MONITORING AND MANAGEMENT

US Signal's Remote Monitoring and Management (RMM) is a server operating system, endpoint monitoring, and altering service designed to assist you with the ongoing management of performance, patching, anti-virus, process automation, and remediation.

AT-A-GLANCE

+ Remote Monitoring and Management infrastructure components fully hosted by US Signal

+ All generated alarms are reported directly to you and or the US Signal's 24/7 Technical Operations Center

+ Work with engineers from US Signal's managed services team to define automated tasks and remediation actions based upon expected altering criteria

+ Automated or manual patching of supported Microsoft operating systems

+ Optional anti-virus enhancement to protect workloads from malware and viruses

+ All traffic between monitored endpoints and hosted management infrastructure is encrypted

PATCH MANAGEMENT

Provides manual or scheduled installation of supported Windows OS and third-party application level software patches based on policies defined and created between you and the US Signal managed services team during the onboarding process.

REMEDIATION

Includes the investigation of sustained alarms by US Signal's managed services team to identify the root cause of the alarm, as well as a resolution or recommendations for a resolution. Remediation and troubleshooting does not extend into the application layer.

TECHNICAL OVERVIEW

The US Signal Monitoring and Management solution is hosted and maintained by US Signal to provide you with 24/7 monitoring, technical remediation, patch management, automation, and virus protection for your covered endpoints. During the RMM deployment, you will work with US Signal's hands-on services team to deploy software agents, adjust monitoring thresholds, determine patching schedules, and automate common maintenance tasks. Depending on the contracted services, engineers from US Signal's managed services team will provide additional personal insight and assistance in remediation.

MONITORING AND MANAGEMENT TECH SHEET

TECHNICAL OVERVIEW CONT.

Service	Standard Tier	Premier Tier
Patch Management	X	X
Server and Network Endpoint Monitoring	X	X
Server Performance Monitoring	X	X
Performance Reports	X	X
Alert Notifications	X	X
Monthly Review of Environment	X	X
Anti-Virus	Optional	X
Process Automation	Optional	X
Remediation	Optional	X
Automated Preventative Maintenance		X

SUPPORTED SERVER OPERATING SYSTEMS

+ Microsoft Windows 2016
+ Microsoft Windows 2012/2012 R2
+ Microsoft Windows Small Business Server 2011
+ CentOS 6.7 and above
+ RedHat Enterprise Linux 6.6 and 7
+ Ubuntu 14.04 and 16.04
+ Debian 8.7 32/64 bit

AUTOMATION MANAGER

Configure to perform automated tasks based on policies defined and created between you and US Signal's managed services team during the RMM onboarding process. The Automation Manager may be used to perform supported OS and third party application level tasks on your behalf when pre-defined parameters or global variables are met.

ANTI-VIRUS

US Signal will install anti-virus software on supported operating systems, which is responsible for scanning for the presence of viruses and malware based on manual or scheduled tasks. US Signal will monitor the anti-virus software to ensure its configured scan intervals are met, operational status, virus signatures and definition files are current, as well as the automated action taken when evidence of a virus or malware is detected.

Supported Operating Systems

+ Microsoft Windows Server 2016
+ Microsoft Windows 2012/2012 R2
+ Microsoft Windows Small Business Server 2011

Detection Types

+ Boot Sector
+ File
+ SMTP
+ POP3
+ Registry

+ Cookie
+ HTTP
+ Phishing
+ Process
+ Stream

MONITORING AND MANAGEMENT TECH SHEET

COMPLIANCE

The US Signal Remote Monitoring and Management solution is built using security standards to be in compliance with the following:

+ HIPAA
+ PCI

CONNECTIVITY

Implement Remote Monitoring and Management on any workload with Internet connectivity. All traffic between monitored endpoints and management infrastructure is protected by SSL/TLS encryption.

SERVICE LEVEL AGREEMENTS

Response Time Objective (maximum elapsed time objective from receipt of alarm within US Signal's alarm management system to customer notification):

+ **Standard Tier:** 30 minutes
+ **Premier Tier:** 15 minutes

The availability metric for the RMM client interface is 99.99%.

Customer Site

US Signal Enterprise Cloud Workloads

Private IP Space

US Signal RMM Infrastructure

SSL Encrypted Traffic

Third Party Cloud Workloads

Private IP Space