



Systems Integration, Inc.
Business Needs. Technology Solutions.

Comprehensive IT Security Solutions

Multi-Layered IT Security Solutions to Protect Your Business

As the unrivaled leader in delivering cutting-edge IT solutions and managed services to small-to-medium businesses throughout southern New England, we leverage our unmatched expertise to navigate every IT issue imaginable. Our priority is delivering the highest quality service. We achieve this by becoming our clients' strategic partners, integrating with their IT teams, and collaborating with senior management to align with business and financial goals.

We excel in managing diverse IT systems and applications, enabling cohesive and efficient operations. Our tailored approach is designed to understand and meet each client's unique needs, ensuring swift resolution of networking and technology issues and providing enterprise-level solutions.

Our security solutions are unmatched whether you have a traditional, cloud, or hybrid network. We use a proactive, multi-layered approach to security management, utilizing the comprehensive National Institute of Standards and Technology (NIST) and Center for Internet Security (CIS) standards and guidelines as a basis for developing, implementing, and maintaining cybersecurity policies, procedures, and controls for our clients' systems and data.



Key Features of Our Security Solutions

1. 24/7 Managed Detection and Response (MDR)

- Real-time monitoring and threat detection across your entire IT infrastructure.
- Automated and human-led incident response to mitigate attacks quickly.
- Advanced threat intelligence integration for proactive protection.

2. Endpoint Detection and Response (EDR)

- AI-driven behavioral analysis to detect, block, and remediate endpoint threats.
- Continuous monitoring of devices (computers, mobile devices, servers) to identify malicious activity.
- Automated incident response and rollback features to reduce downtime.

3. Security Information and Event Management (SIEM)

- Centralized logging and real-time correlation of security events from all network devices, servers, and applications.
- Automated threat detection and response using advanced machine learning.
- Compliance reporting for frameworks like CMMC, HIPAA, and GDPR.

4. Firewall and Network Security

- Managed firewall services to prevent unauthorized access and filter malicious traffic.
- Intrusion detection and prevention systems (IDS/IPS) to monitor and block threats.
- Virtual Private Network (VPN) management for secure remote access.

5. Cloud Security

- Comprehensive security for multi-cloud and hybrid environments.
- Data encryption, secure access, and cloud threat monitoring.
- Continuous security posture management for platforms like Microsoft Azure, AWS, and Google Cloud.

6. Identity and Access Management (IAM)

- Multi-Factor Authentication (MFA) and Single Sign-On (SSO) to secure user access.
- Role-based access control (RBAC) to ensure users only access necessary resources.
- Privileged Access Management (PAM) for managing administrative access to sensitive systems.

7. Email Security and Phishing Protection

- Advanced email filtering to block phishing attempts, spam, and malware.
- Anti-phishing training and testing for employees to reduce human error risks.
- Email encryption to ensure secure communication.

8. Data Loss Prevention (DLP)

- Continuous monitoring and control of sensitive data to prevent unauthorized sharing.
- Data classification and encryption to protect critical business information.
- Automated policy enforcement to comply with industry regulations.

9. Security Awareness Training

- Regular employee training programs on security best practices and phishing awareness.
- Customizable training modules tailored to your organization's needs.
- Simulated phishing campaigns to identify and improve user vulnerabilities.

10. Vulnerability Management and Patch Management

- Continuous scanning and identification of vulnerabilities across systems and applications.
- Regular patch management to ensure all software and firmware are up-to-date.
- Detailed vulnerability reports and remediation recommendations.

11. Incident Response and Forensics

- Rapid incident response services to contain and mitigate security breaches.
- Post-incident analysis and digital forensics to identify root causes and reduce future risks.
- Detailed incident reports and guidance on recovery processes.

Benefits

Proactive Threat Protection

Our solutions use advanced threat intelligence and machine learning to proactively detect and mitigate threats before they impact your business.

24/7 Security Monitoring

Round-the-clock monitoring ensures your systems are continuously protected, even during off-hours, providing you peace of mind.

Customizable Solutions

Tailored IT security services to meet your specific business needs, regardless of size or industry.

Expert Support

Our team of certified security professionals provides expert management and support, including regular consultations and compliance advice.

Compliance Assurance

Ensure your business meets regulatory requirements, such as CMMC, HIPAA, GDPR, and SOC 2, through our built-in compliance tools and reporting.

Cost-Effective Protection

Access enterprise-grade security tools and services without the need for heavy in-house investment.

Who Can Benefit from Our IT Security Solutions?



Small and Medium-Sized Businesses (SMBs) Secure your business without needing a large in-house IT team.



Enterprise Clients Leverage scalable, robust security solutions tailored to your complex infrastructure.



Regulated Industries Healthcare, finance, legal, and government organizations can rely on our compliance-focused security services.

Additional Services

Backup and Disaster Recovery (BCDR)

Fully managed backup and recovery solutions to ensure business continuity in the event of data loss or ransomware.

Security Audits and Risk Assessments

Comprehensive security audits and risk assessments to identify vulnerabilities and optimize your security posture.

Virtual Chief Information Security Officer (vCISO) Consulting

Strategic security guidance and planning through our vCISO services to align your security strategy with business goals.

To learn more or request a consultation on how SII can secure your network from attack, reach out to us at **860-513-0100**, **info@sys-int.com**, or **sys-int.com**

