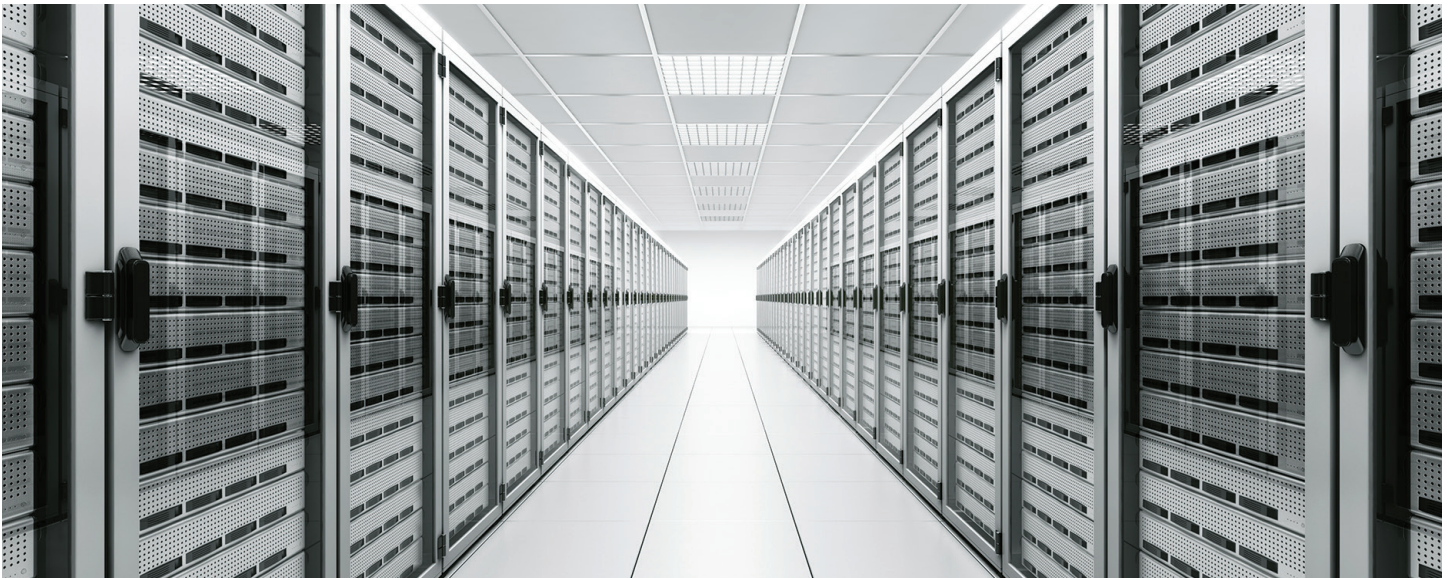**MOTOROLA** *SOLUTIONS*

SAFEGUARD YOUR INFRASTRUCTURE WITH CONTINUOUS ON-PREMISE MONITORING

ON-PREMISE SECURITY MONITORING FOR MISSION-CRITICAL SYSTEMS

PROACTIVE SECURITY MONITORING BECOMES THE NEW NORMAL

Continuous security monitoring is one of the key practices mission-critical organizations are adding to their cybersecurity strategy. With nearly 1 million malware released each day and many with increased sophistication[1], there is consensus that security patching, intrusion detection systems (IDS) and firewalls alone are not enough to protect your network. For mission-critical organizations, now prime targets for hackers, proactive security monitoring is imperative for safeguarding your network from cyber attacks. Also, cybersecurity frameworks such as the National Institute of Standards and Technology (NIST), ISO 27000, and other industry-specific security policies prescribe it as one of the top salient measures you can take against cyber threats.

THE VITAL ROLE OF SECURITY OPERATIONS CENTER

To address the scarce talent pool and offset the substantial expense from continuous security monitoring, organizations are using external security operations centers (SOC) to help monitor their networks remotely. Our SOC is staffed by experienced and trained, mission-critical security experts monitoring networks around the clock and ready to take immediate actions whenever cyber threats are detected. However, there are instances when remote security monitoring is not a viable option. If your mission-critical organization

has this restriction and cannot connect to an external SOC, Motorola Solutions' On-Premise Security Operations Center is a cost-effective and comprehensive alternative for achieving your security monitoring needs.

VALUE-BASED ALTERNATIVE TO REMOTE MONITORING

Installed inside your network perimeter, our On-Premise Security Operations Center allows you to effectively monitor your system for security incidents, potential threats and operational anomalies.

Minimal in comparison to the time, technology and investment required to establish and maintain an internally owned security operations center, our On-Premise Security Operations Center ensures that your system is continuously monitored and that information security continues to be a priority. The areas covered are defined below:

- Firewall, authentication and logging server integration
- Antivirus integration to detect worms, viruses and other forms of malicious software
- Integration of SNMP data pulled from the system SNMP server(s) every 24 hrs
- Network vulnerabilities and threats
- Abnormal network activity and operational anomalies
- Advanced behavioral analytics

The features included are also designed to help you identify and locate the source of cyber attacks as soon as they occur. They are:

Holistic event traffic insights. Capture and examination of system logs throughout your network infrastructure, devices, operating systems, software and applications.

Continuous monitoring. With the capability to function in attended and unattended modes, your system can be monitored round-the-clock without the presence of a physical resource 24x7.

Powerful correlation performance. Use of state-of-the-art "semantic correlation" technique to process more than 2,500 messages per second and handle traffic burst of more than 10,000 messages in one second to pin-point substantiated threats – alleviating false positives and omissions from a manual approach.

End-to-end intelligent alerting. Programmed with auto learning algorithms that become more informed over time from your system log data, alerts are generated based on learned system behaviors. From this, actionable tickets that can be assigned, investigated and resolved are created.

Customized mission-critical provisions. Tailored tool set to address the unique security monitoring needs of mission-critical environments using the knowledge accrued from Motorola Solutions' decades of experience and lessons learned from securing critical systems.

Automated alerting. Instant notification of significant threats to your network the moment they occur for organizations with an email or paging server tied to their systems.

Auto-generated reports. Easy-to-understand customized reports to keep you informed of your system's overall security events and risk posture.

Real-time visualization portal. Regularly updated dashboards reflecting vital information required by your team to identify security events of interest and respond accordingly. This includes an overview of the system status from the homepage.

IP-autonomous monitoring. Continuous monitoring of your system is situated within your isolated network environment alleviating the need for an external connection which further protects your monitoring tool from cyber threats.
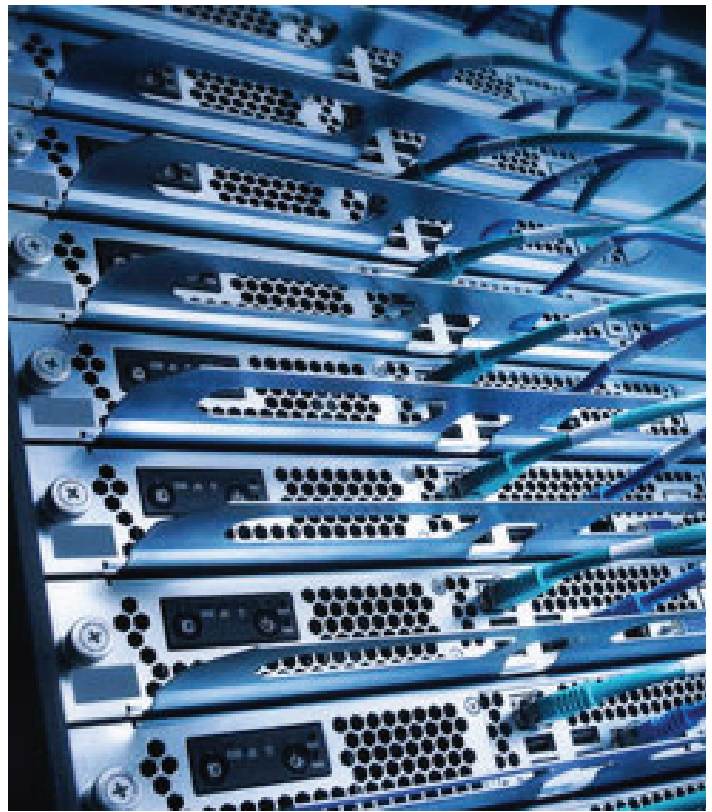
NEARLY 1 MILLION MALWARE RELEASED EACH DAY

With today's security and interconnected environment, you cannot afford to be left in the dark with the millions of cyber threats looking to infiltrate your organization. Designed by experts with robust capabilities to assist with today's cyber risk challenges, our On-Premise Security Operations Center is a reliable solution for continuously monitoring your network in-house. Your team will also have 24x7 access to our experience and highly skilled security analysts to help you response to and resolve detected threats and vulnerabilities.

SOURCE:
1. Symantec's 2015 Internet Security Threat Report (ISTR)

For more information about our On-Premise Security Operations Center, contact your Motorola Solutions representative or visit motorolasolutions.com/cybersecurity.

MOTOROLA SOLUTIONS