

Managed IT Solutions

SentinelOne® + Vigilance Cyber Security Platform

CM3 Building Solutions provides experienced managed Information Technology solutions for your business or facility. We curate the industry's leading products and services to bring the best thinking to every project, and we custom build solutions that fit your business and budget.

We are a proud provider of SentinelOne® + Vigilance, an industry-leading, AI-powered, cloud-based solution.

SentinelOne + Vigilance is redefining cybersecurity by pushing the boundaries of autonomous technology. With AI-powered prevention, detection, response, and threat hunting across user endpoints, containers, cloud workloads, and IoT devices, SentinelOne + Vigilance defends faster, at greater scale, and with higher accuracy across the entire attack surface.



AI-Powered Cyber Security

Built-in Static AI and Behavioral AI analysis prevent and detect a wide range of attacks in real time before they cause damage. Protects against known and unknown malware, Trojans, hacking tools, ransomware, memory exploits, script misuse, bad macros, and more.

Sentinels are autonomous which means they apply prevention and detection technology with or without cloud connectivity and will trigger protective responses in real time.

Recovery is fast and gets users back and working in minutes without re-imaging and without writing scripts. Any unauthorized changes that occur during an attack can be reversed with 1-Click Remediation and 1-Click Rollback for Windows.

Secure SaaS management access Choose from US, EU, APAC localities. Data-driven dashboards, policy management by site and group, incident analysis with MITRE ATT&CK integration, and more.

Firewall Control for control of network connectivity to and from devices including location awareness.

Device Control for control of USB devices and Bluetooth/BLE peripherals.

Rogue visibility to uncover devices on the network that need Sentinel agent protection.











Vulnerability Management, in addition to Application Inventory, for insight into 3rd party apps that have known vulnerabilities mapped to the MITRE CVE database.

Industry Leaders Rely on SentinelOne®



How Vigilance Works

- **Threat Detected**
AI queuing mechanisms prioritize threats
- **Analyst Deep Dive**
Threats are classified by AI/ML, Intel, ActiveEDR+ Storyline, MITRE® TTPs, logs, analyst's judgement
- **Threat Insight**
All console incidents are interpreted and annotated to keep you in the loop
- **Action & Next Steps**
Vigilance mitigates and resolves threats for you and opens proactive escalation as needed

Vigilance	
	24x7x365 Follow-the-sun
	Proactive notifications
	Incident Research
	Event Prioritization
	Fewer Alerts, More Context
	Malware Analysis as Needed
	Accelerated Response Time
	Clean Dashboards
	Executive Reporting
	Mitigation and Containment
	False Positive Reduction

Security Operations	Endpoint Security Capabilities
In-Product threat hunting	Autonomous Agent
Threat hunting API	Full behavioral attack remediation
Custom Detection Rulers	Static AI & Cloud Intelligence file-based attack prevention
Secure Remote Shell for Windows, macOS and Linux	Behavioral AI fileless attack detection
Threat Response/Kill for Windows, macOS and Linux	Agent Anti-Tampering
Threat Quarantine for Windows, macOS and Linux	OS Firewall control for Windows, macOS, and Linux
Remediation Response / 1-click, no scripting for Windows, macOS, and Linux	
Quarantine device from the network	
Incident Timeline	