DATA SHEET

MANAGED MALWARE PROTECTION

Managed Security Services

AT A GLANCE

For customers invested in Cisco's ASA, Firepower or ISE we deliver advanced malware detection and response services to detect and respond to threats.

In a world with dynamically changing threats, targeted attacks and advanced persistent threats (APTs) static security devices are not enough. We can defend our customer networks against threats utilising a market leading Next Generation Intrusion Prevention System and deep integration into our SIEM platform to provide multi-dimensional behavioural analytics, extended visibility and continuous monitoring for real-time threat detection & response.

Our SOC technology (Powered by Si Consult & LogRhythm's Security Intelligence Engine) has a deep integration to Cisco's ASA, Firepower, AMP and ISE devices for real-time analysis, and for correlation of threat activity and known vulnerabilities with other network data.

SOC DETECTION	SOC RESPONSE
Cisco ASA Firepower Our SOC Security Intelligence Platform and Cisco's next-generation ASA firewalls integrate to provide unprecedented visibility and control into client-side applications, operating systems, virtual machines and mobile devices to meet a variety of use cases and strengthen end-to-end threat lifecycle management.	Our SOC can ingest and optimise FireSIGHT data in real-time, and correlate threat activity and known vulnerabilities with other network data to deliver advanced security analytics, extended visibility, and provide continuous monitoring for real-time threat detection and response. Our SOC can initiate immediate protective action such as terminating communications with command-and-control servers or adding the malicious IPs to a Cisco firewall policy to prevent critical applications and servers from exposure.
Cisco FireSIGHT Management Center Integration Our SOC technology leverages Cisco's eStreamer API to collect network security and flow data from the Cisco FireSIGHT Management Center (formerly Sourcefire), including information generated by Cisco's next-generation firewall, Cisco ASA with FirePOWER services, and by Cisco's next-generation Intrusion Prevention System (NGIPS), Cisco FirePOWER NGIPS.	
Cisco AMP Threat Grid LogRhythm continually consumes and analyses malware and threat intelligence data provided by AMP Threat Grid and combines this with other machine data collected from across the environment to help organisations proactively identify and defend against attacks targeting their network.	Our SOC correlates the malware artifacts discovered by AMP Threat Grid and changes to the behaviour of endpoints and users. The SOC rapidly prioritises high risk events and takes immediate action. It then initiates immediate protective action such as automatically adding malicious IPs to a Cisco firewall policy to prevent critical applications and servers from exposure.

FEATURES SUMMARY

- All security logs remain in country
- 24 x 7 monitoring & management
- Real time incident response system
- Advanced malware protection & next-generation IPS
- Packet level forensics and sandboxing
- Network behaviour analysis
- Integration with our next-generation SIEM for behavioral analytics
- Behavioral whitelisting
- Statistical baselining
- Real-time threat management
- Continuous compliance
- Host & network forensics
- Deeper visibility and contextual awareness into network events with advanced correlation across the entire IT environment to deliver enterprise-wide threat detection
- Access to the most up-to-date threat intelligence to help organisations detect advanced malware attacks and realize the extent of the outbreak for fast remediation
- Automated and immediate action against threats such as advanced persistent threats (APT) and zero-day attacks

DATA SHEET

MANAGED MALWARE PROTECTION

Managed Security Services

SECURITY MONITORING FEATURES

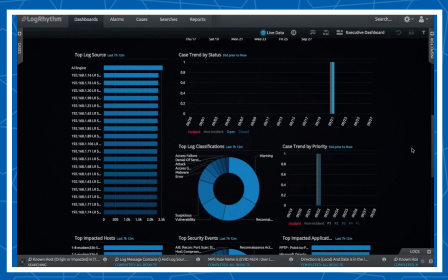
- 24 x 7 monitoring of customer devices
- All security logs remain in country
- Real time incident response system
- Real time events from the firewall
- Storage of events for forensic analysis
- 15 minute SLA escalation response time
- Efficient monitoring of standards in meeting the SLA expectations
- Weekly, monthly and quarterly reports
- Performance, availability & threat management
- Award winning SIEM technology
- Customer security management portal
- Custom dashboards
- Compliance monitoring
- Incident detection
- Incident response support
- Log retention for 90 days
- Custom correlation of security events and alerts

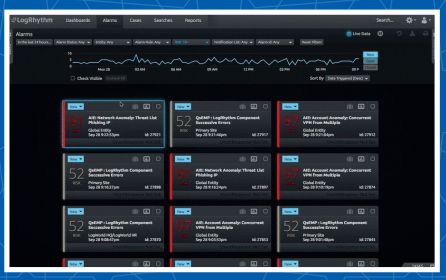
OPTIONAL - SECURITY MANAGEMENT FEATURES

- 24 x 7 management of customer devices
- Configuration of antivirus, antispyware, file blocking, anti-spam, anti-phishing, URL blocking and filtering, and content filtering
- Firewall architecture planning support
- Device migration / deployment
- Policy and rule-set management
- Performance / availability management
- Patch management
- Device backup and recovery
- Compliance reporting
- The service options include:
  - Essential - Security Monitoring
  - Optional - Device Management
  - Optional – IPS Supply

CUSTOMER DASHBOARD

Our customers benefit from direct access to our award winning SOC platform, which is powered by LogRhythm. This provides real time security event monitoring, anomaly detection and policy violation. This allows us to correlate event traffic and contextualize logs with threat, policy and vulnerability metrics.





SLA METRICS

SECURITY ALERT NOTIFICATION		
PRIORITY	SEVERITY LEVEL	MEAN RESPONSE TIME
P1	Critical	15 Minutes
P2	Major	45 Minutes
P3	Minor, Informational	120 Minutes

RESOLUTION / ESCALATION		
PRIORITY	SEVERITY LEVEL	MEAN RESPONSE TIME (HRS)
P1	Critical	4
P2	Major	8
P3	Minor, Informational	24

SERVICE SIZING PARAMETERS

SIZE	USERS	TYPICAL PERFORMANCE	CISCO FIREPOWER 7000 SERIES
Small	50	10-50 Mbps	7010
Medium Small	500	50 - 100 Mbps	7020
Medium	1000	100 - 250 Mbps	7030
Medium Large	2500	250 - 500 Mbps	7050
Large	10000	1 Gbps	7120

CHANGE MANAGEMENT		TARGET LEAD TIME	
		EVALUATION (HRS)	EXECUTION (HRS)
P1	Emergency	4	4
P2	Planned - Major	120	120
P3	Planned - Minor	72	72
P3	Routine	72	72