FM Secure

Multi-layered, proactive approach to cybersecurity

What is it?

FM Secure is our complete range of cybersecurity services designed to keep your organization and its data safe. We take the very best security solutions available, combine them with our in-house IT experts and best-practices to deliver a multi-layered, proactive plan designed to keep your company protected from malicious activity.

Anti-virus is not enough

With today's rapidly-changing landscape of cybercriminal activity, most organizations struggle to keep up. Unfortunately, it's not a matter of **if** you will experience an attack, it's **when**.

Traditional anti-virus software is no longer enough to protect against threats like ransomware and malvertising, and the latest phishing schemes are becoming more and more difficult to distinguish from real emails. A well-rounded, managed approach is needed to make sure your organization and your team are prepared and can minimize vulnerabilities and risk.

FM Secure includes:

- Available Network Security Audits (Vulnerability Scanning & HIPAA Risk Analysis)
- Managed SIEM (Security Information & Event Management)
- DNS Internet Security
- Endpoint Security
- Cloud-to-Cloud Backup & Continuity
- Complete Email Security Service
- Multi-Factor Authentication
- End-User Security and Phishing Training

Feature	What these features mean to you	Components	Essentials	Complete
Network security audit	A site audit and deep network scan to highlight potential risk areas resulting in a detailed report pointing to areas of concern. Offers practical and policy-related solutions for tightening up security and data backup	Vulnerability scanning	Optional	✓
		HIPAA risk analysis scanning	Optional	Optional
DNS internet security	FM perimeter protection service enables DNS-layer security and interactive threat intelligence to block domains associated with phishing, malware, botnets and other high risk categories. Users are protected both within the corporate network as well as working remotely through a single cloud service gateway.	Network perimeter security	✓	✓
		Roaming device security	✓	✓
Endpoint security	Advanced endpoint security keeps your organization ahead of threat actors with AI-driven security algorithms that provide best-in-class detection, prevention, and response capabilities.	Endpoint security	✓	✓
Cloud protection (continuity)	Cloud-to-Cloud Backup provides comprehensive and scalable protection for your Office 365 data. It automatically and securely backs up your email, contacts, folders, schedules, and tasks, along with your OneDrive for Business, SharePoint, Groups, and Teams data. This can be combined with Cloud Archiving where data is backed up outside of your operational email environment in a dedicated tamper-proof repository, ensuring it will be retained securely for as long as your need it without risk of corruption or deletion. (Cloud archiving can be required for certain industries/ compliance requirements)	Cloud-to-Cloud Backup	Optional	✓
		Cloud Archiving	Optional	✓
Email security service	FM's Email Security Service sanitizes every email before it is delivered to your mail server to protect you from email-borne threats. Using virus scanning, spam scoring, real-time intent analysis, URL link protection, reputation checks, and other techniques, this solution provides you with maximum protection. Anti-Phishing is a service that uses artificial intelligence (AI) to detect signs of malicious intent and deception.	Email security with advanced detection	✓	✓
		Anti-spear phishing	✓	✓
Managed SIEM (security information and event management)	Managed SIEM is a proactive step to protect your environment from security breaches, while meeting compliancy requirements. Managed SIEM collects operational logs from various computers, applications, devices throughout the network and from SaaS services, and correlates the data using machine intelligence to differentiate between suspicious and normal activity. If suspicious activity is identified, the SIEM solution alerts Fully Managed so the team can handle the issue.	Managed SIEM	Optional	Optional
Multi-Factor Authentication	Additional layer of security requiring multiple sources of verification. Secure, mobile authentication application for quick, push notification-based approval to verify your identity via a smartphone, smartwatch or U2F token support.	Multi-Factor Authentication	Optional	✓
Security training	End-user cybersecurity awareness training against the most pervasive threats, including Phishing and Ransomware, which target users to breach your security defenses.	End-user security training modules	✓	✓