

5 REASONS YOUR BUSINESS NEEDS A SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Today's threat landscape calls for intelligent, automated, real-time threat detection with integrated compliance tools.

1

HOLISTIC VISIBILITY

SIEM collects logs and generates security alerts from your entire network, including cloud resources and mobile devices, providing full visibility in one central location.

2

THREAT DETECTION

Imagine having to comb through hundreds, even thousands, of security alerts over the course of a day. There's actually a name for it. It's called "alert fatigue." A SIEM uses advanced analysis and cross-correlation to automatically filter out false alerts so real threats bubble to the surface.

3

FAST RESPONSE

The longer it takes to detect a threat, also called "discovery time," the more potential damage to your business.

A SIEM identifies real threats faster so your response team can act quickly before a breach occurs.

TOP TRENDS DRIVING SIEM DEMAND:

- Cyberattacks continually rising in frequency and sophistication
- Regulatory agencies stepping up compliance requirements
- Cybersecurity insurers calling for more advanced security technologies

4

COMPLIANCE AND AUDIT REQUIREMENTS

Businesses in healthcare, finance, accounting and government industries must meet stringent regulatory requirements. An effective SIEM is key to complying with PCI, HIPAA and FFIEC standards.

5

INSURANCE COVERAGE

SIEM can check all the boxes on today's stringent cybersecurity insurance applications. And once you get coverage, a SIEM can provide the detailed forensic analysis insurers require before they pay out in the event of security breach.



WE MAKE SIEM SIMPLE

We understand you may not be a security expert. Partner with security experts who make technology simple.

Finch Technical Solutions Ltd

01270 323777

<https://finch-ts.co.uk>

The Campus, Crewe Green Road

Crewe, Cheshire CW1 5DU