Flagship ITSentinel™ Managed Endpoint Security

ENHANCED ENDPOINT PROTECTION AND SECURITY OPERATIONS CENTER

FLAGSHIP
NETWORKS

100 Beard Sawmill Rd
Suite 340
Shelton, CT 06484

203.358.0800

FlagshipNetworks.com

203.358.0800

“ALWAYS-ON” ENDPOINT DEFENSE

Cyber criminals seek the easiest path to a payday, often targeting small and medium-sized organizations with high-value assets—but with limited security defenses. It’s critical to continuously monitor your endpoints, such as workstations, servers, laptops, etc., for detection of suspicious activity and have the means to automatically initiate response and containment measures.

The Challenge

Hackers are skilled at bypassing traditional perimeter and antivirus defenses on their way to vulnerable endpoints. Once a beachhead is established, they begin their lateral movement tactics towards crown jewel assets. Unfortunately, their malicious intent too often appears as ‘normal’ user activity, rendering organizations with limited detection tools, monitoring and the expertise to discern a real threat from ‘white noise’ at risk of a data breach—or becoming the next ransomware hostage.

The Solution

Limited defense tools? We’ve got you covered. Limited security expertise? We can help with that! Our "always-on" endpoint defense delivers enterprise-grade Endpoint Detection and Response (EDR), remediation, and the benefits of a dedicated 24x7 Security Operations Center (SOC).

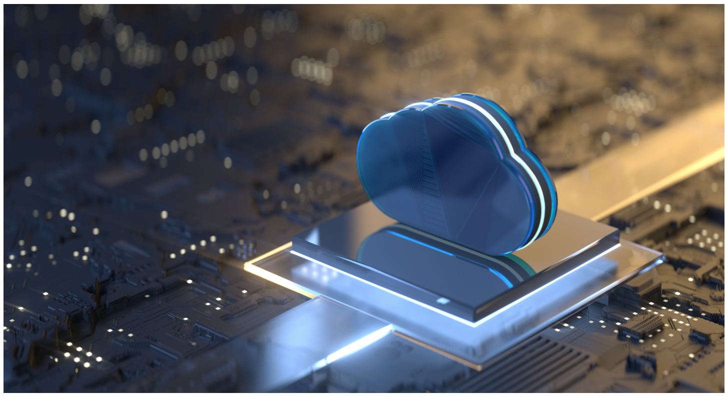
As a managed endpoint detection and response service, your environment is continuously monitored for thousands of virus and malware variants including multi-variant ransomware attacks and the latest crypto-mining infiltrations. Designed to rapidly identify the root cause of a threat and diagnose related corrupt source processes and system settings, when malicious behavior is detected immediate response and remediation measures are initiated on the endpoint including disconnect, quarantine, or roll back to an acceptable no-risk state. Threats are contained before they can do harm, and you stay operational.

Flagship Endpoint Defense Highlights

- Detect and remediate threats early in the threat lifecycle
- Strengthen the protection of critical assets
- Gain the expertise and coverage of a 24x7 SOC
- Remove the cost and complexity of solution deployment and management
- Focus on your running your business

ENHANCED DETECTION & RESPONSE

Flagship ITSentinel EDR (Enhanced Detection & Response) is a single autonomous agent combining End-Point Protection (EPP) and Advanced Detection and Response that is made for enterprises that need modern endpoint security and control with threat hunting capabilities. ITSentinel EDR is powered by SentinelOne®, which is used by the most discerning global enterprises for their unyielding cybersecurity demands.



ITSentinel EDR consolidates attack prevention, detection, response, and recovery into a single agent that protects Windows, Mac, and Linux. It works in real time with or without cloud connectivity to detect highly sophisticated malware, memory exploits, script misuse and other fileless attacks as they attempt to do damage, and adds visibility of all benign data.

The following are key EDR features.

- **Endpoint Prevention** to stop a wide range of malware, Trojans, hacking tools, and ransomware before they start
- **Active EDR Responds** at machine speed to autonomously contain damage
- **Active EDR Recovery** gets users up and running in minutes and includes remediation as well as rollback for Microsoft Windows
- **Device Control** for policy-based control of all USB device peripherals
- **Firewall Control** for policy-based control of network connectivity to and from assets, including location awareness
- **Vulnerability Management** and Application Inventory for insight into 3rd party apps that have known vulnerabilities mapped to the MITRE CVE database
- **Full Remote Shell** that provides for direct endpoint access by incident responders and forensics personnel
- **Deep Visibility Threat Hunting** for advance forensic mapping, visibility, and nuanced response capability for the enterprise SOC.
- **Advanced Enterprise Threat Hunting** automatically contextualizes all operating system events with S1's patented TrueContext™ function, saving analysts tedious event correlation tasks and getting to the root cause fast. Its ease-of-use is personified by the active nature of the solution in autonomously responding to attacks.

ITSENTINEL™ SECURITY OPERATIONS CENTER

Keeping pace with the daily grind of monitoring your client environments for attacks-in-motion can burnout the best of staff. As the alerts build and response is stretched thin, the protection you rely upon becomes vulnerable to failure.

The Flagship ITSentinel™ Security Operations Center (SOC) is here to help! Flagship leverages the ConnectWise® SOC as an extension of our team. Collectively, we provide certified security analysts, cutting-edge threat intelligence, and the latest solutions to manage all your security monitoring, 24/7/365.

The SOC staff understand the different types of cyber-attacks, and continuously work to understand malicious actors' attack methods and the vulnerabilities they seek to exploit. They leverage their deep cyber expertise to detect, respond and defeat a variety of threats ongoing–ensuring defense in depth across a diverse threat landscape. Your business will be more secure and better able to scale and grow.

Complete SOC Services Without the Need for In-House Expertise

24/7/365 Threat Monitoring and Response

Cybercriminals don't work normal hours. Attacks can hit at any time, and the ConnectWise SOC is ready when the time comes. We're continuously monitoring, detecting, and remediating threats to keep your clients secure. The ConnectWise SOC augments ConnectWise MDR™ (EDR), ConnectWise SaaS Security, and ConnectWise SIEM.

Fully Staffed Team of Security Experts

The ConnectWise SOC team includes certified security techs, including security analysts, incident response analysts, security researchers, and threat hunters. Do you already have a few security techs on staff? Our team will take care of alerting and triaging and consult your team when there are issues that they need to handle.

Cutting-edge Security Intelligence

The threat landscape is always changing. We leverage the ConnectWise Cyber Research

Unit to identify the latest threats, ensuring the SOC team is on high alert to catch what's lurking in the shadows.

Scale Your Business Securely

It's hard, and expensive, to build out a security team, let alone a fully staffed, 24/7 in-house SOC. We'll jump in when it comes to keeping your clients secure and take recruiting, hiring, and retaining security operations staff off your already full plate.

Quick On-boarding & Customization

As part of the Flagship ITSentinel SOC on-boarding process, we work with you collaboratively to ensure you are up and running quickly and tuning your tools and alerts based on your customers' unique requirements. This level of customization provides for adaptability as computing environments and client use cases change over time—a process we constantly review with you for maximum security optimization.

We deliver everything you need for comprehensive threat detection and analysis, including intrusion detection, threat intelligence, log storage with configurable retention, and managed SOC services. By removing the necessity of having multiple security products and the related costs and complexity, you gain a stronger security and compliance posture, and ease of operation.

The result: You're free to focus on what you do best – run your business!

NOTE: Flagship ITSentinel EDR is also available as a co-managed or SaaS offering without the Security Operations Center.

FLAGSHIP
NETWORKS

100 Beard Sawmill Rd
Suite 340
Shelton, CT 06484

203.358.0800

FlagshipNetworks.com