DATA SHEET

SOC As A Service

Threat Detection, Incident Response & Compliance in One Managed Service

CLEARNETWORK
YOUR CYBERSECURITY EXPERTS

**FREE SECURITY AUDIT AND REVIEW

These days we know it all too well, Anti-virus and Firewalls are not enough. Attackers continue to advance, using increasingly sophisticated techniques to infiltrate organizations. They invest significant resources conducting reconnaissance to learn about organizations and to develop techniques specifically designed to bypass the security defenses being used. IT staffs know about the problem, but they lack the time, expertise, and budget to properly watch all their ever-changing on prem and cloud infrastructure for threats. They are also bombarded by a flood of security products and services that all promise different outcomes and don't know what to do. What they need is a solution that works with the security products and infrastructure that's already in place. A service that proactively watches their on-prem, cloud and hybrid infrastructure for both threats and vulnerabilities and gives them actionable information backed by skilled security analysts.

Clearnetwork SOC As A Service, also commonly referred to as Managed SOC, Cyber Threat Monitoring or Managed Detection and Response delivers powerful threat detection, incident response, and compliance management in one fully managed service. We combine all the security capabilities needed for effective security monitoring across your cloud and on-premises environments: asset discovery, vulnerability assessment, intrusion detection, endpoint detection and response, behavioral monitoring, SIEM log management, compliance reports and more.

Built for today's resource-limited IT teams, Clearnetwork SOC As A Service is affordable, fast to deploy (less than 1 hr), and requires no additional security expertise. It eliminates the need to deploy, integrate, and maintain expensive solutions like a SIEM and maximizes your existing security investments like your firewall and anti-virus by including their logs in our analysis. With no upfront costs or additional skill needed and consistent pricing, SOC As A Service offers low total cost of ownership (TCO) and flexible, scalable deployment options for organizations of any size or budget.

With Clearnetwork SOC As A Service, we focus on what matters most — protecting your IT infrastructure against today's emerging threats, safeguarding your reputation, minimizing risk and helping you meet compliance.

Multiple Essential Security Capabilities in a Single Managed Service

Clearnetwork SOC As A Service provides multiple essential security capabilities in a single managed solution, with everything needed for threat detection, incident response, and compliance management—all in a single pane of glass. With SOC As A Service, we do all the analysis and time-consuming security work, providing your team with actionable information and walking them through the response process. An elastic, cloud-based security solution, SOC As A Service can readily scale to meet your threat detection needs as your IT environment changes and grows.

CLIENT BENEFITS

- Unify visibility across your network, endpoints, applications and the cloud
- Full time Human SIEM analysis and correlation with machine learning
- Proactive Vulnerability Assessments and Asset Discovery minimize risk
- Reduce false positives and focus your time where it matters most
- Maximize ROI on existing security investments
- Eliminate the skills gap for hard to find security expertise
- Gain up-to-the-minute threat intelligence
- Actionable remediation steps with human guidance
- Customized reporting for PCI-DSS, HIPAA, NIST, SOX and many others

Asset Discovery

› API-powered asset discovery
› Network asset discovery
› Software and services discovery

Vulnerability Assessment

› Network vulnerability scanning
› Cloud vulnerability scanning
› Cloud infrastructure assessment

Intrusion Detection

› Cloud Intrusion Detection
› Host-based Intrusion Detection (HIDS)

Endpoint Detection and Response

› File integrity monitoring
› Continuous endpoint monitoring & proactive querying

Behavioral Monitoring

› Asset access logs
› Cloud access and activity logs (Azure Monitor, AWS: CloudTrail, CloudWatch, S3, ELB)
› AWS VPC Flow monitoring
› VMware ESXi access logs

SIEM & Log Management

› Event correlation
› Log management, with at least 12 months log retention
› Incident response

Key Product Features and Highlights

Security Monitoring for Your Cloud & On-Premises Environments

Clearnetwork SOC As A Service 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 SOC As A Service 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 (offices, 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 SOC As A Service 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 off connections between assets, users, and activities and the changes occurring between them

Skilled Security Analysts

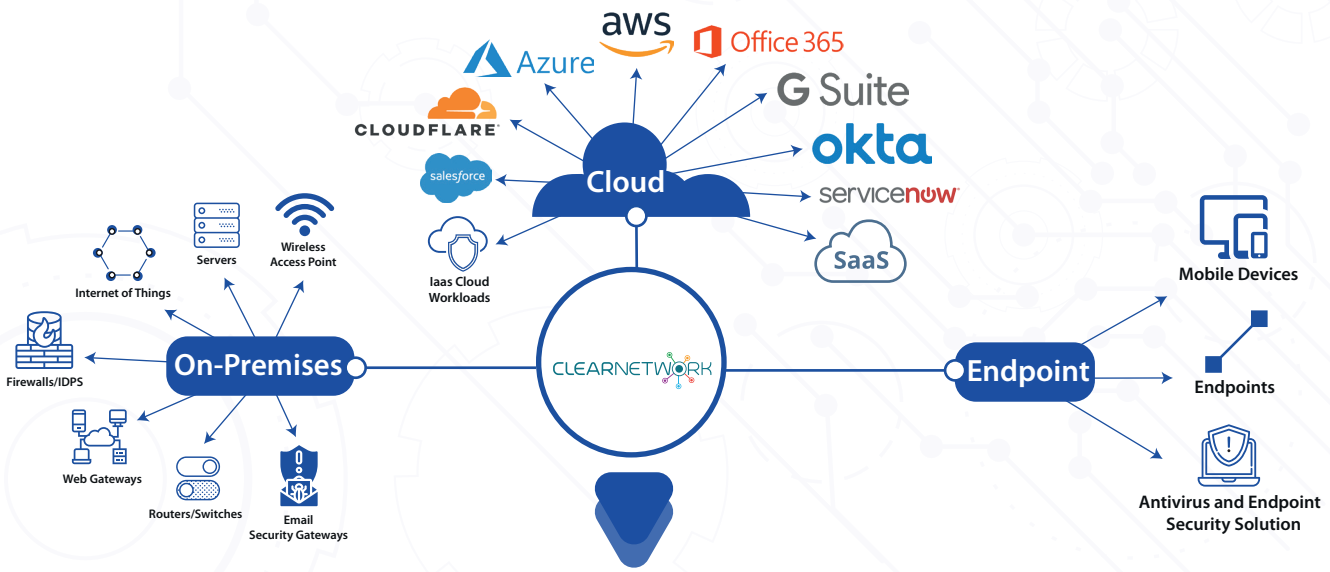
The lack of skilled security expertise on staff and the high cost to find and hire them due to the skill shortage has organizations scrambling. Clearnetwork SOC As A Service solves this issue by bringing you a fully managed service backed by security professionals with decades of combined experience. 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 SOC As A Service provides "audit ready" reports for PCI-DSS, HIPAA, NIST, ISO-27001, NERC-CIP, SOX, SOC2 and more!

Deploying Clearnetwork SOC As A Service is Fast and Easy

Clearnetwork SOC As A Service consists of a highly scalable, two-tier architecture to manage and monitor every aspect of your cloud and on-premises security. SOC As A Service Sensors and Agents collect and normalize data from your cloud and on-premises environments and securely transfers that data to SOC As A Service 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 SOC As A Service automatically. Install typically takes less than 1 hour.



Data Storage in SOC As A Service
Dedicated, Single-Tenant Data Store

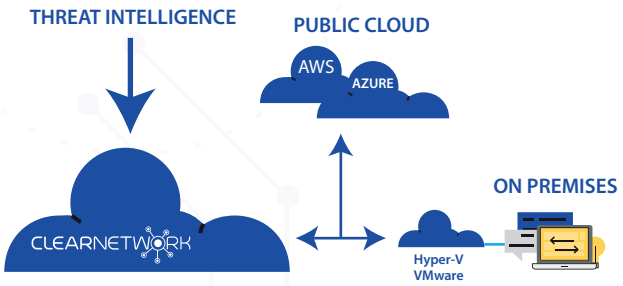
When you send sensitive security-related data to a security monitoring solution in the cloud, you want to ensure that your data is protected and leak-proof. That's why Clearnetwork uses a single-tenant data store architecture to securely manage all of our customers' accounts.
With SOC As A Service, your data is stored in its own dedicated container, which
is completely isolated from other customers' data. Whereas multi-tenancy is prone to data leakage and breakage that can affect multiple customer accounts, especially as SaaS providers scale, single-tenancy ensures that all customers' data is kept separate and leak-proof. It's a better architecture for you and for us.

Compliance-Ready Cold Storage

Clearnetwork SOC As A Service supports long-term log retention, known as "cold storage." By default, SOC As A Service enables 12 months of cold storage with the ability to extend your long-term storage capacity. In addition, SOC As A Service supports a "write once, read many" (WORM) approach to prevent log data from being modified. Logs can be readily requested for a specific date range from within SOC As A Service as needed.

Integrated Threat Intelligence for the Best Protection

Clearnetwork SOC As A Service receives continuous threat intelligence updates both internally and from multiple high-end sources. These dedicated teams spend countless hours researching and analyzing the different types of attacks, emerging threats, vulnerabilities, and exploits —so you don't have to.



Immediate Scalability.

SOC As A Service scales with your business needs. You can add or remove software Sensors and Agents, bring on additional cloud services, and scale central log management as your business needs change. The SOC As A Service pricing is based on the monthly data ingestion capacity. All the essential security capabilities are included in the service and scale

› Maximum raw data ingestion per month subscription
› Subscription tiers for all environment sizes starting at 250GB per month
› Support and maintenance included
› Threat Intelligence included
› 12 months of cold storage included, with the ability to extend your storage capacity

SOC As A Service Sensors and Agent

Our Agent is a lightweight, adaptable endpoint agent based on osquery that extends the powerful threat detection capabilities of SOC As A Service to the endpoint. It enables endpoint detection and response (EDR), file integrity monitoring (FIM), and rich endpoint telemetry capabilities that are essential for complete and effective threat detection, response, and compliance. You can deploy our Agent on your Windows and Linux endpoints in the cloud, on premises, and remote.
Clearnetwork SOC As A Service Sensors give you deep security visibility into your cloud and on-premises environments. The sensors conduct scans, monitor packets on the networks, and collect logs from assets, the host hypervisor, and cloud environments. This data is normalized and securely sent to SOC As A Service for analysis and correlation.

SENSOR TYPE	SYSTEM REQUIREMENTS
AWS Sensor	t2.large instance in Amazon VPC or m3.large instance in EC2-Classic 12 GB EBS volume for short-term storage as data is processed
Azure Sensor	D2 Standard or DS2 Standard 12 GB Data volume
VMware Sensor	Total Cores: 4
Ram:	12 GB of memory dedicated to VMware
Storage:	100 GB data device and 50 GB root device (150 GB total) VMware ESXi 5.1 or later
Hyper-V Sensor	Total Cores: 4
Ram:	12 GB of memory dedicated to the Hyper-V virtual machine
Storage:	100 GB data device and 50 GB root device (150 GB total) 2012 R2 OS with Hyper-V Manager or System Center Virtual Manager (SCVMM) 2012

SENSOR PERFORMANCE	
IDS Throughput (Mbps)	600

1 In each environment listed above, internet connectivity to your SOC As A Service instance is required.
2 Actual sensor performance may vary depending on environment, configuration, etc.
3 IDS throughput relates to on-premises network-based IDS. It applies to the VMware and Hyper-V sensor types only.

Additional sensors can be added to your Clearnetwork SOC As A Service install easily, just speak with our team.

CLEARNETWORK

Ready to experience Clearnetwork SOCaas?

Why not take it for a test drive on a Free 14-day Proof of Concept?

Email us at sales@clearnetwork.com
Or
give us a call at 800-463-7920 x3