



Reduce vulnerabilities and risks with turnkey, public safety-grade managed services

With the move to IP-based next generation systems, new, more advanced cybersecurity threats have emerged that can hamper and potentially even suspend Emergency Communication Centre (ECC) operations. Around the world, cyberattacks have increased in numbers, types and their level of sophistication. As such, many ECCs are turning to a managed cybersecurity approach to combat and protect against potential cybersecurity threats.

Our Managed Services team was systematically established to monitor and protect critical ECC call management infrastructure and provide an increased level of protection over traditional out-of-the box solutions.

Active Remote Monitoring (ARM) Service

Active Remote Monitoring (ARM) is a real-time monitoring and response system that adds a layer of support that will identify system anomalies before they can become problems 24/7/365. Using trend analysis along with factory certified technicians from our Network Operations Centre (NOC), ARM looks for system vulnerabilities and seeks to predict incidents before they happen to ensure a quick response to any critical system alerts.

ARM uses several different means and protocols to provide comprehensive monitoring of your system and IP devices. Items such as memory, CPU, disks, fans and temperature performance are monitored, while servers are managed via Simple Network Management Protocol (SNMP).

Network management is guarded against unauthorized access, intrusion attacks and hacking with network switches and routers evaluated at the port level.

SNMP queries are used to detect different Object Identifiers (OID's) as well as monitor connected devices while constant presence is tracked via Internet Control Message Protocol (ICMP). Network Interface Cards (NICs) and lines on analog gateways are analyzed to identify abnormal usage, errors and changes including incoming/outgoing traffic.

Firewall Patching Service

Keep software and firmware updated as required annually to protect against system vulnerabilities.

GUARDIAN MANAGED SERVICES

Patch Management Service (Linux & Windows)

The Patch Management service provides thorough testing of patch files in conjunction with your specific operating environment to ensure updates and security patches are applied in a timely manner. The latest updates and patches are selected for rigorous testing and certification in our Product Verification lab. After a thorough assessment, updates and patches are synchronized for distribution to system servers and computers at the end user facility. Biannual updates are pushed out to all servers and workstations. The Managed Services team coordinates system rebooting with the end user's IT staff to seamlessly manage the update with no interruption to service.

Managed Antivirus Service

The Managed Antivirus service protects your call handling system from malicious programs by remotely monitoring, scanning, and mitigating threats. All antivirus definitions are validated prior to installation via our product verification lab. The Managed antivirus service includes:

- » Real-time Antivirus and Anti-malware Detection and Removal Engines
- » System Performance Optimizer
- » File Encryption
- » Managed Services
 - » Multiple Scan Levels
 - » USB Immunizer (protects flash drives from virus infection when connected to a PC)



Managed Cybersecurity Service

Operated by highly trained security analysts, our Managed Cybersecurity Service provides regular reports every 6 six (6) months (coordinated with Microsoft® updates) summarizing alerts, actions taken, and provides a current assessment of your overall status. Our comprehensive cybersecurity service includes:

- » Endpoint Detection and Response (EDR) is focused on detecting and investigating suspicious activities on hosts/endpoints including workstations, servers, gateways, firewalls, or anything connected to the internet.
- » Managed Detection and Response (MDR) provides threat hunting, reporting, logging, and archiving services as well as responds to threats upon discovery.
- » Security Information Event Management (SIEM) which includes EDR protects critical

endpoints and servers from zero-day attacks and mutating malware. SIEM provides the ability to gather security data from information system components and presents it as actionable information via a single interface.

- » Threat and Vulnerability Management (TVM) is a platform designed to discover and monitor network assets and vulnerabilities.

IT environments of ECCs are becoming increasingly more complex. By partnering with Solacom we will assess, pinpoint, and prioritize vulnerabilities. Our remediation services with confirmed vulnerabilities as well as and any risks that could compromise system operations are addressed promptly keeping you one step ahead.

To get more information on our Managed Services, please speak with your local Solacom Account Manager.

ABOUT SOLACOM

Solacom (a subsidiary of Comtech Telecommunications Corp.) provides the most flexible multimedia emergency call handling solutions for emergency communications centres (ECCs). Comtech Telecommunications Corp. is a leading global technology company providing terrestrial and wireless network solutions, next-generation emergency services, satellite and space communications technologies, and cloud native capabilities to commercial and government customers around the world. Our unique culture of innovation and employee empowerment unleashes a relentless passion for customer success. With multiple facilities located in technology corridors throughout the USA and around the world, Comtech leverages our global presence, technology leadership, and decades of experience to create the world's most innovative communications solutions. For more information, please visit www.comtech.com.

1 (888) 765-2266 // 1 (819) 205-8100 // cst-sales@comtech.com