## Clearnetwork USM – Unified Security Management - PCI-DSS Compliance

At Clearnetwork, we understand that PCI compliance is a process, not a checkbox. To achieve compliance takes focus, determination, and the right set of tools. Clearnetwork USM is a fully managed solution that provides you with in-depth coverage of PCI-DSS requirements without the headaches of multiple solutions that are managed on-site. When a vulnerability, threat or compliance issue arises, our security analysts quickly alert you so your IT team or consultant can remediate it. Multiple detailed PCI-DSS Compliance Reports are provided on request.

The following is a breakdown of what is provided with our USM service

- Asset Discovery and Inventory
- Vulnerability Assessment
- Intrusion Detection (IDS)
- File Integrity Monitoring (FIM)
- SIEM Event Correlation
- Log Management & Monitoring
- PCI DSS Compliance Reporting

**Here are the PCI requirements that are covered by our USM service**

**1.1, 1.2, 1.3**

• Built-in asset discovery provides a dynamically updated inventory of assets across your cardholder data environment, ensuring only authorized endpoints are deployed.

• Capture events relating to configuration changes on firewalls and routers, including when user accounts get updated.

• Discover unauthorized communications, such as between untrusted networks and systems within the cardholder data environment.

**2.1, 2.2, 2.3, 2.4, 2.6**

• Identify use of default system accounts on Windows machines.

• File Integrity Monitoring can detect changes and access to critical system and application files, and Windows Registry entries.

• Identify vulnerabilities such as where an application may have a cryptographic algorithm vulnerability, and recommend if patches or workarounds are available.

• Identify services are running, and what ports are open, on systems.

• Built-in asset discovery provides a dynamically updated inventory of what systems are operational in your environment, and what software is running on each.

• Discover and monitor assets running on-premises, and in cloud environments (including Azure, VMware, Hyper-V, AWS).

**3.6, 3.7**

• Monitor for changes to Office 365 policies including Data Leakage Protection (DLP), information management, and more.

• File Integrity Monitoring can detect when SSH or similar cryptographic keys are modified.

• Unified log review and analysis, with triggered alarms for high risk systems.

**4.1, 4.3**

• Identify when network traffic goes to unauthorized networks.

• Identify systems using compromised or insecure protocols that may increase their risk of being attacked.

• Monitor for changes to Office 365 policies including Information Management, and more.

**5.1, 5.2, 5.3, 5.4**

• Identify systems susceptible to known vulnerabilities, or that may not have antivirus installed and/or operational.

• Identify for indicators of malware-based compromise, and orchestrate manual and automated actions to isolate infected systems and block malicious domains

• Monitor and store events from antivirus solutions that could indicate a compromise, or attempt to disable antivirus software.

• Monitor for changes to Office 365 policies including Information Management, and more.

**6.1, 6.2**

• Identify systems susceptible to known vulnerabilities, with systems ranked as ‘high’, ‘medium’ and ‘low’ risk vulnerabilities.

• Identify patches or workarounds available to vulnerable systems.

**7.1, 7.3**

• Identify attempts to access systems using privileged accounts.

• Identify escalation of privilege attempts.

• Monitor for changes to Office 365 policies including Information Management, and more.

**8.1, 8.2, 8,5**

• Aggregate logs and events from systems, applications and devices from across your on-premises and cloud environments.

• Identify attempts to use retired or default user credentials.

• Monitor and alarm on Group Policy errors.

**10.1, 10.2, 10.3, 10.4, 10.5, 10.6, 10.7, 10.8**

• Aggregate, analyze and archive logs and events from systems, applications and devices from across your on-premises and cloud environments.

• Identify logon success and failures.

• Identify privilege escalation attempts.

• Identify where systems are out of sync with the current time and/or Domain Controller, or for nontypical traffic on port 123.

• Identify unauthorized attempts to access or modify key logs.

• Identify where security tools, such as antivirus and firewalls, have been disabled or have failed to start.

• Captures all user account creation and modification activities.

**11.1, 11.2, 11.4, 11.5, 11.6**

• Assess systems for vulnerabilities, and where found rank them as 'high', 'medium' and 'low' risk.

• Monitor access to and attempt to modify system and application binaries, configuration files, log files.

• Monitor user and administrator activities in cloud environments such as Azure and AWS, and within cloud applications such as Office 365.

• Apply labels to alarms

• Generate incident tickets within popular solutions like ServiceNow

**12.1, 12.5, 12.8**

• Monitor for changes to Office 365 policies including Data Leakage Protection (DLP), information management, and more.

• Monitor all administrative activities through popular authentication and authorization solutions like Azure Active Directory.

• Monitor network traffic for violations of policy, such as communications that cross your cardholder data environment perimeters.