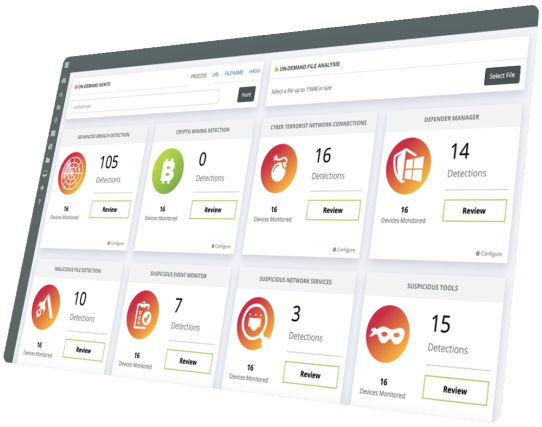
ES Cyber Security

MANAGED SOC

24x7 Threat Monitoring

Stop attackers in their tracks with our managed cybersecurity detection and response solution backed by a world-class security operations center.



Complete Managed Security for Today's Threats

ENDPOINT SECURITY

Windows & macOS event log monitoring, advanced breach detection, malicious files and processes, threat hunting, intrusion detection, 3rd party NGAV integrations and more.

NETWORK SECURITY

Firewall and edge device log monitoring integrated with real-time threat reputation, DNS information and malicious connection alerting.

CLOUD SECURITY

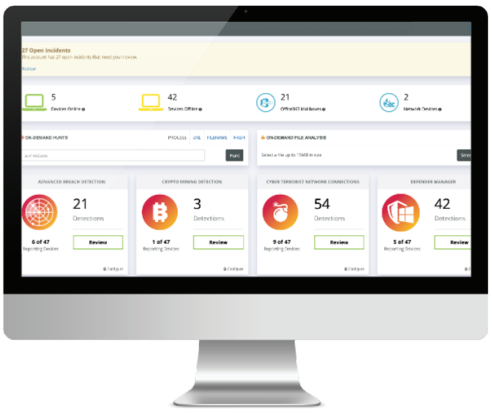
Secure the cloud with Microsoft 365 security event log monitoring, Azure AD monitoring, Microsoft 365 malicious logins and overall Secure Score.



24x7 Cyber Security Powered by Experts

Managed SOC (security operation center) is a managed service that leverages our Threat Monitoring Platform to detect malicious and suspicious activity across three critical attack vectors: Endpoint | Network | Cloud. Our elite team of security veterans hunt, triage and work with your team when actionable threats are discovered including:

- **Continuous Monitoring** – Around the clock protection with real-time threat detection
- **World Class Security Stack** – 100% purpose-built platform backed by over 50 years of security experience
- **Breach Detection** – The most advanced detection with to catch attacks that evade traditional defenses
- **Threat Hunting** – Elite security team proactively hunt for malicious activity
- **No Hardware Required** – Patent pending cloud-based technology eliminates the need for on-prem hardware



Managed SOC Key Features

The most comprehensive set of features means you can focus you're your business while our team of security experts ensures the you have the most advanced protection leveraging your existing tools and technologies across endpoint, network and cloud.

SIEMLESS LOG MONITORING

Monitor, search, alert and report on the 3 attack pillars: network, cloud and endpoint log data spanning Windows and macOS, Firewalls and Network Devices, Microsoft 365 & Azure AD without requiring SIEM hardware.

THREAT INTELLIGENCE & HUNTING

Real-time threat intelligence monitoring, connecting to premium intel feed partners giving our customers the largest global repository of threat indicators for our SOC analysts to hunt down attackers.

BREACH DETECTION

Detect adversaries that evade traditional cyber defenses such as Firewalls and AV. Identifies attacker TTPs and aligns with Mitre Attack, producing a forensic timeline of chronological events to deter the intruder before a breach occurs.

INTRUSION MONITORING

Real-time monitoring of malicious and suspicious activity, identifying indicators such as connections to terrorist nations, unauthorized TCP/UDP services, backdoor connections to C2 servers, lateral movements and privilege escalation.

NEXTGEN MALWARE

Use your own malware prevention or leverage our command and control app for Microsoft Defender backed up with a secondary line of defense using our malicious detection of files, tools, processes and more.

PSA TICKETING

Our SOC analysts investigate each alert, triaging the data and produce a ticket to your PSA system accompanied with the remedy details so you can focus on your operations without hiring security additional engineers.

Security App Store

Get more by monitoring your existing tools 24/7 and with our App Store turn on just the monitoring you want with over 35 cybersecurity Apps across the most popular products including:

- AV/AM Monitoring with SentinelOne, Cylance, Webroot, BitDefender, Windows Defender, Sophos and Deep Instinct.
- Firewall Analyzer & Monitoring with Fortinet, WatchGuard, SonicWall, Sophus, Barracuda, Juniper, Cisco Meraki, PfSense, Untangle, and Ubiquiti.
- Email Monitoring & DNS Monitoring with Microsoft 365, IRONSCALES, Barracuda, DNSFilter and Cisco Umbrella.
- And much more…

