

Log & Event Manager Helps Blue Detect Suspicious VPN Attempts

“Rates Log & Event Manager 9/10, because of: “Great flexibility in event retrieval.”

On how Log & Event Manager helped identify and deal with a major security incident in the organization: “Multiple VPN attempts from different countries on the same day.”

Challenges

- For Blue, **user activity** is the most critical security area.
- Demonstrates and meets SOX compliance requirements with SolarWinds **Log & Event Manager**.

Use Case

- For Blue, the three most critical features that will help detect and respond to threats are:
 - Threat intelligence
 - Centralized real-time event detection, correlation & notifications
 - Anomaly detection

Results

With Log & Event Manager, Blue:

- Detects 11 – 50 security incidents, every month.
- Saved **\$100,001 – \$200,000** within the past 12 months.
- Their favorite Log & Event Manager feature is **in-depth search and log analysis**.
- Blue now feels more prepared to deal with *security and compliance issues* with Log & Event Manager

About SolarWinds Log & Event Manager

SolarWinds delivers powerful, affordable, and easy-to-use IT security tools to help you monitor, patch, and eliminate security threats and vulnerabilities across your network. Get fast and easy compliance reporting for HIPAA, PCI, SOX, ISO, and more.

Learn More:

[SolarWinds](#)

[SolarWinds Log & Event Manager](#)