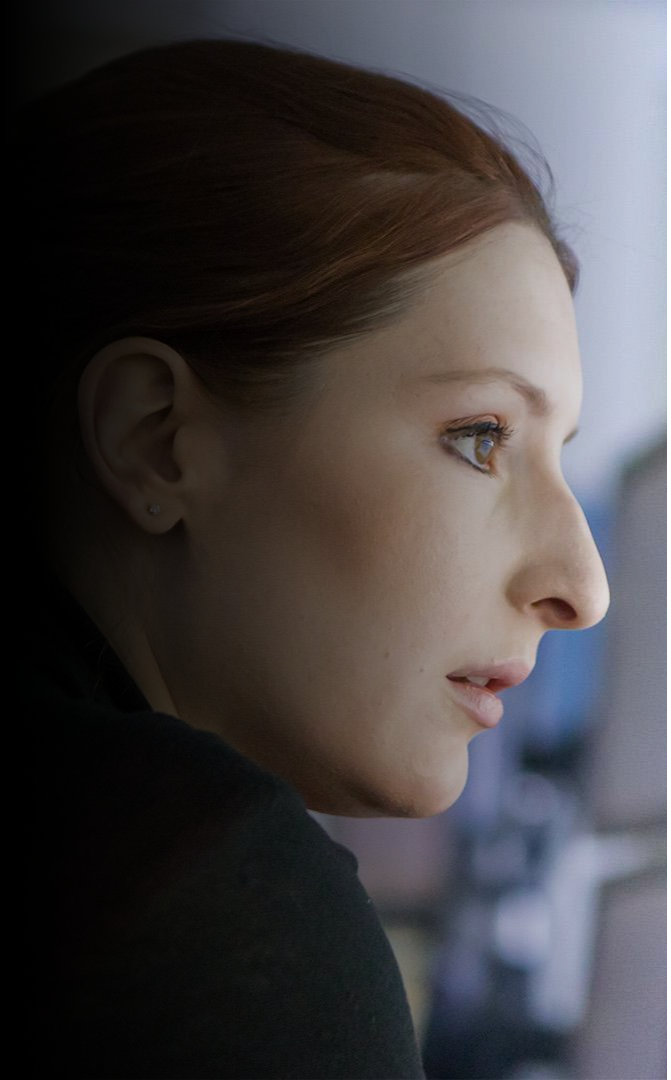
CYBER THREATS TO PUBLIC SAFETY

PAUL HILL, MOTOROLA SOLUTIONS

SEPTEMBER 2020

MOTOROLA SOLUTIONS



Agenda

The Public Safety Landscape

The Security Challenge

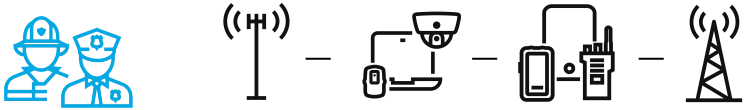
Cyber Threats to Public Safety

The Solution

Key Takeaways

MOTOROLA SOLUTIONS

THE PUBLIC SAFETY ECOSYSTEM



Frontline Responder

Mission-critical technologies - LMR, Broadband, Video Analytics

Incident Awareness

Incident Management

Post-Incident Resolution

COMMUNITY ENGAGEMENT

Citizen

EMERGENCY CALL MANAGEMENT

911 Call Taker

VOICE & COMPUTER AIDED DISPATCH

Dispatcher

REAL-TIME INTELLIGENCE OPERATIONS

Intelligence Analyst

RECORDS & EVIDENCE MANAGEMENT

Records Specialist

ANALYSIS & INVESTIGATION

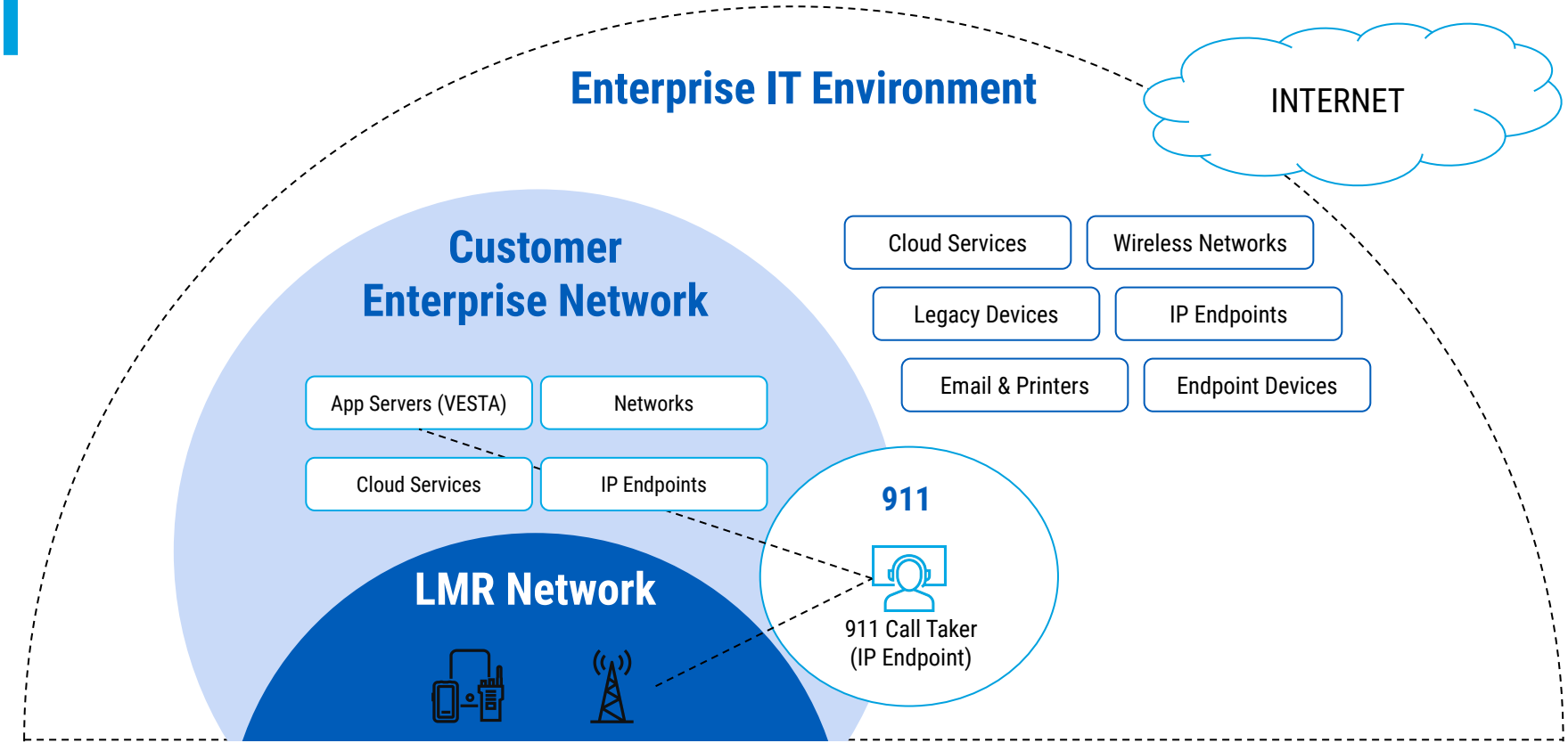
Crime Analyst

JAIL & INMATE MANAGEMENT

Corrections Officer

CYBERSECURITY FOR YOUR PUBLIC SAFETY PLATFORM

THE PUBLIC SAFETY LANDSCAPE



THE SECURITY CHALLENGE

DIGITAL TRANSFORMATION

60%

of digital businesses would suffer major service failures due to inability to manage digital risk

Technology innovation & remote operations are increasing the cyber attack surface

INCREASING COMPLEXITY

57

average number of tools that security teams are grappling to manage

Complex & fragmented IT environments have generated visibility challenges, made worse by number of security tools

CHALLENGED RESOURCES

4M

estimated number of unfilled cybersecurity jobs worldwide

Unrelenting pressure to do more with less, difficult to recruit and retain the new tech skill sets

CYBER THREATS OVERVIEW - ENTERPRISE

Cyber attacks are increasing in number and sophistication, costing billions of dollars in a matter of minutes.

Advancement in cyber attack techniques, lack of security expertise, outdated systems, need for remote operations and cloud-based solutions are putting relentless pressure on cyber resilience.

300%

increase in reported cybercrimes due to COVID-19 pandemic

$6T

estimated costs to organizations due to cybercrime in 2021

18M+

websites infected with malware at any given time

CYBER THREATS OVERVIEW - PUBLIC SAFETY

Cyber attacks are increasing in number and sophistication, costing billions of dollars in a matter of minutes.

Advancements in cyber attack techniques, lack of security expertise, outdated systems, need for remote operations and cloud-based solutions are putting relentless pressure on cyber resilience.

450+

cyber attacks on public safety agencies in the past 24 months

$18M

cost to Baltimore to recover from a ransomware attack in 2019

24

hours for a coordinated ransomware attack to hit 23 cities in Texas

RISING THREATS TO PUBLIC SAFETY

- Ransomware
- Telephony Denial of Service (TDoS)
- Misconfiguration
- Data Breaches / Data Leakage
- Advanced Persistent Threat (APT) Groups
- Insider Threats

MOTOROLA SOLUTIONS' CYBERSECURITY SERVICES

STRENGTHEN YOUR CYBER RESILIENCE

ADVISORY SERVICES

Risk assessment and consulting, penetration testing, governance and compliance.

MANAGED SECURITY SERVICES

Network and application monitoring, incident management and reporting, security patching, advanced threat detection and response.

NIST-ALIGNED PORTFOLIO

SYSTEM RECOVERY SERVICES

Business continuity and major incident response planning, system recovery, post-incident analysis.

CYBERSECURITY TRAINING

Cloud security, incident response management, risk management and privacy planning, certifications.

ADVISORY SERVICES

ADVISORY SERVICES

RISK ASSESSMENTS

Discover vulnerabilities and develop a robust cybersecurity strategy mapped to regulatory frameworks

PENETRATION TESTING

Evaluate the security of IT and communications infrastructure by trying to exploit its vulnerabilities

CYBERSECURITY CONSULTING

Expertise, guidance, and augmentation of your IT, communications or cybersecurity teams

GOVERNANCE AND COMPLIANCE

Demonstrate adherence to regulatory cybersecurity requirements in line with organizational needs

MANAGED SECURITY SERVICES

MANAGED SECURITY SERVICES

IDENTIFY & MITIGATE SYSTEM VULNERABILITIES

ADVISORY SERVICES | **MANAGED SECURITY** | SYSTEM RECOVERY | CYBER TRAINING

SECURITY PATCHING FOR LMR & EMERGENCY CALL HANDLING

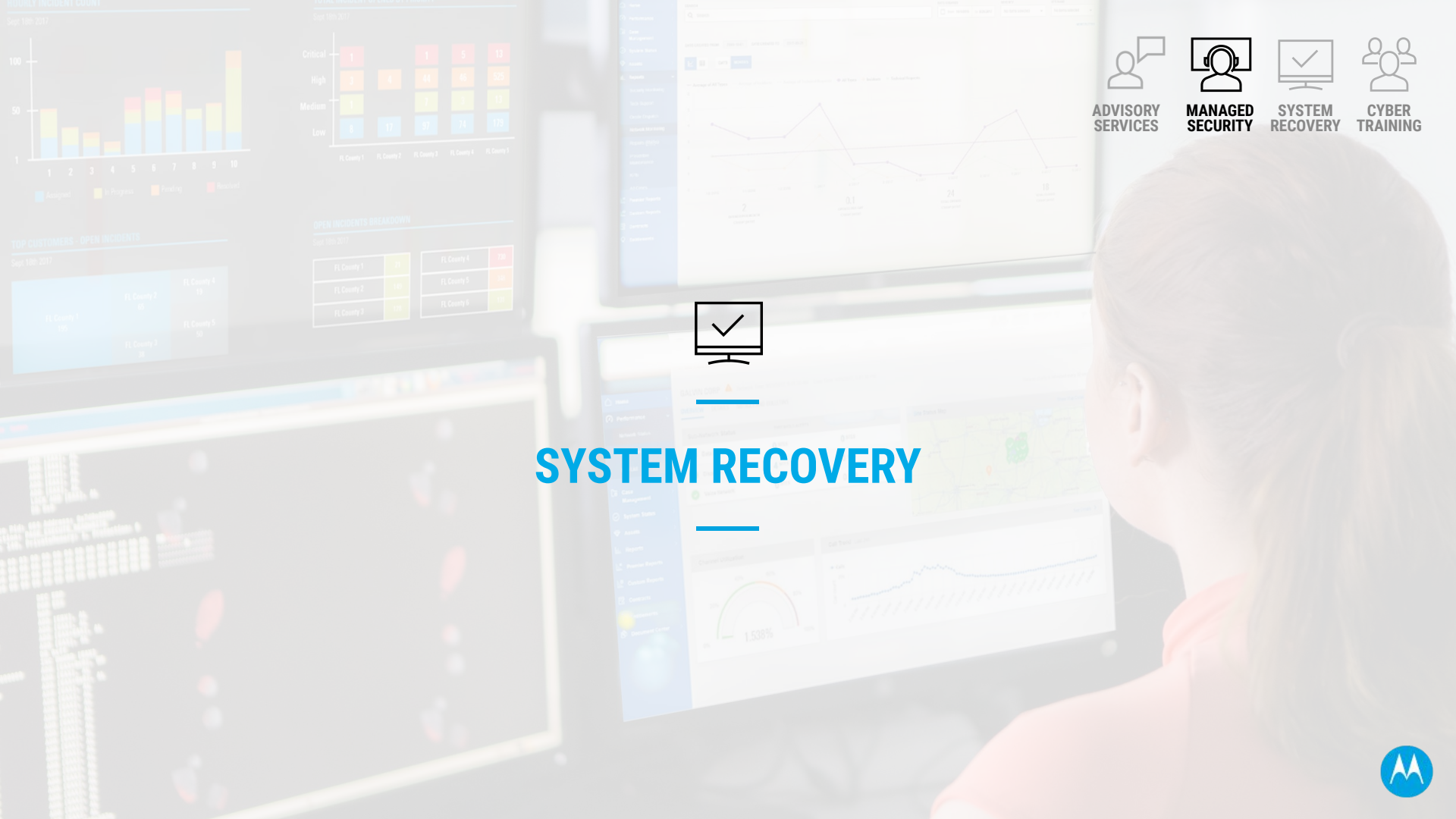
- Pre-testing, validation and anti-malware software updates in line with industry standards
- Flexible consumption models include self install, remote install, reboot support service, onsite delivery

SECURITY MONITORING FOR LMR & EMERGENCY CALL HANDLING

- Assessment of configuration settings against best practices for each environment
- Continuous monitoring of logs to identify management activity and user access
- Enrichment of data streams with threat data and machine learning analytics to identify potential threats

ADVANCED THREAT DETECTION AND RESPONSE FOR ENTERPRISE IT

- 24/7 monitoring for enterprise cloud, network and endpoints
- Cloud infrastructure and SaaS monitoring
- Ongoing threat and vulnerability insights for enterprise networks



SYSTEM RECOVERY

RESPOND AND RECOVER FROM SECURITY INCIDENTS

SYSTEMATIC AND SWIFT APPROACH TO MITIGATION AND RECOVERY

RESPONSE TO DATA BREACH OR CYBER ATTACK

- Identify key system components and data sources impacted
- 24/7 support from security experts while the incident is ongoing
- Final report of all findings and response efforts

THREAT HUNTING FOR SUSPICIOUS MALICIOUS ACTIVITY

- Analyze network and cloud environments, collect artifacts
- 45 days of in-depth system monitoring
- Final report of all findings and response efforts

POST-INCIDENT ANALYSIS & SYSTEM RECOVERY

- Visibility into system issues through compromise assessments
- Reinstate and improve network controls
- Preventive measures and problem management

CYBERSECURITY TRAINING

DELIVERED IN THE BEST WAY TO HELP YOU LEARN

ADVISORY SERVICES | MANAGED SECURITY | SYSTEM RECOVERY | **CYBER TRAINING**

CLASSROOM LEARNING AND LABS

In-person and interactive instructor-led training sessions in line with leading and accepted industry-led security practices

ON-LINE TRAINING

Self-directed, self-paced computer-based training that equips you with the skills needed to fight back against modern cyber threats

VIRTUAL INSTRUCTOR-LED TRAINING

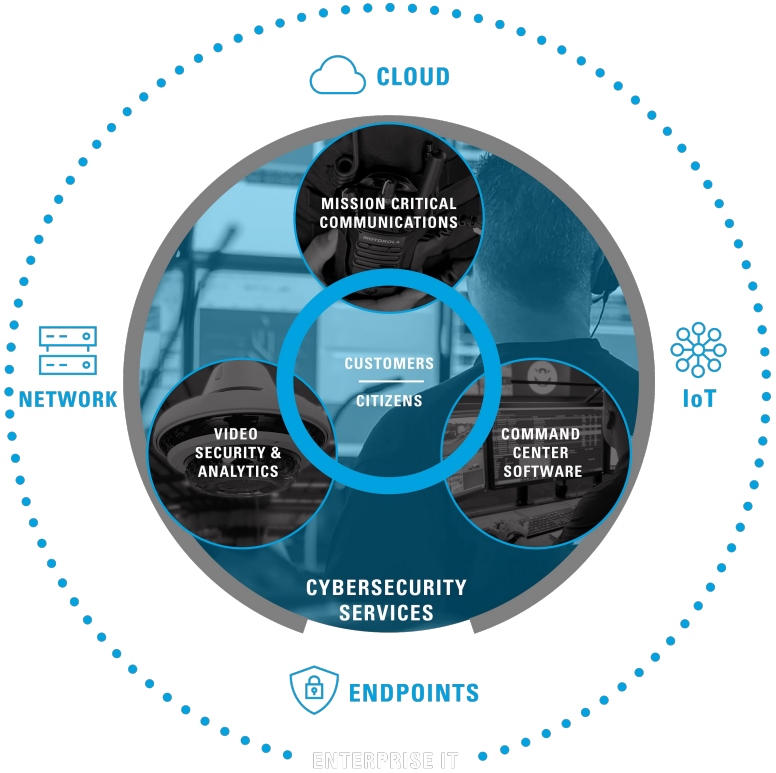
Training delivered in a virtual or simulated environment, or when the instructor and learner are in separate locations

ONE SERVICE PROVIDER FOR YOUR CYBERSECURITY NEEDS.

PURPOSE-BUILT & INTEGRATED APPROACH TO END-TO-END CYBER RESILIENCE

90+

Years of experience in providing mission-critical technologies - LMR, Broadband, Video, Software & Analytics across 100+ countries



20+

Years of developing advanced threat detection and response technologies for sophisticated security incidents

GLOBAL SCALE & EXPERIENCE

ENABLING TECHNOLOGY ECOSYSTEMS TO BE RESILIENT WITH ADVANCED CYBERSECURITY CAPABILITIES

300+

Security experts focused on 24/7 monitoring & response

9B

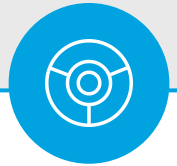
Security events proactively monitored each day

20+

Years of experience developing cybersecurity solutions

PEOPLE

Experts with top industry certifications work hand-in-hand to ensure system availability and security



PROCESS

Mission-critical ITIL framework for scalable service operations that can easily handle peak load

TECHNOLOGY

Network to security operations, security orchestration and automation - designed to accelerate service response

100% co-managed approach for visibility and control

KEY TAKEAWAYS

- The public safety landscape is changing and becoming increasingly interconnected
- The sophistication and regularity of cyber attacks is increasing
- The threats to public safety are specific to the industry
- A holistic, risk based approach is the best way to protect your environment

THANK YOU