ENHANCED SECURITY SERVICES

Acumera's Enhanced Security Services (ESS) provide network traffic monitoring, managed detection and response, and around-the-clock support for your multi-site business.

LOG MONITORING AND 24x7x365 NETWORK SUPPORT

- **Proactive defense-in-depth architecture** that combines network traffic inspection with managed detection and response (MDR)

- **Dedicated security personnel** to review network traffic using established processes to target and resolve threats at every location in your network

- **Global traffic analysis** with continuous review of inbound and outbound network traffic passing through the Acumera's MG™ Edge Security Device and managed switches

- **PCI compliant retrieval, storage and access** to your network and device logs in support of PCI DSS r. 10.7

MANAGED DETECTION AND RESPONSE

- **Threat intelligence feeds** to monitor for critical traffic anomalies and indicators of compromise (IoC) as well as monitor the capture and retention of firewall logs

- **Alerts** on basic traffic anomalies and IoC, such as communication with anonymous proxy endpoints, changes in overall traffic patterns, anomalous traffic to non-US countries and spikes in blocked outbound traffic

- **Automated and manual responses** to detection of threats, including incident triage, reporting, analysis and closure

- **Web filter and Intrusion Detection System (IDS)** with real-time traffic analysis, full packet capture and active threat response (available with ESS PLUS)

- **Internal and external scanning** to meet PCI DSS requirements (available with ESS PCI)

Enhanced Security Services Options

	ENHANCED SECURITY SERVICES STANDARD	ENHANCED SECURITY SERVICES **PLUS**	ENHANCED SECURITY SERVICES **PCI**
Threat Monitoring Global traffic threat monitoring and analysis of traffic anomalies and indicators of compromise (IoC)	✓	✓	✓
Log Retention Capturing and storage of firewall logs; one-year retention and immediate access to recent logs in support of PCI DSS r.10	✓	✓	✓
Alerting Alerts on traffic anomalies and indicators of compromise (IoC), managed through the AcuVigil™ Dashboard	✓	✓	✓
Reporting and Security Planning Customized monitoring and reporting, as determined with your dedicated security expert	✓	✓	✓
Threat Response Automated and manual response processes for identified threats, including incident triage, reporting, analysis and closure	✓	✓	✓
Intrusion Detection System Intrusion detection by traffic anomaly and behavioral analyses, plus deep packet inspection utilizing threat intelligence from numerous sources; supports PCI DSS r. 11.4		✔	✓
Web Filter Service Filtering to block viruses and malware via DNS; includes blacklisting, content blocking and SafeSearch features		✔	✓
PCI Scanning Internal and external scanning services to meet PCI DSS requirements; automated and reviewed in the AcuVigil Dashboard; external scans conducted by an Approved Scanning Vendor (ASV) as required by PCI			✔

TO ORDER OR FOR MORE INFORMATION: 512.687.7410 | sales@acumera.net