CYBERSECURITY SERVICES FOR MISSION-CRITICAL OPERATIONS

CONTINUOUSLY SECURING YOUR TECHNOLOGY ECOSYSTEM

eBOOK

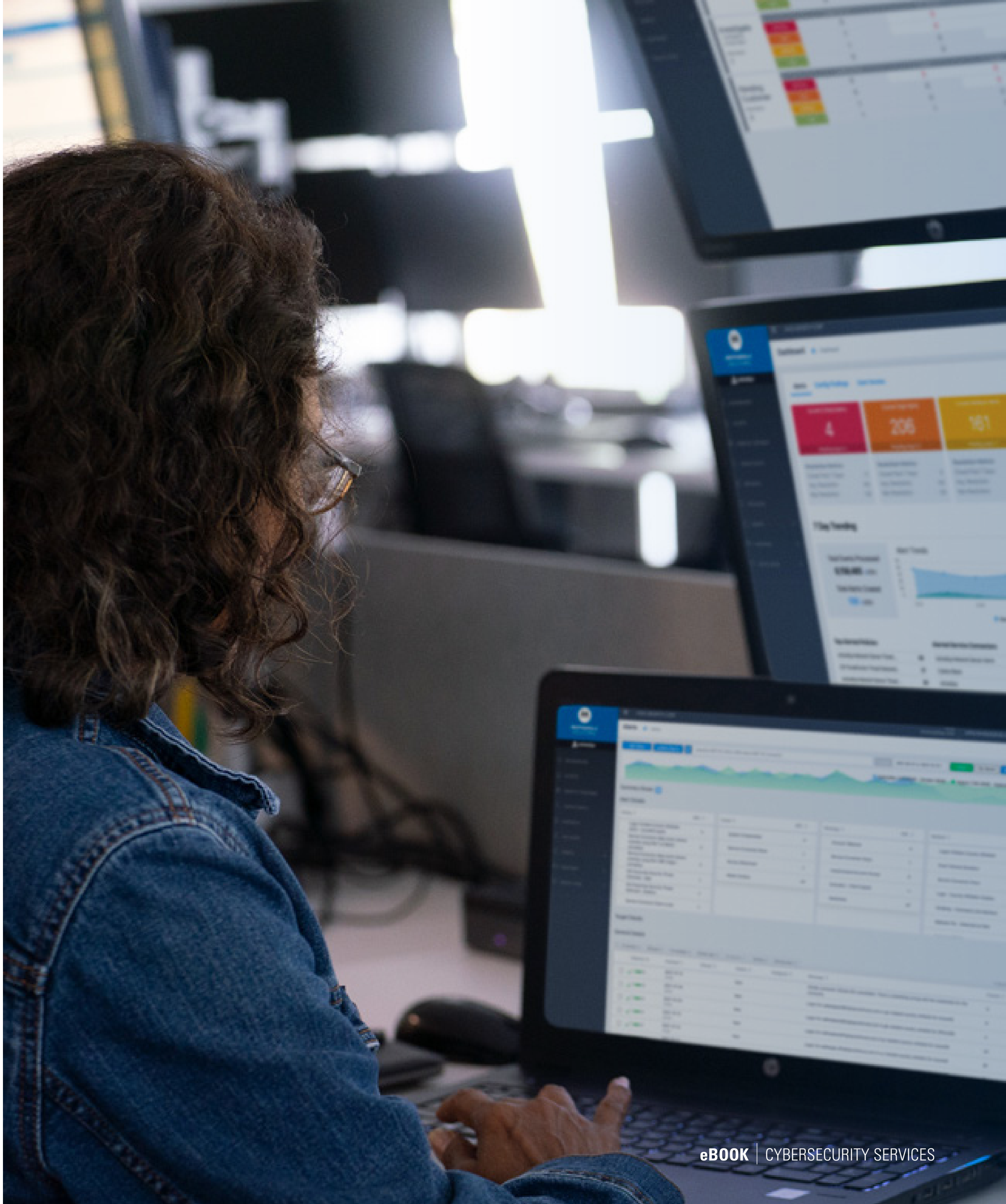
MOTOROLA SOLUTIONS

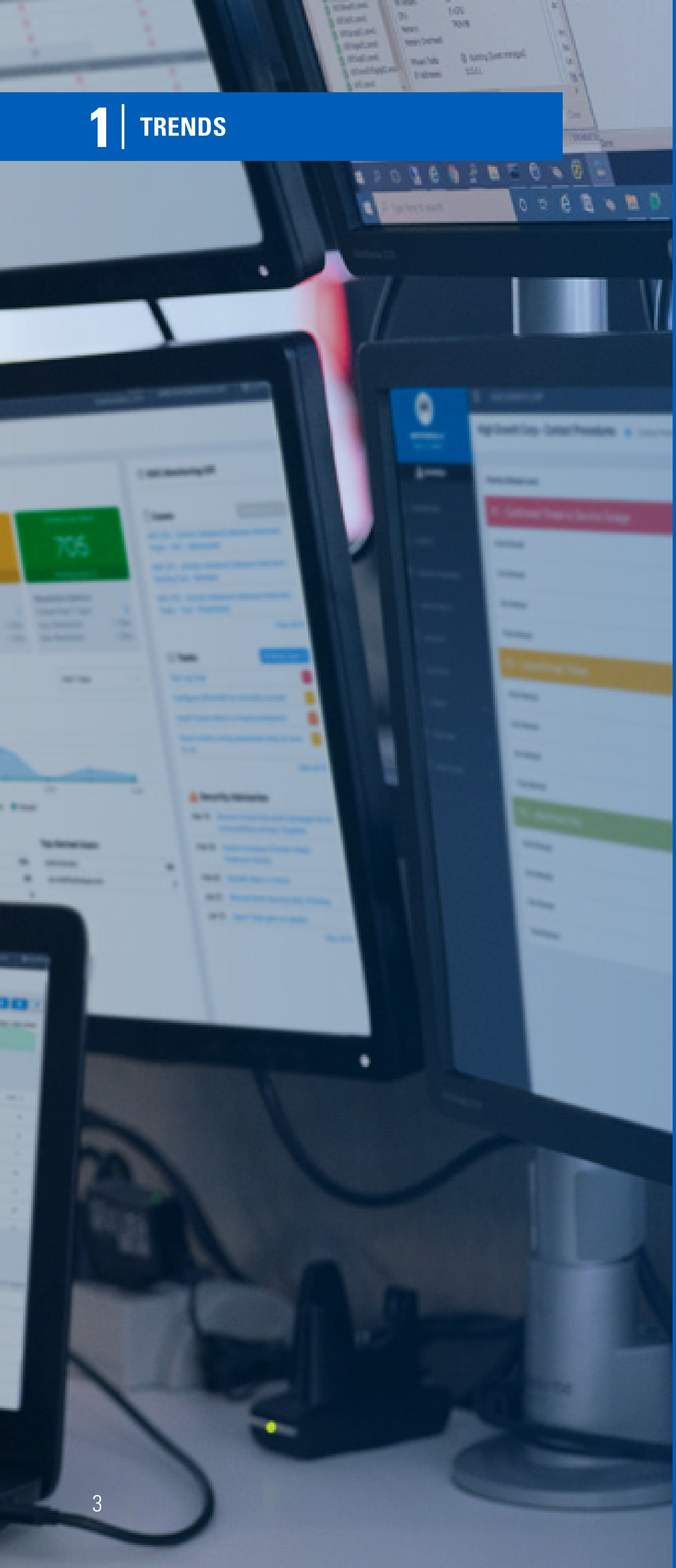
CYBER ATTACKS ARE A REALITY. AND THE STAKES ARE HIGHER THAN EVER.

System downtime is not an option for organizations today. Secure systems are imperative.

As cyber crime continues to proliferate throughout both public and private spheres, governments and businesses are becoming increasingly concerned about cybersecurity – and with good reason. Cyber attacks continue to increase in number, frequency and sophistication – costing agencies millions of dollars in a matter of minutes. For organizations around the globe, the uncertainty and the financial implications of an attack have made cybersecurity a top concern.

In the world of cybersecurity, things are changing at a rapid pace. The emergence of new technologies has lowered the bar for modern cybercriminals, expanding the cyber crime landscape for ransomware attacks and creating new vulnerabilities. Meanwhile, cyber attack types and techniques continue to evolve – disrupting operations without a moment's notice.





$10.5 TRILLION

IN ESTIMATED, ANNUAL GLOBAL COSTS DUE TO CYBERCRIME BY 2025.[1]

560 K

NEW PIECES OF MALWARE ARE DETECTED EVERYDAY.[2]

93%

OF COMPANIES ARE VULNERABLE TO CYBER CRIMINAL ATTACKS.[3]

287 DAYS

IS THE AVERAGE TIME MOST COMPANIES TAKE TO DETECT A DATA BREACH.[4]

FOR ORGANIZATIONS AROUND THE GLOBE, THE UNCERTAINTY AND THE FINANCIAL IMPLICATIONS OF A CYBER ATTACK HAVE MADE CYBERSECURITY A TOP CONCERN.

THE SECURITY CHALLENGE

The security strategies of the past are inadequate to protect against today's advanced and evolving cyber threats. Further compounding these challenges are a lack of security expertise, outdated systems, and a need for remote operations and cloud-based solutions. And while organizations continue to acknowledge the importance of protecting their systems, keeping up with reality can be a challenge.

DIGITAL TRANSFORMATION

While technological innovations, increased remote operations and a rise in cloud-based operations are bringing new functionalities and capabilities to organizations around the world, they are also increasing the potential cyber attack surface.

INCREASING COMPLEXITY

Today's complex but fragmented IT environments have generated visibility challenges across organizations. These challenges are being made worse by an increased number of security tools being operated to secure operations and meet regulatory requirements.

CHALLENGED RESOURCES

Continued difficulty in recruiting and retaining cyber security talent has created a growing skills shortage. And strained budgets and resources are resulting in out-of-date technology and an inability to invest in needed solutions. Ultimately, today's organizations are facing unrelenting pressure to do more with less.

60%

OF DIGITAL BUSINESSES

WILL SUFFER MAJOR SERVICE FAILURES DUE TO THE INABILITY TO MANAGE DIGITAL RISK.[5]

76

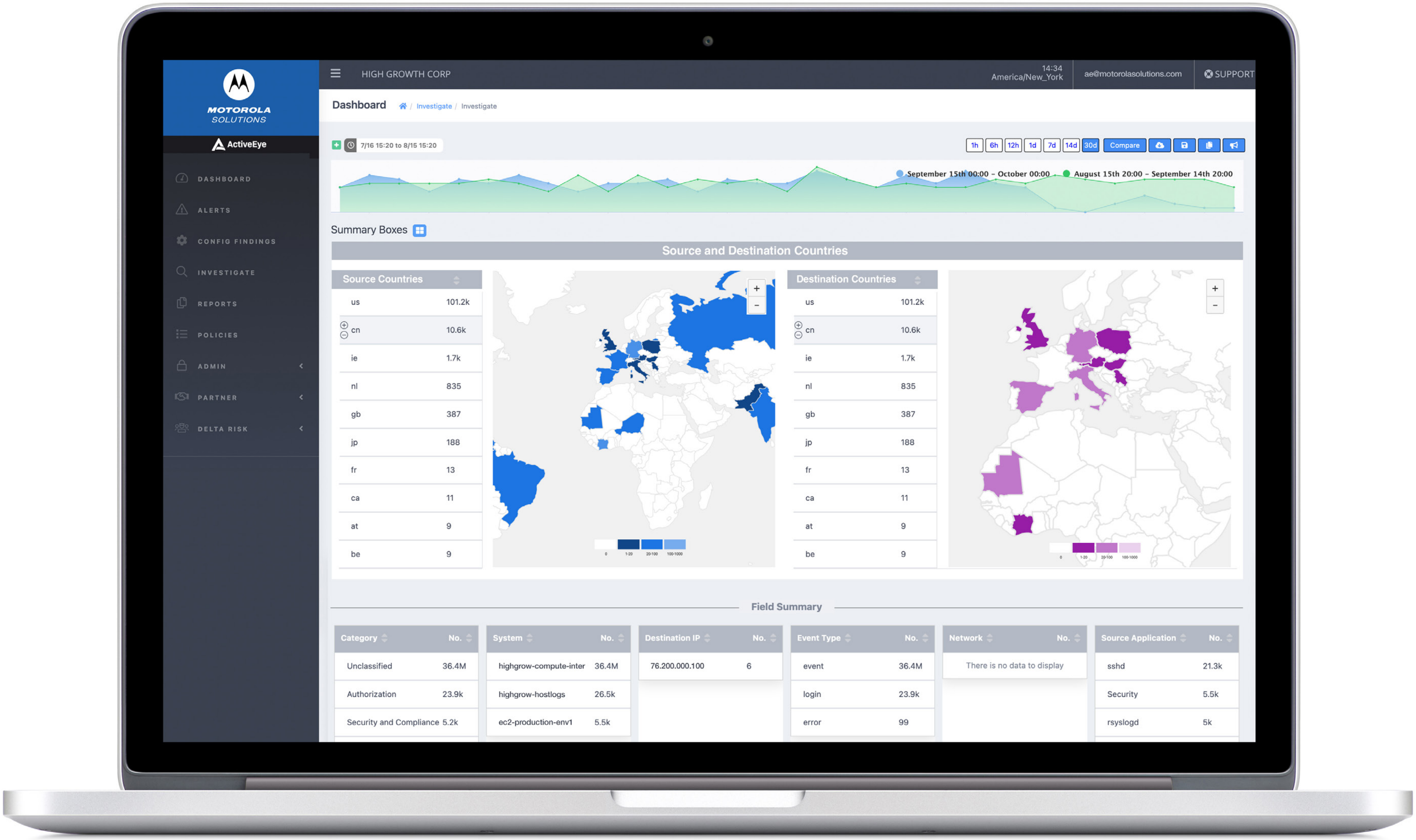
AVERAGE NUMBER

OF TOOLS ORGANIZATIONS ARE MANAGING.[6]

4

MILLION

UNFILLED CYBERSECURITY JOBS ESTIMATED WORLDWIDE.[7]



Dashboard / Investigate / Investigate

7/16 15:20 to 8/15 15:20

Summary Boxes

Source and Destination Countries

Source Countries	
us	101.2k
cn	10.6k
ie	1.7k
nl	835
gb	387
jp	188
fr	13
ca	11
at	9
be	9

Destination Countries	
us	101.2k
cn	10.6k
ie	1.7k
nl	835
gb	387
jp	188
fr	13
ca	11
at	9
be	9

Field Summary

Category	No.
Unclassified	36.4M
Authorization	23.9k
Security and Compliance	5.2k

System	No.
highgrow-compute-inter	36.4M
highgrow-hostlogs	26.5k
ec2-production-env1	5.5k

Destination IP	No.
76.200.000.100	6

Event Type	No.
event	36.4M
login	23.9k
error	99

Network	No.
There is no data to display	

Source Application	No.
sshd	21.3k
Security	5.5k
rsyslogd	5k

THE RIGHT PLAN

You need the right plan for secure and resilient operations. And you need a service provider who can provide unified security management and visibility across networks, devices, software and video, ensuring mission-critical responsiveness, resiliency and availability while enabling a predictable spend.

MANAGE COMPLEXITY

Today's mission-critical ecosystem is a set of sophisticated IT-interdependent technologies. You need to be able to simplify management and gain visibility and control into a heterogeneous system, while improving operational efficiency. This requires unified security management across the entire ecosystem – from networks to endpoints and cloud applications to radios.

MANAGE PERFORMANCE

"Always on, always-secure" is an imperative for your mission-critical operations. With highly responsive, resilient, always-available and secure systems you can ensure optimal business operations. In the case of cyber attacks, breaches can translate into huge financial losses and reputational damage – even regulatory actions.

MANAGE COSTS

Effective security management of systems doesn't have to come at a cost. Partnering with the right service provider can help reduce the total cost of ownership. Additionally, as-a-service models can give you the flexibility to pay for what you use – driving transition to an OPEX financial model. Predictable spend can minimize the risk of unexpected investments.

> THE RIGHT SERVICE PROVIDER CAN PROVIDE UNIFIED SECURITY MANAGEMENT AND VISIBILITY ACROSS NETWORKS, DEVICES, SOFTWARE APPLICATIONS, VIDEO, CLOUD ENVIRONMENTS AND ENDPOINTS.

TRUSTED CYBERSECURITY SERVICES FROM MOTOROLA SOLUTIONS

Motorola Solutions Cybersecurity Services bring together an integrated portfolio aligned to the National Institute of Standards and Technology (NIST) framework. As a trusted business partner, we help you develop roadmaps to safeguard your information, employees and systems.

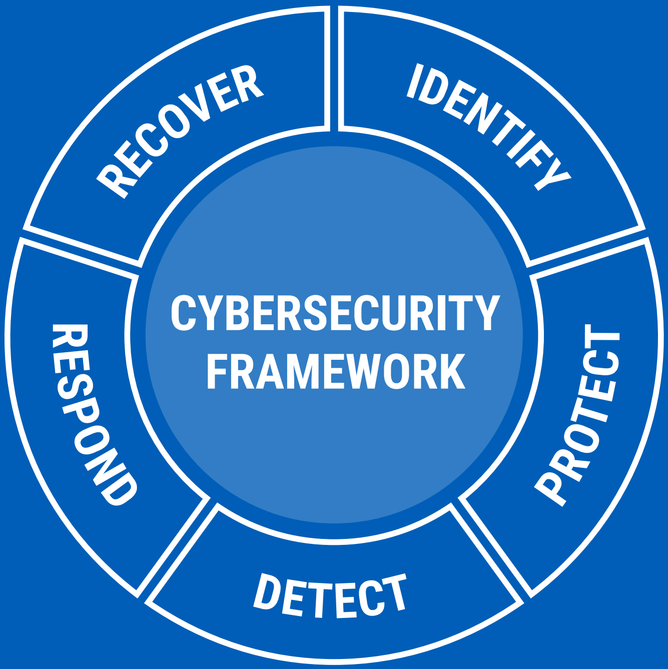
NIST-ALIGNED PORTFOLIO

ADVISORY SERVICES

Identify vulnerabilities and develop a robust cybersecurity strategy with risk assessments, penetration testing and system recovery services.

MANAGED SECURITY SERVICES

Protect your endpoints, network, cloud and mission-critical systems. As a managed security services provider (MSSP), we provide cost-effective solutions and expert assistance.



SECURITY PATCHING

Mitigate your cybersecurity risk with effective patching. Our security patching includes pre-testing, validation and anti-malware software updates aligned with industry standards.

CYBERSECURITY TRAINING

Combat potential cybersecurity attacks with cybersecurity training. Our program ensures your workforce has the right skills and expertise to address any incident.

ADVISORY SERVICES

To protect your systems it's critical to have a complete understanding of where you might be vulnerable and which regulatory and compliance frameworks impact your organization. Our security advisors can assess your organization and deliver critical insights to help you make informed decisions on the best security procedures and controls to implement. Our consultants can help build a robust cybersecurity strategy and roadmap in line with your business needs and industry best practices.

PENTESTING & TECHNICAL ASSESSMENTS

We offer a broad range of penetration testing and technical assessments, including internal, external and wireless pentesting. Our security experts simulate the thought processes and actions of attackers to get unauthorized access to systems or to extract sensitive information. Using a flexible methodology, rather than a fixed set of tools, we reveal issues that could put your organization at risk – before a malicious hacker exploits them.

RISK & GAP ASSESSMENTS

We start by understanding your requirements and current environment. Then we identify and define specific risk elements unique to your environment and compare them to compliance requirements and industry standards for cybersecurity. We deliver a readiness dashboard that addresses vulnerabilities, business process and skills alignment based on your technology attributes, security architecture and governance policies.

STRATEGY & COMPLIANCE

Document your cybersecurity program's strengths, accomplishments and key shortfalls – before the auditors and examiners do. Our compliance assessments give you the data-driven, prioritized recommendations to inform better cyber risk management and decision-making. Services include virtual Chief Information Security Officers (vCISOs), Vendors Assessments and Business Continuity/Disaster Recovery Planning.

CYBER EXERCISES

Tabletop exercises are valuable for evaluating existing security defenses, testing new procedures and establishing a fundamental method for training your security personnel on evolving threats. Our team uses their real-world expertise to develop engaging, discussion-based tabletop exercises. Tailored, scenario-based engagements can improve your ability to detect and respond to cybersecurity incidents faster.

INCIDENT RESPONSE PLANNING

When a cyber attack happens, will your team be ready? Our Incident Response Planning services provide best-in-class training and exercises to ensure that when a security incident or attack happens, your organization will be prepared to handle it. Whether you want to minimize damages or you're concerned that you've been breached and don't know it, we're ready to help. Our proven agile and evidence-driven approach will keep you in control of whatever chaos an incident may bring.

READ SOLUTION BRIEFS

Discover System Vulnerabilities with Penetration Testing ▶

Cybersecurity Frameworks and Standards for Risk Assessment and Consulting ▶

MANAGED SECURITY SERVICES

There's a constant need to prevent small security threats from evolving into bigger incidents, and to detect and remediate security issues faster. A service provider with the right people, technology and proven processes can proactively monitor and manage your security needs to stop small issues from becoming big ones. Our suite of Managed Security Services deliver 24/7 threat management and data protection across networks, endpoints, cloud infrastructure and applications.

MANAGED DETECTION AND RESPONSE

Our ActiveEye^{SM} security platform synchronizes security efforts between you and Motorola Solutions by allowing you to view threat insights, event investigations, security reports, threat advisories and the status of any security cases.

ActiveEye Managed Detection and Response (MDR) leverages our advanced ActiveEye security platform and experienced analysts to detect and respond to cyber threats in your IT environment as well as computer-aided dispatch (CAD), VESTA® 9-1-1 systems and ASTRO® 25 systems.

ActiveEye Advanced Threat Insights is an optional service that expands the standard SOC monitoring services provided by ActiveEye MDR. This service provides a more proactive, in-depth security research function to enrich awareness of your ongoing cybersecurity posture, optimize the value of existing security controls and ultimately lower cybersecurity risk. With the Advanced Threat Insights service, Motorola Solutions will assign a dedicated cybersecurity analyst to proactively work with you and your team.

Motorola Solutions' Security Operations Center (SOC) can monitor networks, applications, and devices for security threats 24/7 via ActiveEye. Our SOC analysts possess deep technical skills on both the offensive and defensive side of security to help recommend security device configurations that optimize threat detection and implement playbooks to cut through the noise and quickly address the most critical threats.

PUBLIC SAFETY THREAT ALLIANCE

Motorola Solutions established the Public Safety Threat Alliance (PSTA) in 2022, a cyber threat Information Sharing and Analysis Organization (ISAO) recognized by the Cybersecurity and Infrastructure Security Agency (CISA). The PSTA is designed to provide public safety agencies with the knowledge they need to better defend against risks like ransomware and data breaches. It operates as a single organization focused on the collection, analysis, production and sharing of actionable cyber threat information. Our global reach, combined with more than 90 years of experience supporting public safety customers and the communities they serve, allows us to rapidly establish a network of trusted partners and share information and intelligence on the most pressing cyber threats to public safety.

READ SOLUTION BRIEFS

Endpoint Security Services For Enterprise IT ▶

Be Resilient: Protect Your IT Network with Advanced Cybersecurity Services ▶

Get Deep Analysis and Dedicated Support with AcitveEye Advanced Threat Insights ▶

SECURITY PATCHING

Gaps in your software security can leave you open to a cyber attack - a chance you can't afford to take. Our security patching services can help you fix vulnerabilities within your system and protect for future events. Safeguard your mission-critical systems with our comprehensive Security Patching services that include patch identification, testing and flexible deployment, both remotely and on-site.

SECURITY PATCH IDENTIFICATION

The first step is to identify all patches required to keep your system secure. This includes servers and hardware-based appliances like firewalls and routers. Our engineers track all available anti-malware definitions and software patches. Only the applicable patches needed for your system are identified and selected for testing. This validates that no unnecessary software is introduced via the patching process.

SECURITY PATCH TESTING

This is a critical step. Before applying patches to your production system all potential patches are first implemented in a test environment to identify any potential risks or issues. This can be expensive for an agency to build an in-house test environment. We have a dedicate Information Assurance lab with test systems to validate patches, test interactions and identify procedures including if a reboot is required.

SECURITY PATCH DEPLOYMENT

Once validated as safe for deployment, we offer multiple ways to implement security patches. You can deploy patches or we can implement them for you by setting up a deployment cadence, weekly, monthly or quarterly. We work with you until the job is done. Our patch deployment reporting tool can illustrate your security patch operations and help you to better manage your cybersecurity operations.

> "THE REASON WHY WE CHOSE SECURITY PATCHING WAS REALLY TO PREVENT RANSOMWARE ATTACKS. WHAT WE TRY TO DO IS MAKE IT MORE DIFFICULT FOR THOSE PEOPLE THAT ARE WEARING BLACK HATS TO GET INTO OUR SYSTEM TO IMPACT THE FUNCTIONALITY."
>
> - Chris Petterson, Manager of the Waukesha County Radio Services[8]

READ SOLUTION BRIEF

Robust Security Patching Mitigates Cybersecurity Risks ▶

CYBERSECURITY TRAINING

Investing in your front-line defense with continuous cyber learning provides the opportunity for employees to both learn new skills and develop existing ones, ensuring that knowledge remains fresh and that employees remain confident in their abilities. Security professionals with the right skills and expertise can effectively address and combat cyber attacks.

Our delivery methods ensure you receive the right training, at the right time, via the method that works best for you – classroom learning and labs, on-line training and virtual instructor-led training.

Our instructors come from the ranks of full-time industry engineers and analysts to infuse training with real-world operational experience.

Training programs cover top cybersecurity concerns such as cloud security, incident response management, risk management and privacy planning and Telephony Denial Of Service (TDOS) / Distributed Denial Of Service (DDOS) attacks. We work together with your organization to bring a portfolio of credentials that are part of a holistic, programmatic approach to security and privacy.

DIVERSE LEARNING AND FLEXIBLE OPTIONS

You can take advantage of both formal and informal learning through a wide variety of options that include classroom, online, instructor-led, self-paced, hands-on labs, learning experience portal, virtual environment, custom courses and more.

RICH COURSE CATALOG

Courses spanning all State and Local, Department of Homeland Security (DHS) and Department of Defense (DoD) National Cybersecurity Workforce Framework (NICE) are available in line with your organizational needs, policy and procedures.

FIELD-PROVEN SECURITY AND PRIVACY EXPERTS

Our instructors come from the ranks of full-time industry engineers and analysts to infuse cybersecurity training with real-world operational experience and knowledge from customers across the globe.

POWERFUL PARTNERSHIP

We partner with your organization to understand your security requirements and bring a portfolio of relevant and valued credentials that are part of a holistic, programmatic approach to security and privacy.

READ SOLUTION BRIEF

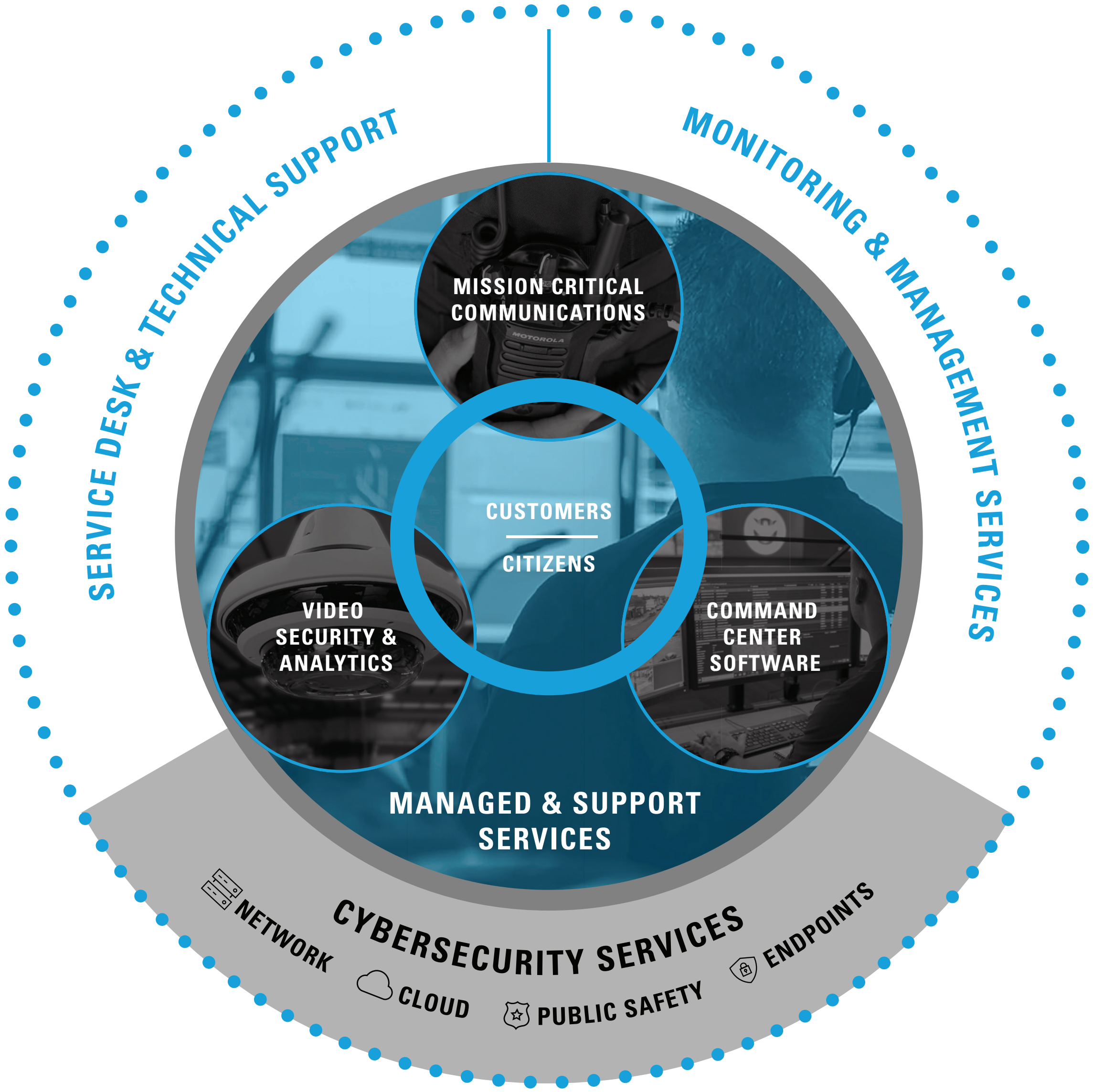
Keeping Skills Sharp Across the Complex Cybersecurity Landscape ▶

ONE SERVICE PARTNER FOR YOUR CYBERSECURITY NEEDS

With more than 90 years of experience managing mission-critical technologies and more than 20 years of developing cybersecurity solutions, Motorola Solutions is well-positioned to be the 'one service provider' for your cybersecurity needs.

With best-in-class people, process and technology we bring scalable operations that can help organizations manage cyber risk awareness, detection, response and recovery. Our cutting edge security automation and orchestration platform delivers 24/7 insights on security management, system performance and service delivery, enabling a 100 percent co-managed approach to security management.

We provide a purpose-built and integrated approach to end-to-end cyber resilience.


SERVICE DESK & TECHNICAL SUPPORT
MONITORING & MANAGEMENT SERVICES
MISSION CRITICAL COMMUNICATIONS
CUSTOMERS
CITIZENS
VIDEO SECURITY & ANALYTICS
COMMAND CENTER SOFTWARE
MANAGED & SUPPORT SERVICES
CYBERSECURITY SERVICES
NETWORK
CLOUD
PUBLIC SAFETY
ENDPOINTS

GLOBAL SCALE AND EXPERIENCE

300+

Security experts focused on 24/7 monitoring & response

9B

billion 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

Real-time visibility into threats via our ActiveEye Security Orchestration, Automation and Response (SOAR) platform

100% co-managed approach for visibility and control

Resources

1 https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

2 https://dataprot.net/statistics/malware-statistics/

3 https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=52a8a0337864

4 https://venturebeat.com/2022/05/25/report-average-time-to-detect-and-contain-a-breach-is-287-days/#:~:text=We%20are%20excited%20to%20bring,and%20virtually%20July%2020%20%2D%2028

5 https://www.gartner.com/en/newsroom/press-releases/2016-06-06-gartner-says-by-2020-60-percent-of-digital-businesses-will-suffer-major-service-failures-due-to-the-inability-of-it-security-teams-to-manage-digital-risk

6 https://www.infosecurity-magazine.com/news/organizations-76-security-tools/

7 https://www.infosecurity-magazine.com/news/cybersecurity-skills-shortage-tops

8 https://www.motorolasolutions.com/content/dam/msi/docs/services/waukesha-county-case-study.pdf

For more information on our Cybersecurity Services, contact your
Motorola Solutions representative or visit us at **www.motorolasolutions.com/cybersecurity**

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, Il 60661 U.S.A. **motorolasolutions.com**