



# Zivaro Managed Security Information & Event Management

Navigating the constantly changing cybersecurity landscape has never been more challenging - or more critical. Because as networks grow, the attack surface expands, increasing our threat exposure. And more network complexity makes it more challenging than ever to see who - and what - is on your network.

We'll provide you with a safety net to catch the malicious activities that slip through traditional defenses.

Zivaro helps regulated market customers overcome security obstacles by designing, deploying, and managing best-of-breed, cloud-enabled security solutions - including SIEM. We have almost a decade of experience as a Splunk partner, and our Splunk Certified Architects use their expertise to deploy and provide continuous managed SIEM administration.

Zivaro's Managed SIEM solution, powered by Splunk Enterprise, gives you the advanced detection and investigation capabilities of a SIEM platform, so you don't need to hire a team of technical experts.

## KEY BENEFITS OF ZIVARO'S MANAGED SIEM SOLUTION:



Deployment, management, and administration of your Splunk SIEM platform



Tier-1 and Tier-2 cybersecurity incident response provided by our staff of certified cyber-analysts



Continuous refinement and optimization of your SIEM platform to ensure you're always protected

## More network complexity makes it harder than ever to see who and what is on your network

**90%**

of surveyed organizations aren't aware of devices accessing their networks

**40%**

of network/endpoint infrastructure can become unknown or unmanaged when an organization lacks visibility

**85%**

of cyberattack victims don't realize they've been attacked for weeks - or longer

**43%**

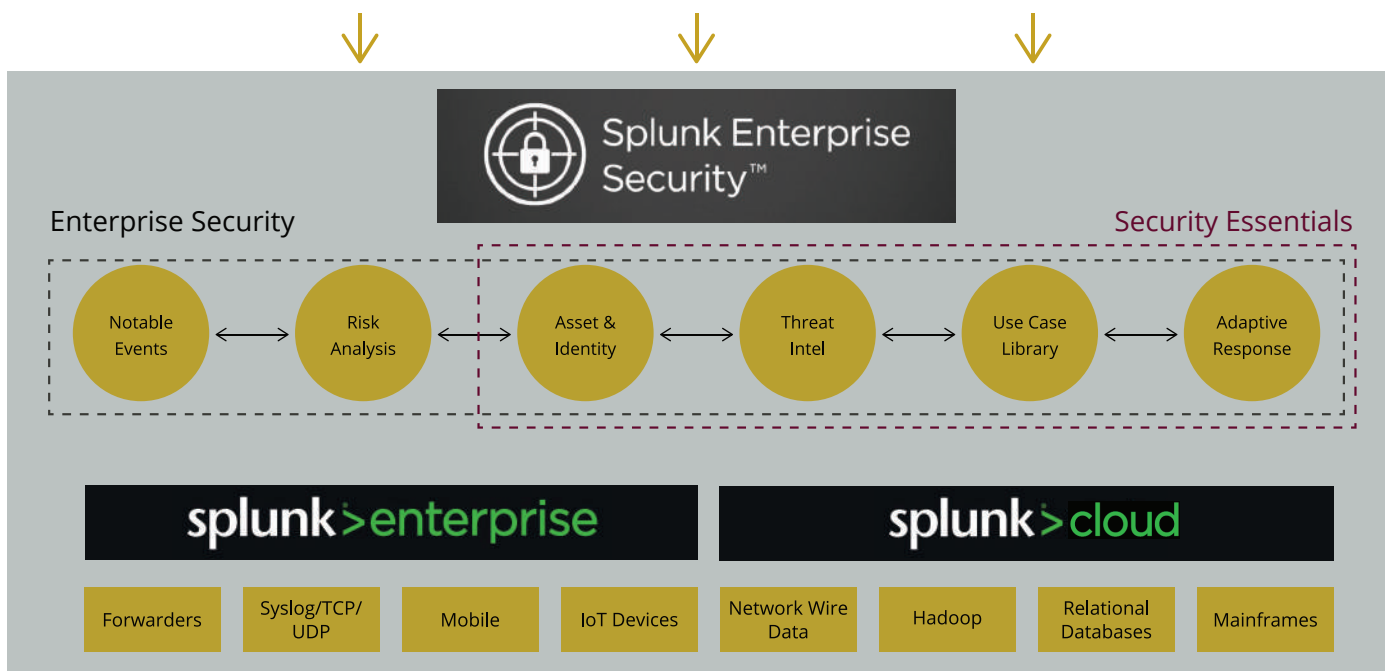
of cyberattacks target small businesses

**Don't unintentionally create silos. We'll bring real solutions and holistic awareness across your IT teams.**



# Zivaro Managed Security Information & Event Management

## Zivaro Managed SIEM Personnel



### SPLUNK SECURITY SUCCESS STORIES

- Security Operation Center (SOC) design and management for DOE agency, with machine data as the centerpiece for all use cases around Identity, Access, Posture, APT and forensics
- Design, deployment, and resident engineering services support for large aerospace services provider's SIEM platform, enabling centralized security services in support of governance, risk, and compliance controls
- Design, deployment, and training services for SIEM solution for F100 financial services subsidiary, enabling automation resulting in 95% of Tier 1 events never being touched by an analyst
- SIEM design, deployment, and annual use case enhancement services to enable real-time security monitoring and reporting for PCI DSS Level 1 Service Provider SaaS company
- Assessment, design, training, and SIEM implementation services for a cybersecurity software provider, making available a global security posture managed by geographically distributed teams on three continents
- Provided DOD client with network infrastructure and architecture design, cybersecurity RMF support, and advanced analytics for Missile Warning Center Operations Support
- SIEM design, implementation, and on-going support services for State Government entity, helping them gain security visibility and contextual awareness for their multi-terabyte deployment
- Core Splunk and Enterprise Security assessment, design, training, and implementation services for an energy company providing enhanced security posture awareness across both IT and OT teams



**CONTACT YOUR SERVICES ADVISOR**

877.603.1984

advisor@zivaro.com

