Flagship ITSentinel® Secure

FLAGSHIP NETWORKS' CORE SECURITY PLATFORM

FLAGSHIP NETWORKS

100 Beard Sawmill Rd
Suite 340
Shelton, CT 06484

203.358.0800

FlagshipNetworks.com

ESSENTIAL CYBERPROTECTION

Businesses and institutions must protect themselves from so many cybersecurity threats these days. You need to protect your data, your business processes, and your IP. It feels like there is news of a new threat each week, and so many solutions on the market to address them. Business and institution leaders just want to know, "What are the essential security tools I need to protect my organization?"

Flagship Networks ITSentinel® Secure platform provides that protection with a suite of tools that offer a mix of **prevention**, **detection**, **remediation** and **education**. Only a mix of security measures can secure your assets against today's threats and ever-changing attack vectors.

If you are concerned about maintaining high security while staying within budget, our ITSentinel™ Secure platform services will enable you to do just that. As a full-service IT provider these solutions enable us to provide you with 24/7 threat detection monitoring, incident response and risk assessment in a flexible, integrated solutions that are available as **fully managed services**, **co-managed** or **SaaS** offerings.

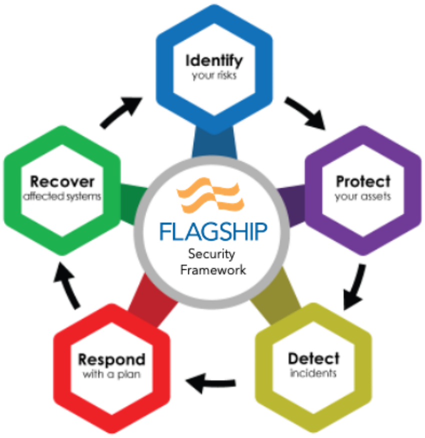
COMPREHENSIVE & EXTENSIBLE

ITSentinel Secure bundles together services that allow for multiple best-in-class security services licensed for one affordable monthly or yearly price – whichever best suits your operational model. The ITSentinel Secure platform is:

- **Best of Breed:** We've consolidated the best solutions for small and medium businesses.
- **Comprehensive:** It provides the essential coverage that every business needs.
- **Flexible:** It enables us to change the underlying elements as new products and updates emerge in the market.
- **Extensible:** Flagship has selected options to address special needs or additional protection for organizations that require them.

SUPPORTS FLAGSHIP SECURITY FRAMEWORKS

ITSentinel Secure® protects your organization by employing our Flagship Security Framework to each point of your business's exposure to cyber risk. Our framework is based on the National Institute of Standards and Technology (NIST) Cyber Security Framework. Its functions represent a comprehensive security lifecycle in which each function plays an essential role in defining controls, processes and technologies to fulfill each of five core function in the security lifecycle:



- **Identify** pinpoints all the systems and platforms in the company's infrastructure that may be a security risk.
- **Protect** implements appropriate safeguards to ensure the delivery of critical services.
- **Detect** enables timely discovery of cybersecurity events.
- **Respond** implements the appropriate activities when facing a detected security event.
- **Recover** implements the appropriate activities for resilience and restoring any capabilities or services that were impaired due to a security event.

Each function is essential to good security posture and successful management of cybersecurity risk. This is a lifecycle, or process, that never ends. It is very important for a security process to constantly develop, self-evaluate and adjust because attackers are constantly evolving their tactics as well.

ENSURES THAT YOU ARE COVERED

The ITSentinel Secure Platform is comprised of best-of-breed products that address your primary exposure to cyberattacks. The solutions will identify, protect, detect, respond and recover across your business's end users, infrastructure endpoints, servers and web domain.

	ITSentinel® Secure Solutions
End Users	Managed Detection & Response for Office 365 Advanced Email Protection – Phishing Security Awareness Training Office 365 backup
Endpoints	Managed Detection & Response/Security Operations Center (MDP/SOC) Managed Breach Detection Secure Web Gateway
Servers	Managed Detection & Response - Security Operations Center (SOC) Managed Breach Detection Zero Trust Endpoint Protection - Servers Windows login/Admin login Protection
Domain	Dark Web Monitoring

ITSENTINEL® SECURE SOLUTIONS

ITSentinel MDR for Microsoft 365

ITSentinel MDR for Microsoft 365, powered by Huntress Labs, is specifically designed to mitigate risks within Microsoft 365 environments. This offering enhances protection against costly business email compromise (BEC) and account takeover attacks. Huntress MDR for Microsoft 365 offers proactive, real-time threat monitoring, identity protection, and expert analysis to enhance security. Threat experts in the Huntress Security Operations Center vigilantly watch for suspicious activities, such as unusual login patterns, signs of email tampering, and attempts at privilege escalation. By identifying threats in real time, swift response is enabled to prevent account takeovers and other security breaches.

To protect against identify compromise, MDR for Microsoft 365 offers one-click fixes and, if necessary, automated account lockdown. The incident reports provided by Huntress SOC are actionable and straightforward. This approach ensures efficient incident resolution and minimizes the impact of security threats.

ITSentinel Security Awareness Training

ITSentinel Security Awareness Training, powered by BullPhish ID, is a comprehensive security awareness training and phishing simulation solution designed for businesses. With its unified approach, Security Awareness Training empowers organizations by turning their workforce into a proactive line of defense against phishing attacks, data breaches, and financial losses. By combining education, testing, and customization, it equips employees with the knowledge and skills needed to safeguard sensitive information and maintain a strong security posture.

ITSentinel Security Awareness Training also streamlines email campaign management with automated import, advanced scheduling, and randomization features. Users can quickly import organizations, groups, and contacts for phishing simulation and training campaigns. Campaigns can be scheduled up to a year in advance. Send times and phishing messages are randomized, making the simulations more realistic and effective in preparing employees to recognize and respond to actual threats.

ITSentinel Advanced Email Protection

ITSentinel Advanced Email Protection, powered by Inky, is a robust solution designed to protect against email threats, prevent data leaks, and guide users in making safe decisions. ITSentinel Advanced Email Protection leverages cutting-edge technologies like computer vision, AI, and machine learning to stay ahead of evolving threats. It uses Behavioral Email Security to analyze email behavior, flag suspicious emails, and guide users toward safe actions.

ITSentinel Office 365 Backup

ITSentinel Office 365 Backup, powered by Cove, is a comprehensive data protection solution designed to safeguard critical information stored in Microsoft 365. It ensures that your Microsoft 365 data remains secure, recoverable, and efficiently managed through its unified interface and cloud-centric approach. Its Unified Dashboard Backup offers a single, centralized dashboard for managing Microsoft 365 backups and recoveries, so you can efficiently handle data protection for Microsoft 365 alongside other critical systems, streamlining administrative tasks. Office 365 Backup protects essential data from Microsoft Exchange, OneDrive, SharePoint, and Teams.

Office 365 Backup embraces a cloud-first strategy, leveraging the power of cloud computing. It offers streamlined backup, disaster recovery, and archiving while reducing complexity and cost. By prioritizing the cloud, ITSentinel Office 365 Backup maintains speed, reliability, and scalability for your data protection needs.

ITSentinel Secure Web Gateway

ITSentinel Secure Web Gateway, powered by DNSFilter is a cloud-based, AI-driven content filtering and threat protection service to securing networks and ensuring safe browsing for all users. It employs advanced algorithms and machine learning to identify and block malicious websites, preventing threats such as malware, ransomware, and phishing attacks. It can be deployed and configured in minutes without requiring any software installation.

ITSentinel Secure Web Gateway follows a zero-trust approach. It actively evaluates each domain and categorizes it based upon risk. If a website is flagged as potentially dangerous, this service blocks access to it, reducing the chances of accidental exposure to harmful content.

ITSentinel Managed Detection & Response with SOC

ITSentinel Managed Detection & Response with SOC (MDR/SOC), powered by SentinelOne Complete and ConnectWise Security Operations Center, is an advanced security solution that provides comprehensive protection for endpoints, cloud environments, and identity systems. Its role is critical in today's interconnected digital landscape. It acts as the first line of defense against cyber threats, providing real-time, 24/7 monitoring, incident response, and proactive security measures. MDR/SOC reduces complexity and ensures organizations can respond effectively to cyber threats.

ITSentinel MDR/SOC employs a single agent that covers multiple security aspects, including automated prevention, detection, response, and threat hunting. It also provides protection for various surfaces, such as endpoints, cloud environments, and identity systems.

ITSentinel MDR/SOC utilizes patented Storyline™ technology, which automatically tracks relationships within operating systems in real time during attacks. This efficient hypothesis testing helps them reach rapid conclusions. With Enhanced Incident Response, it assists in making informed decisions during security incidents.

Incident response remediation is simplified with one-click remediation. It can reverse unauthorized changes without manual scripting. It also includes a Hunter's Toolkit, which offers features like historical EDR data retention, customizable network isolation, and enhanced visibility.

ITSentinel Zero Trust Endpoint

ITSentinel Zero Trust Endpoint, powered by ThreatLocker, is an endpoint protection platform (EPP) designed to safeguard businesses against zero-day attacks, such as malware, ransomware, and other threats that can compromise system integrity. It operates with a Zero Trust posture, employing a default deny approach to minimize the attack surface and mitigate potential cyber vulnerabilities. it doesn't automatically trust any application or process – it verifies and authorizes each one before allowing execution. This capability is combined with stringent endpoint protection and streamlined management to enhance cybersecurity defenses for businesses.

ITSentinel Managed Breach Detection

ITSentinel Managed Breach Detection, powered by Huntress Labs, offers a comprehensive Managed Security Platform that includes Endpoint Detection and Response (EDR) for unparalleled visibility and a 24x7 Security Operations Center (SOC) ensures that businesses can act promptly to mitigate risks.

EDR continuously monitors endpoints for malicious activity. When threats are detected, it generates incident reports, allowing swift response and proactive remediation by the Security Operations Center. Managed Breach Detection provides near real-time endpoint detection and response.

ITSentinel DUO Windows Authentication

Duo Authentication for Windows Logon is a security solution that seamlessly integrates with Microsoft Windows client and server operating systems. It adds two-factor authentication to various Windows logon scenarios, enhancing security for both local and remote access. Even if primary credentials are compromised, the secondary authentication step helps prevent unauthorized access. Duo Authentication for Windows Logon strikes a balance between security and user convenience, enhancing protection while maintaining usability. Whether users log in via the local console or RDP, Duo ensures robust authentication.

ITSentinel Dark Web Monitoring

ITSentinel Dark Web Monitoring, powered by Dark Web ID, is a comprehensive solution designed for IT professionals. It provides continuous monitoring of business and personal credentials on the dark web, helping organizations identify compromised data and mitigate security risks. Using Credential Monitoring, it continuously scans the dark web for exposed credentials, including email addresses, passwords, and other sensitive information. It detects compromised data from various sources such as dark web markets, data dumps, and forums.

Dark Web Monitoring provides 24x7 protection with a combination of human and machine-powered monitoring. It alerts organizations promptly when compromised credentials are detected, allowing them to take proactive measures before cybercriminals exploit the data.

FLAGSHIP
NETWORKS

100 Beard Sawmill Rd
Suite 340
Shelton, CT 06484

203.358.0800

FlagshipNetworks.com