ziften
PARTNER

Ziften + Splunk

Real-Time Monitoring & Response

Accelerate the detection of threats and advanced attacks using Ziften for Splunk.

A Strategic Partnership

Love Splunk? So do we.

It's simple: We leverage Splunk's strength in Big Data Analytics to offer better protection, accelerate the detection of threats and advanced attacks, reduce investigation and response times, and decrease the time to mitigation and remediation.

The final outcome? A powerful and comprehensive approach to threat detection and response.

Customers can quickly coordinate across both their cloud and on-premise security ecosystems involving network security, endpoint security, identity, and threat intelligence products. Reducing investigation and response times, while decreasing the time to mitigation and remediation.

Native Integration

Ziften Makes Splunk Even Better.

Continuous endpoint visibility enables real-time detection and response, along with incident prevention

Sophisticated security analytics assess dynamic risk indicators to prioritize findings for security teams

Innovative and valuable intelligence span across both security and operational teams to enhance long-term value

Augment and enhance Splunk Enterprise and Splunk ES, with Ziften's CIM-compliant App and Technology Add-on

Increase security efficiency toward prevention, detection, and response to security threats at the endpoint, in a faster and more cost effective manner

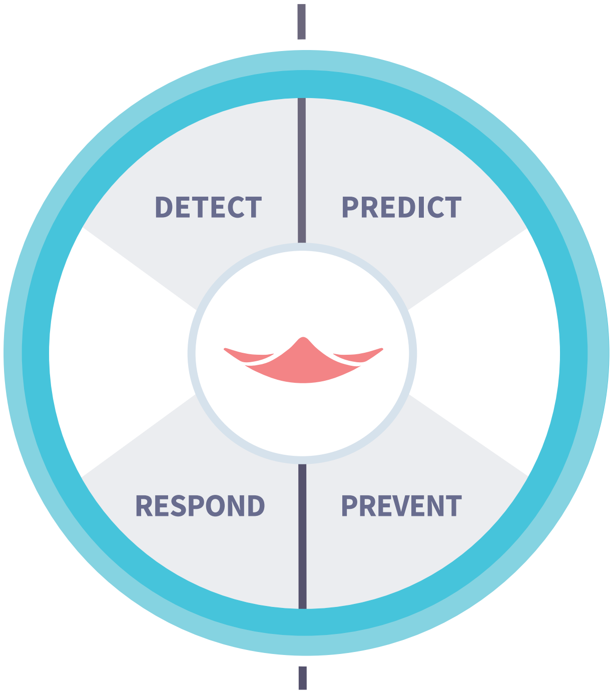
Integration Highlights

Visibility into all endpoint activity	Detection of threats and security incidents	Correlation with other security data	Threat mitigation and quarantine

Use Cases

Security

- Threat Detection
- Insider Threat Detection
- Unmanaged & Rogue Asset Discovery
- Malware Analysis
- Cloud Activity Monitoring
- Ransomware & Cryptoware Protection



Operations

- Network Traffic Monitoring
- Proactive Incident Creation
- Application Health
- Cloud Migration Management
- Accurate Endpoint and Application Inventory
- Patch Deployment Analysis

Why Ziften + Splunk?

Detailed analytics and real-time visibility into endpoint activity across the entire enterprise.

Continuously monitor for operations, security, and hygiene.

Respond faster with helpful direction to the right problem

Fill the gaps created by a lack of people resource

Plug the gap between existing tools (antivirus, firewalls, IDS/IPS, anti-malware, encryption, identity & access management)

Scan for vulnerabilities when people forget to tell their peers

Illuminate traffic on or off-net, in data centers, or across the cloud.

We help you understand what's happening in your environment.

Ziften for Splunk shines a light on security blindspots by providing additional endpoint context of processes, application and user attribution.

PARTNER

ziften