

# 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 billions 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.



**\$6 TRILLION**  
IN ESTIMATED COSTS TO ORGANIZATIONS DUE TO CYBERCRIME IN 2021.<sup>1</sup>

**18 MILLION+**  
WEBSITES ARE INFECTED WITH MALWARE AT ANY GIVEN TIME.<sup>2</sup>

**300%**

INCREASE IN CYBERCRIMES SINCE THE COVID-19 PANDEMIC.<sup>3</sup>

**6 MONTHS**

IS THE AVERAGE TIME MOST COMPANIES TAKE TO DETECT A DATA BREACH.<sup>4</sup>

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 Further compounding these challenges are a lack of security expertise, outdated systems, and a need for remote operations and cloud-based solutions.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.<sup>5</sup>

**57**  
SECURITY TOOLS

ARE MANAGED ON AVERAGE BY SECURITY TEAMS.<sup>6</sup>

**4**  
MILLION

UNFILLED CYBERSECURITY JOBS ESTIMATED WORLDWIDE.<sup>7</sup>



## 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

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.

#### 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

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.

### RISK ASSESSMENTS

Our assessments provide your organization with useful insights, paint a full picture of your current environment and identify critical vulnerabilities and gaps that need to be addressed. We then use this information to develop a robust cybersecurity strategy that is mapped to key regulatory frameworks.

### PENETRATION TESTING

Our experts evaluate the security of your IT and communications infrastructure by trying to exploit its vulnerabilities. By detecting, analyzing and investigating threats we can reveal issues that could leave your organization at risk – before a malicious actor exploits them.

### CYBERSECURITY CONSULTING

Our team's expertise can help guide and augment your current IT, communications or cybersecurity teams – freeing up resources and helping to support operations. Our ongoing consultative approach ensures that security practices of your organization are ready to combat an ever-evolving threat landscape.

### GOVERNANCE AND COMPLIANCE

We ensure your team adheres to the regulatory cybersecurity requirements that are in line with your unique organizational needs and follow industry best practices – including ISO 2700/1, CMMC PCI, HIPAA, HITRUST, GDPR and more.

### 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.

### SECURITY PATCHING

Security patching provides your first line of defense against cyber attacks. All software needs to be patched – whether it sits on a disk or runs on a server, resides on a chip or in an app. We help streamline your organization's patch management by identifying and validating required updates, conducting extensive testing to ensure the system is ready and implementing installations on a weekly, monthly or quarterly cadence.

### SECURITY MONITORING

Proactive security monitoring helps you stay one step ahead. Our team of experienced, highly-trained and certified security professionals are staffed 24/7 at our Security Operations Center (SOC) and are dedicated to monitoring the secure state of your LMR and emergency call handling networks. We provide reporting services to ensure real-time visibility in your system's security performance as well as data analysis to improve ongoing security health.

### ADVANCED THREAT DETECTION AND RESPONSE

With resources in high demand, we can help your organization perform threat investigation and incident response around the clock. Our advanced security orchestration and automation platform, ActiveEye™, reduces noise and prioritizes threats for your enterprise IT team. We offer a co-managed solution to give you the flexibility you need. You can be assured that your organization has 24/7 monitoring for cloud, network and endpoint security – including ongoing threat and vulnerability insights.

### READ SOLUTION BRIEFS

Robust Security Patching Mitigates Cybersecurity Risks ▶

Stay Vigilant: Protect Your Network with Security Monitoring ▶

Advanced Threat Detection and Response for Enterprise IT ▶

## SYSTEM RECOVERY SERVICES

Breaches can translate into huge financial losses, downtime and reputational damage – even regulatory actions. Detecting threats earlier to address them faster can minimize the potential impact of cyber attacks on organizations. Our System Recovery Services are designed to help you swiftly respond to and recover from cyber attacks.

### BUSINESS CONTINUITY AND RESPONSE PLANNING

It's important to be prepared for a potential incident. We work with you to develop business continuity plans that will help you quickly develop an understanding of the potential systems, critical applications and data sources that may have been impacted during an incident. Our communication and escalation protocols ensure that all stakeholders receive status updates and are aware of steps being made to remediate a security incident.

### SYSTEM RECOVERY

Our team of security experts provides 24/7 support while an incident is ongoing. We begin with a deep-dive analysis and compromise assessment in order to scope out system vulnerabilities that might have been exposed. We then work together with your team to reinstate your system and improve network controls.

### POST-INCIDENT ANALYSIS

Following an incident, we complete a full report of all findings and response efforts to recommend and develop stronger application and network security controls. The data insights provided in the report will help your organization implement preventive measures and problem management.

**BREACHES CAN TRANSLATE INTO HUGE FINANCIAL LOSSES, DOWNTIME AND REPUTATIONAL DAMAGE – EVEN REGULATORY ACTIONS. OUR SYSTEM RECOVERY SERVICES ARE DESIGNED TO HELP YOU SWIFTLY RESPOND TO AND RECOVER FROM CYBER ATTACKS.**

### READ SOLUTION BRIEF

Swiftly Respond to and Recover from Cyber Attacks ▶

## 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.

### 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.

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.

### FIELD-PROVEN SECURITY AND PRIVACY EXPERTS

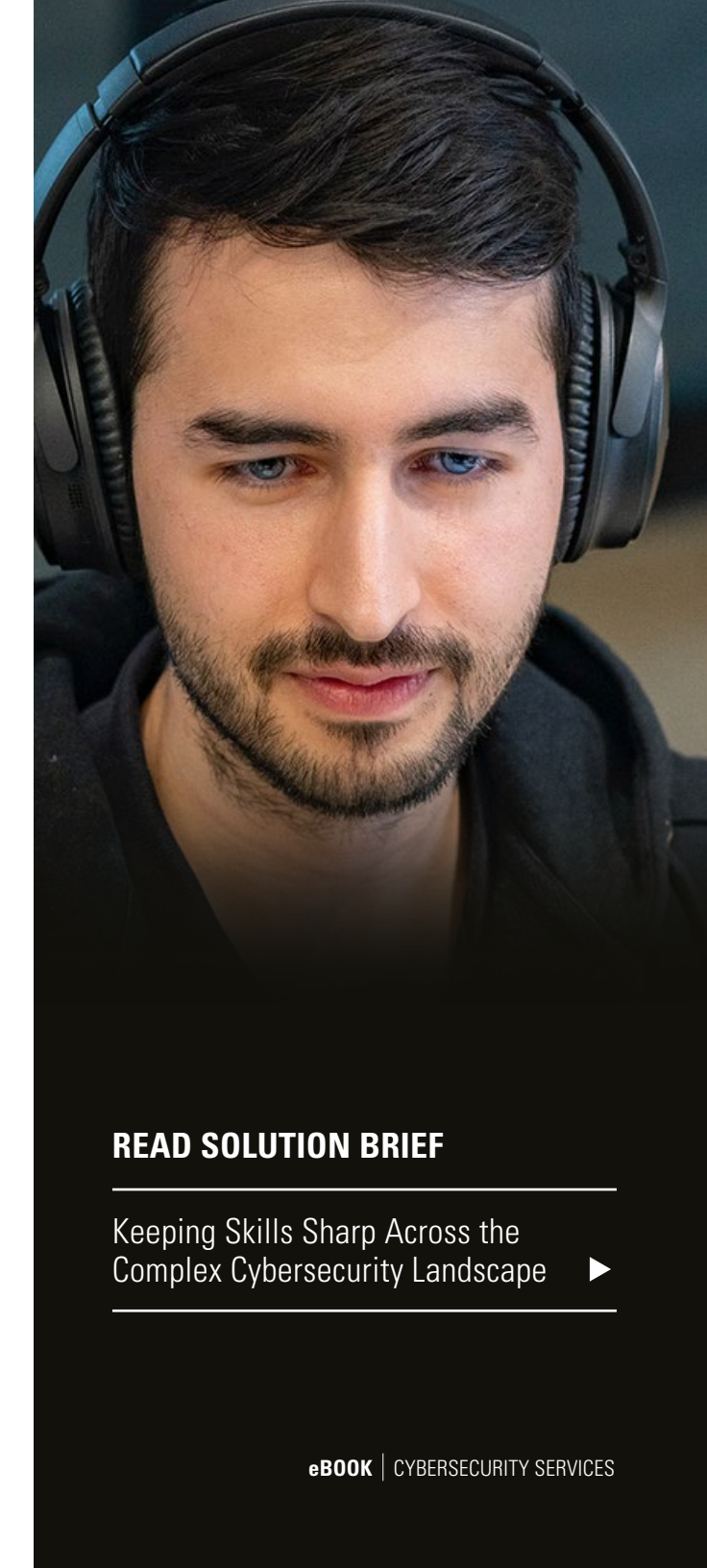
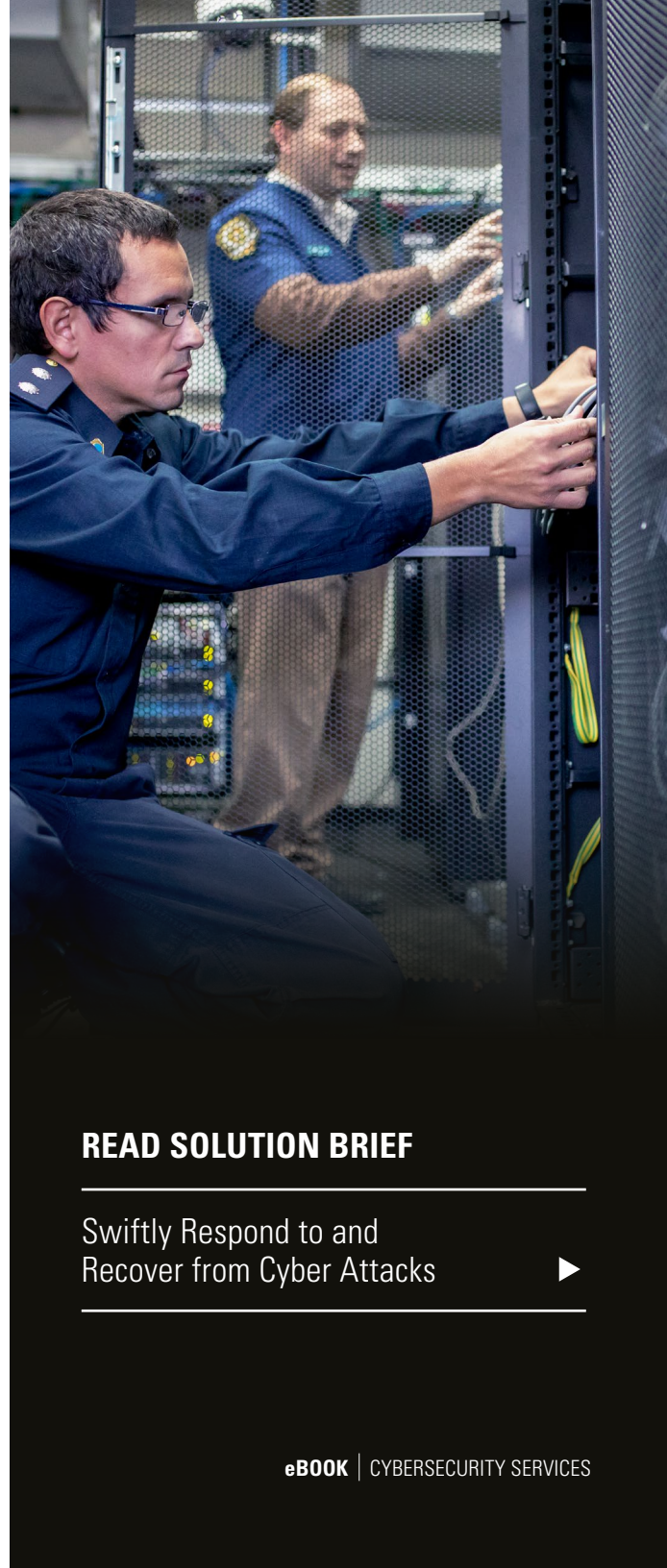
Our instructors come from the ranks of full-time industry engineers and analysts to infuse cybersecurity training with real-world operational experience and knowledge from customers across the globe.

### 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.



# GLOBAL SCALE AND EXPERIENCE

**300+**

Security experts focused on 24/7 monitoring & response

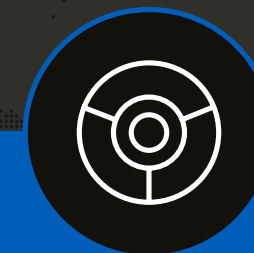


## PEOPLE

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

**9B**

billion security events proactively monitored each day



## PROCESS

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

**20+**

Years of experience developing cybersecurity solutions



## TECHNOLOGY

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

**100%** co-managed approach for visibility and control



## Resources

- 1 <https://www.natlawreview.com/article/ransomware-attacks-predicted-to-occur-every-11-seconds-2021-cost-20-billion>
- 2 <https://www.securityweek.com/185-million-websites-infected-malware-any-time>
- 3 <https://www.imcgrupo.com/covid-19-news-fbi-reports-300-increase-in-reported-cybercrimes>
- 4 <https://www.cybintsolutions.com/cyber-security-facts-stats/>
- 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.securitymagazine.com/gdpr-policy?url=https%3A%2F%2Fwww.securitymagazine.com%2Farticles%2F90334-how-cisos-can-consolidate-security-tools>
- 7 <https://www.infosecurity-magazine.com/news/cybersecurity-skills-shortage-tops>

For more information on our Cybersecurity Services, contact your Motorola Solutions representative or visit us at [www.motorolasolutions.com/cybersecurity](http://www.motorolasolutions.com/cybersecurity)



Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. [motorolasolutions.com](http://motorolasolutions.com)

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. ©2020 Motorola Solutions, Inc. All rights reserved.