Key Product Features and Highlights

Security Monitoring for Your Cloud & On-Premises Environments

Clearnetwork USM brings you powerful threat detection capabilities across your cloud and on-premises landscape, helping you to eliminate security blind spots and mitigate unmanaged shadow IT activities. Even as you migrate workloads and services from your data center to the cloud, you have the assurance of seamless security visibility.

Clearnetwork USM natively monitors

› AWS and Microsoft Azure public clouds
› Windows and Linux endpoints in the cloud and on prem
› Virtual on-premises IT on VMware / Hyper-V
› Physical IT infrastructure in your data center
› Other on-premises facilities (stores, retail stores, etc.)
› Cloud applications like Office 365 and G-Suite

Comprehensive Incident Response

Clearnetwork's security experts learn your network, they work hard to minimize false positives and bring you actionable information on threats and vulnerabilities in your organization. We will call you for serious threats, and send a ticket/email for normal non-priority threats. With select devices/applications like Cisco Umbrella, Palo Alto Firewalls, Carbon Black Next Gen-AV and several others, we can even respond to threats directly for you.

We also can –

› Generate custom alarms from parameters you provide
› Integrate with your ticketing system
› Disable the network card to prevent threats from spreading before you remediate

Built Natively in the Cloud for the Cloud

Unlike other legacy security solutions that have been modified to work in the cloud, USM is a truly cloud-native security monitoring solution that leverages the unique security elements of public cloud infrastructure. It uses direct hooks into cloud APIs to give us a richer data set, greater control over the security of your cloud infrastructure and SaaS applications, and more immediate visibility across your entire environment within minutes of installation.

Advanced SIEM and Correlation

Clearnetwork USM takes an enhanced approach to SIEM event correlation that makes security analysis faster, more flexible, and more effective than ever. Our unique, graph-based approach to correlation, enables us to:

› Quickly and efficiently run ad-hoc queries on large and complex data sets
› Enhance correlation by keying on connections between assets, users, and activities and the changes occurring between them

Skilled Security Analysts

The lack of skilled security expertise on staff and the high cost to find and hire them due to the skill shortage has organizations scrambling. Clearnetwork USM solves this issue by bringing you a fully managed service backed by security professionals with decades of combined experience. They will walk you through the threat response process by email and phone and are always available to answer your questions at no additional cost.

Comprehensive Compliance Reporting

To meet compliance mandates of PCI DSS, HIPAA, NIST and other regulatory standards, you must demonstrate that you regularly monitor your IT environments and that your IT controls are working. This demands rigorous reporting on your assets, vulnerabilities, and potential threats, which can be very time-consuming if done manually and can slow down or jeopardize your audit process.

Clearnetwork USM provides "audit ready" reports for PCI-DSS, HIPAA, NIST, ISO-27001, NERC-CIP, SOX, SOC2 and more!

Deploying Clearnetwork USM is Fast and Easy

Clearnetwork USM consists of a highly scalable, two-tier architecture to manage and monitor every aspect of your cloud and on-premises security. USM Sensors and Agents collect and normalize data from your cloud and on-premises environments and securely transfers that data to USM for centralized collection, security analysis, threat detection, and compliance-ready log management. The only thing you deploy in your environment are Sensors and Agents. Clearnetwork maintains, secures, and updates USM automatically. Install typically takes less than 1 hour.