Global Logistics Organization

Contained Ransomware Before Business Operations Were Disrupted

How SilverSky identified vulnerable medical devices, detected signs of active exploitation, and helped a healthcare provider reduce risk while maintaining critical patient services.

Operational Challenges

Ransomware Threats

Evolving attacks threatened critical business operations.

Operational Continuity

Business systems required uninterrupted availability.

Early Threat Detection

Rapid detection helped contain threats before they spread.

Lateral Movement Prevention

Identifying attacker movement reduced organizational risk.

Lean Security Team

Limited internal resources made 24×7 monitoring challenging.

Business Resilience

Stronger security was needed without disrupting daily operations.

Overview

During the deployment of SilverSky Lightning Managed Endpoint Detection & Response (MEDR), SilverSky identified active ransomware already present within a customer's environment. Indicators of compromise were detected before the malware could spread throughout the organization's network, creating an opportunity to contain the threat before it impacted critical business operations.

By immediately activating advanced endpoint protections, isolating compromised devices, and coordinating remediation efforts with the customer's IT team, SilverSky helped stop the attack in its early stages.

The incident demonstrated the value of continuous detection, rapid response, and expert-led security operations—helping the organization minimize operational disruption while strengthening its overall cyber resilience.

The Challenge

The customer was in the process of deploying SilverSky MEDR across its environment when ransomware indicators were detected on multiple endpoints.

While traditional antivirus had failed to identify the threat, SilverSky's behavioral analytics recognized malicious activity and alerted implementation engineers before widespread encryption occurred.

The SilverSky Response

SilverSky immediately transitioned endpoint protection from learning mode into an active defensive posture.

Compromised systems were quarantined, malicious communications were blocked, and incident response activities began immediately.

Although several devices not yet onboarded experienced encryption, deployment priorities ensured critical systems remained protected while remediation efforts restored the remaining endpoints.

The Outcome

Critical Infrastructure Protected

Business-critical systems remained operational throughout the incident.

Ransomware Contained

Rapid response prevented widespread encryption.

Improved Endpoint Security

Advanced endpoint protection replaced legacy antivirus capabilities.

Stronger Security Program

The customer developed a roadmap for continued security improvement.

Security Has To Be Operated.

Cybersecurity isn't defined by the tools an organization owns—it's defined by how effectively those tools are monitored, managed, and continuously improved. Every customer engagement reinforces SilverSky's commitment to operational security, helping organizations reduce risk, strengthen resilience, and respond confidently to evolving cyber threats.

When business operations depend on uptime, rapid response matters. SilverSky identified and helped contain ransomware activity early, minimizing operational disruption and strengthening the organization's resilience against future attacks.

Why It Mattered

Rapid detection and coordinated response often determine whether ransomware becomes a business interruption or a contained security event.

SilverSky's operational approach helped minimize business disruption while strengthening long-term resilience.

Talk to a Security Expert

See how SilverSky helps organizations detect ransomware earlier, accelerate incident response, and protect critical business operations through continuous monitoring and expert-led threat containment.

www.SilverSky.com | Learn@SilverSky.com