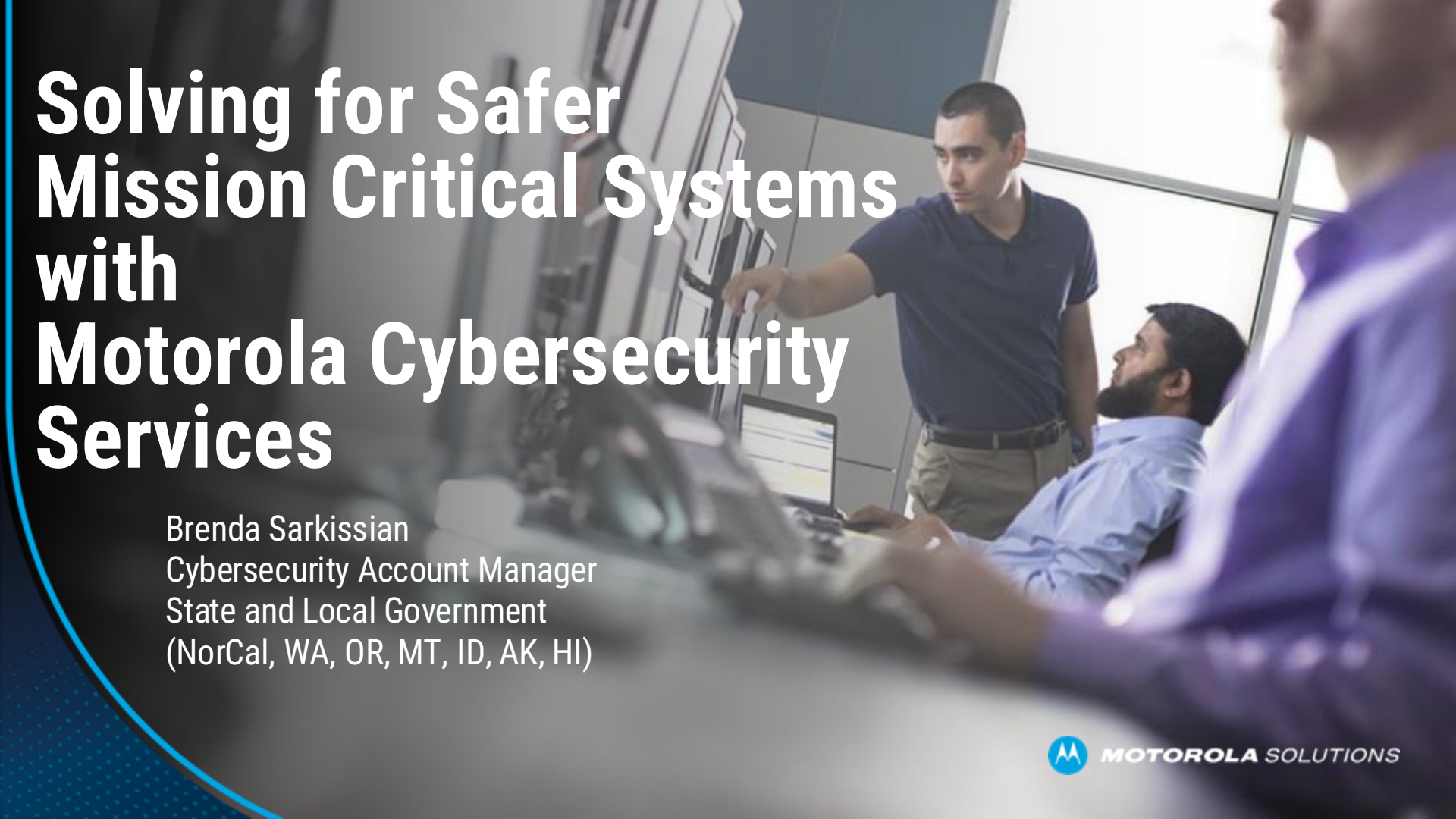
Solving for Safer Mission Critical Systems with Motorola Cybersecurity Services



Brenda Sarkissian
Cybersecurity Account Manager
State and Local Government
(NorCal, WA, OR, MT, ID, AK, HI)

MOTOROLA SOLUTIONS

RANSOMWARE CONTINUES TO DOMINATE

21

Average # of days of downtime

287

Average # of days to fully recover

$1.1B

Total paid in ransoms in 2023

$650K

Average ransom payment in 2023

THREATS CONTINUE TO ADAPT AND BEHAVE DIFFERENTLY

COMPLEXITY AND IMPACT TO TARGET SYSTEMS ARE MORE DEVASTATING

Generation 5 - Present, Large scale, multi-vector attacks using attack tools and connected systems/users for access and is driving EDR, IAM, SOAR products → **Systemic Attacks (Colonial Pipeline)**

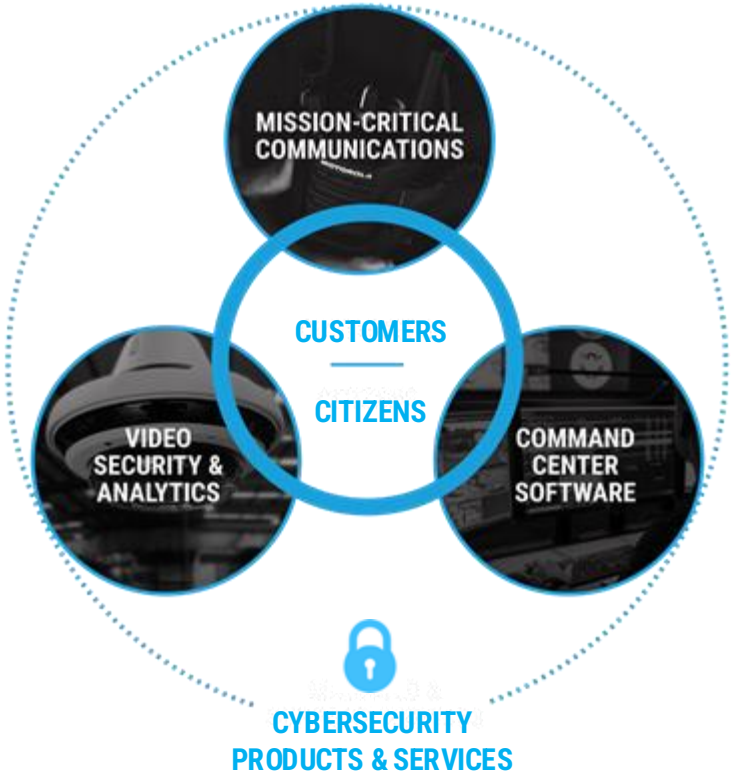
Generation 4 - Present, rise of targeted, evasive attacks affected most business and drove behavior analysis products. → **Trusted Resource Attacks (RNI and CEN based attacks)**

Generation 3 - Early 2000s, exploiting vulnerabilities in applications affected most businesses and drove intrusion prevention/detection systems (IPS/IDS) products → **Internal Network Attacks**

Generation 2 - Mid 1990s, attacks from the internet affected all business and drove creation of the firewall. → **Perimeter Attacks (Fortinet Vulnerability)**

Generation 1 - Late 1980 , virus attacks on stand-alone Personal Computers affected all businesses and drove antivirus products → **Virus Attacks**

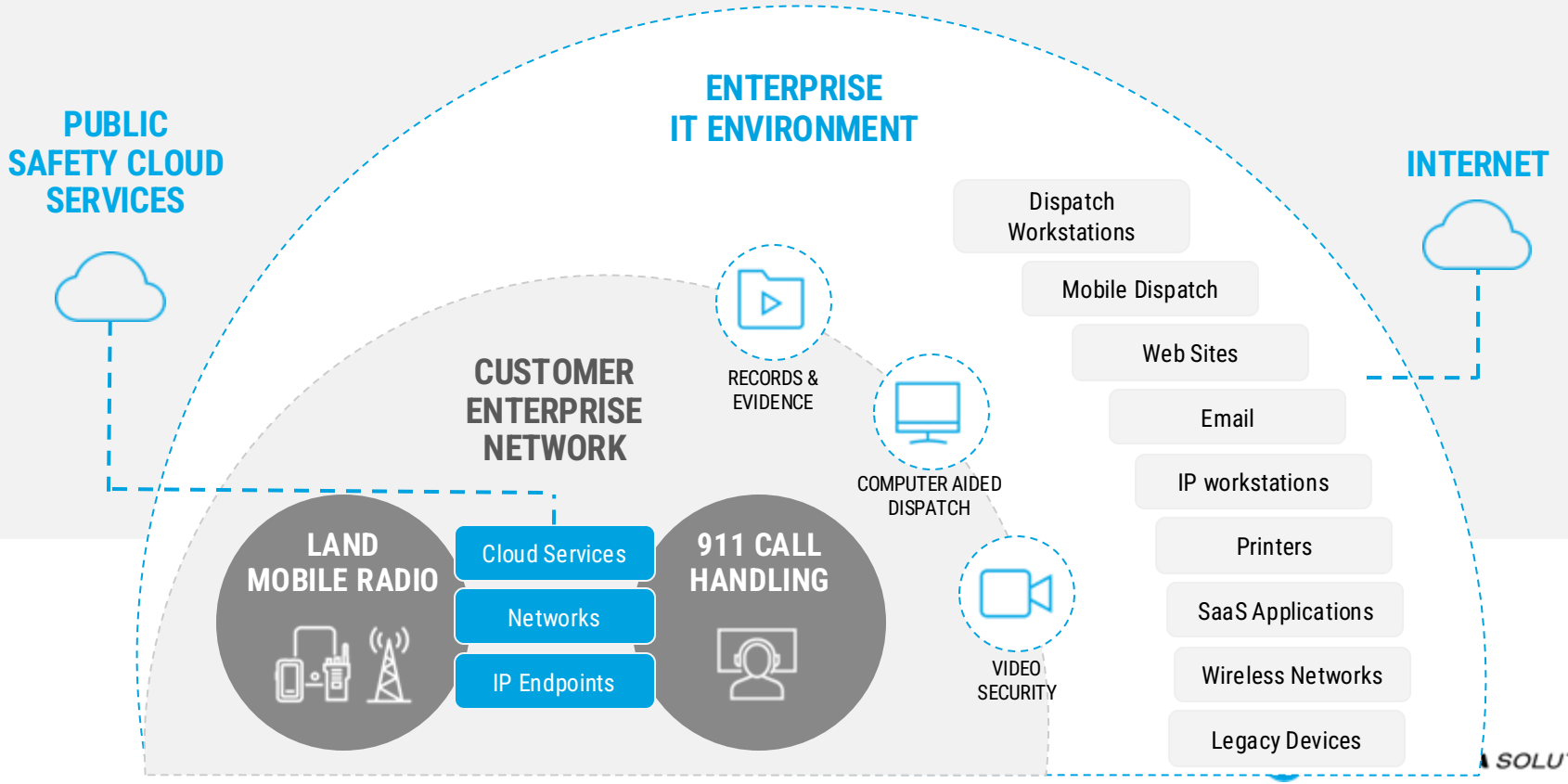
CYBERSECURITY IS CRITICAL TO PUBLIC SAFETY



- A **cybersecurity attack** has the ability to take away the Confidentiality, Availability & Integrity of **mission critical** communications.
- Only with products built securely as well as continuous cybersecurity services can you **stay one step ahead of the attacker**

CYBERSECURITY LANDSCAPE

FOR PUBLIC SAFETY

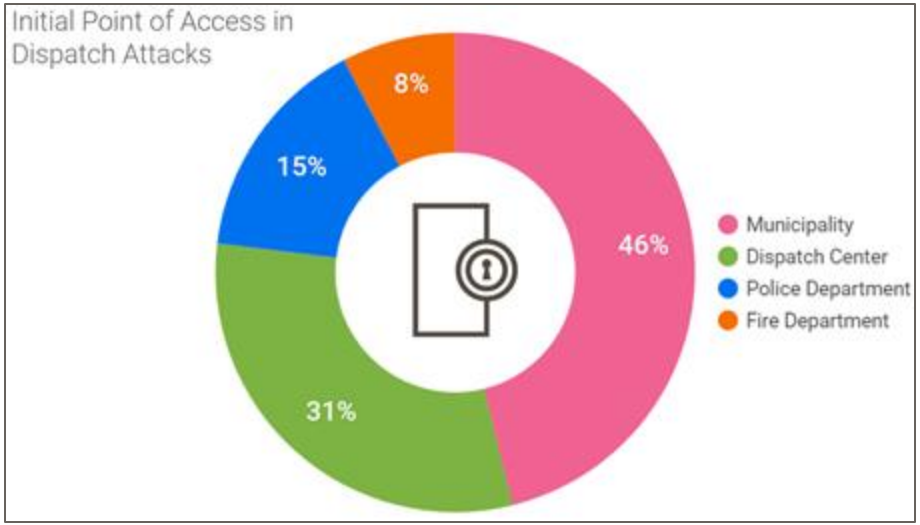


THERE IS NO SUCH THING AS A CLOSED NETWORK

- INSIDER THREAT
- EXTERNAL NETWORK CONNECTIONS
- UNAUTHORIZED CONNECTIONS
- BYOD AND MAINTENANCE LAPTOPS
- EXTERNAL DISC MEDIA AND USB DRIVES

Cyber disruptions to 9-1-1/ dispatch centers

- **12** cyberattacks have degraded CAD operations this year
- **90%** of observed attacks involved ransomware
  - Average downtime was **15** days; **5** day minimum
- **77%** of CAD and PSAP victims were located in the U.S.



MOTOROLA SOLUTIONS CYBERSECURITY

TRUSTED CYBER PARTNER CAPABILITIES

NIST National Institute of Standards and Technology U.S. Department of Commerce

ADVISORY

Assessment & Compliance

RISK ASSESSMENT

PENETRATION TESTING

MANAGED SECURITY

Vulnerability & Threat Insight

Detection & Response

CISO KPI Dashboard

Investigation & Reporting

Log Storage & Forensics

THREAT DETECTION & RESPONSE | **VULNERABILITY ASSESSMENT** | **PATCH TESTING & DEPLOYMENT**

24x7 Expert Security Operations Center

Public Safety Expertise and Deep Threat Intelligence

RECOVERY

Response & Recovery

INCIDENT RESPONSE PLANNING

SYSTEM RECOVERY PLANNING

CYBERSECURITY TRAINING

ARE YOU CJIS COMPLIANCE?

FBI-CJIS MANDATE: CUSTOMERS NEED HELP TO MANAGE ENDPOINT PROTECTION

FBI-CJIS

- Public Safety security standards
- Requirement to protect customer's sensitive Criminal Justice Information (CJI)

Endpoint protection is required for CJIS

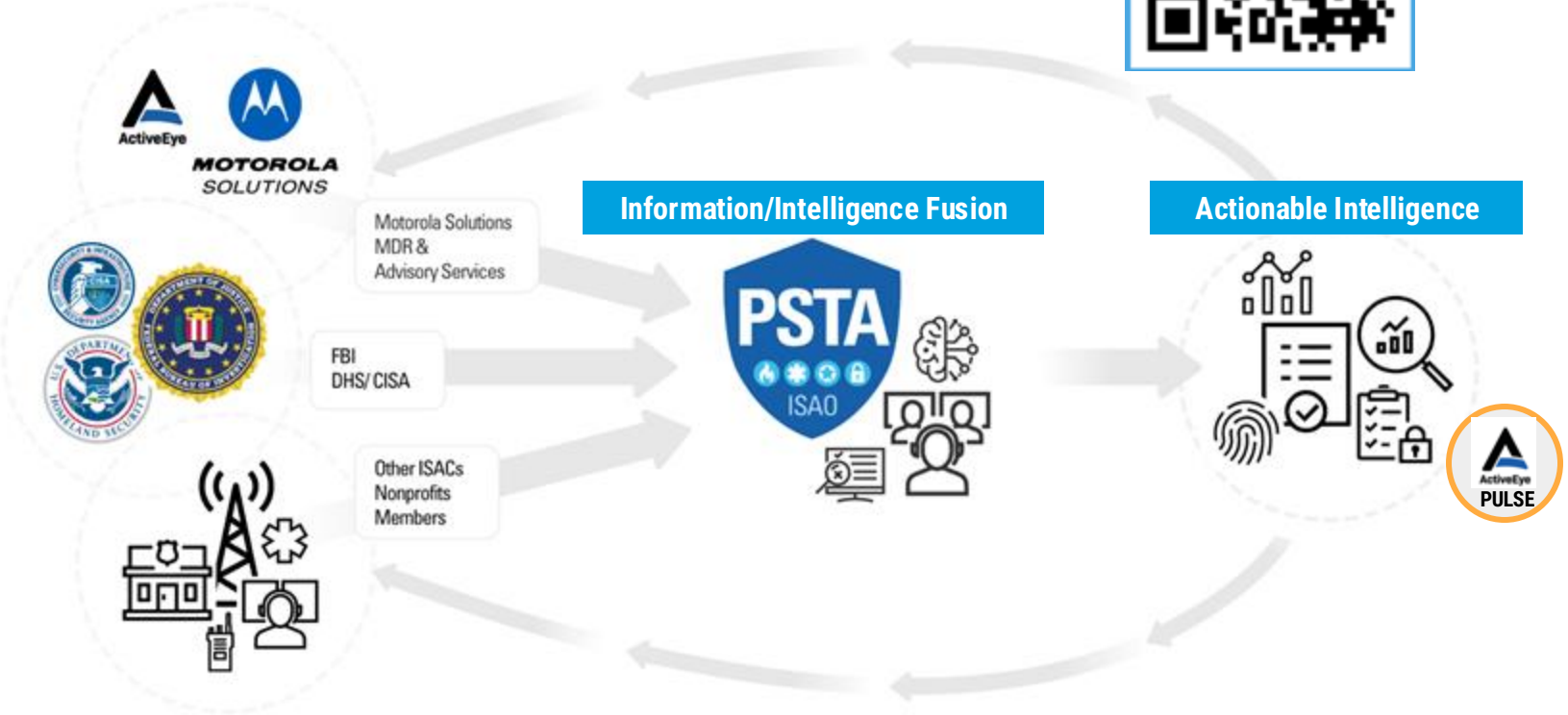
- MSI goes further: we test it with Astro Systems
- Customers need our help to monitor the endpoint protection agent

ActiveEye is CJIS compliant cloud-based tool

- Our SOC personnel meet CJIS requirements
- ActiveEye does not collect and store unencrypted CJI data
- As best practice, we still meet many CJIS requirements

PSTA UPDATE

INFORMATION/INTELLIGENCE FLOW



PSTA
PUBLIC SAFETY THREAT ALLIANCE
PUBLIC SAFETY ISAO

MOTOROLA SOLUTIONS


THANK YOU