

Unified Systems Management and Security For Client Devices, Data Centers, and Cloud Workloads

We provide unified systems management and security. Our unique approach helps enterprises, governments, and managed service providers (MSP) monitor, manage and protect client devices, data centers, and cloud workloads. Ziften gives IT Operations and Security Operations teams real-time intelligence and control to conduct continuous monitoring, systems discovery and management, threat detection and response, and one-year lookback forensic investigations. Additionally, Ziften integrates with and extends the value of incumbent tools that benefit from enhanced visibility and control. With Ziften in your environment, you can take your physical and virtual systems from managed to secure.

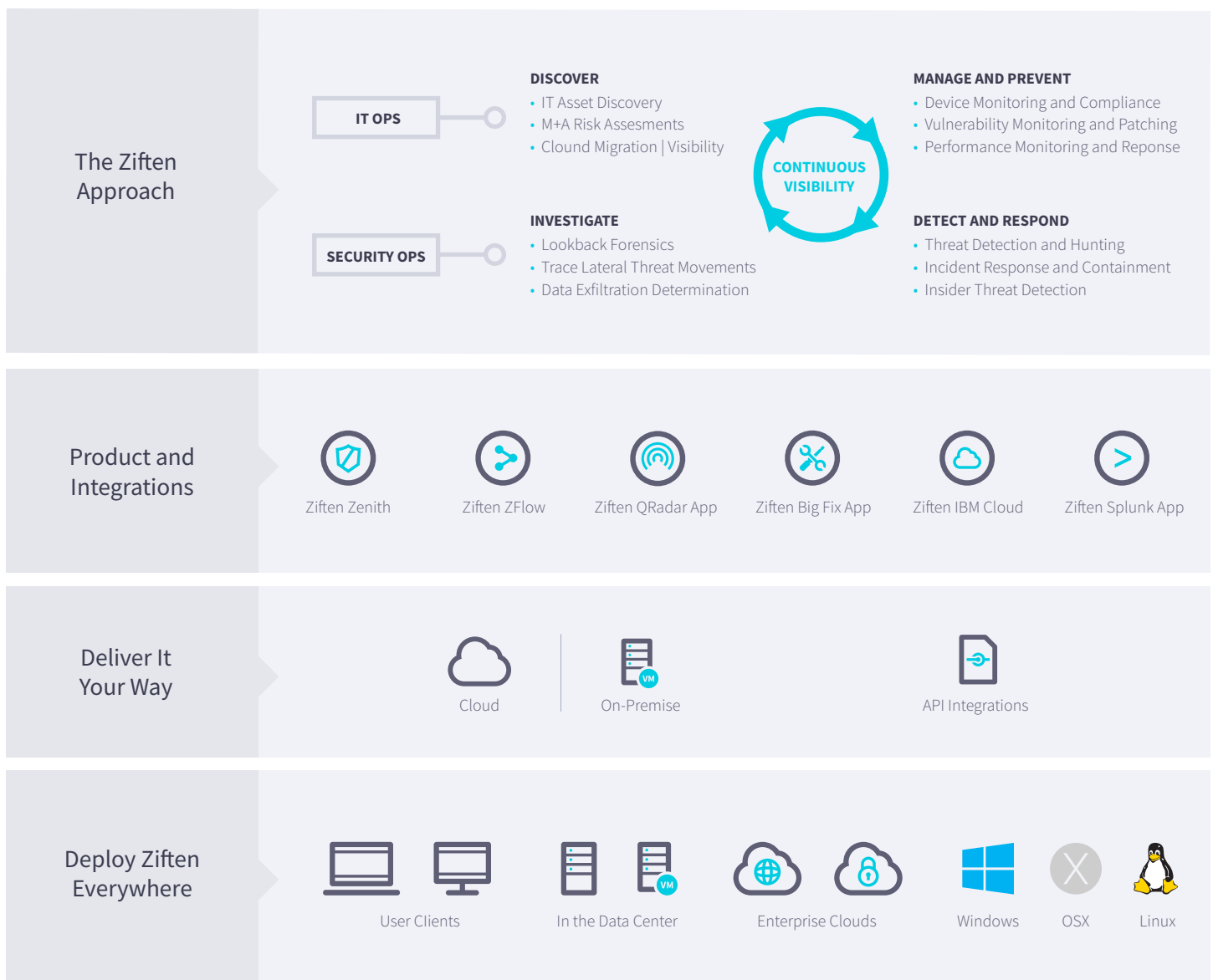
Core Vertical Markets

ENTERPRISE

- Communications
- Energy / Utilities
- Financial Services
- Healthcare
- Education
- Manufacturing
- Retail

GOVERNMENT

MANAGED SERVICE PROVIDERS



Ziften Milestones

- 2011**
 - Ziften 1.0
- 2012**
 - Ziften 2.0
- 2013**
 - Ziften 3.0
 - VMWare TAP Program
 - Ziften 4.0
- 2014**
 - Ziften App for Splunk
 - Alien Vault OTX Program
 - ServiceNow Integration
 - Lancope Partner Program
- 2015**
 - Ziften 4.5
 - Ziften ZFlow
 - Ziften Extensions Program
- 2016**
 - Ziften App for IBM QRadar
 - Blue Coat Integration
 - Splunk Adaptive Response Initiative
 - Fortinet Integration
 - Live Action Integration
- 2017**
 - Ziften Zenith (5.0)
 - BigFix Integration
 - Ziften IBM Cloud Security

Ziften Products and Integrations

Ziften Zenith

Zenith helps organizations take physical and virtual systems from managed to secure – (1) maintaining end-to-end visibility, (2) improving systems hygiene, (3) protecting against known and unknown threats, and (4) properly investigating and implementing corrective actions for identified performance issues and breaches.

Ziften App for IBM QRadar

The Ziften App for IBM QRadar provides additional intelligence, control, and forensics capabilities directly in the QRadar console. In addition, with Ziften’s unique network telemetry augmenting QRadar data, joint customers can more quickly connect network based alerts to a specific device, application, process, and user.

Ziften IBM Cloud

A validated solution, for the IBM Cloud for VMware. Ziften brings added visibility, context, and attributes for compliance, operational management, and control. With Ziften, organizations can maintain control and governance of hybrid clouds, just like their data center environments.

Ziften ZFlow

ZFlow delivers extended NetFlow from client devices, servers, and cloud. Organizations can augment existing NetFlow collection and analysis to (1) see east-west traffic in their data centers, (2) see what’s happening in their cloud deployments, and (3) link every network flow to a specific device, application, process, and user.

Ziften Big Fix Integration

Integrating Ziften’s continuous data extends IBM BigFix’s systems management capabilities for Windows, OS X, Linux, and cloud including (1) continuous asset discovery and agent deployment, (2) continuous vulnerability and device state management, and (3) continuous software inventory with detailed utilization reporting.

Ziften App for Splunk

The Ziften App for Splunk provides native integration of all Ziften data into Splunk so joint customers can monitor, manage, and protect client devices, data centers, and cloud workloads directly from Splunk Enterprise. The Ziften app populates Splunk Common Information Models (CIM) with rich endpoint data for use with other Splunk apps.

Technology Partners

- Alien Vault
- Cisco / Lancope
- FireEye
- Fortinet
- IBM
- LiveAction
- Palo Alto Networks
- ReversingLabs
- ServiceNow
- Splunk
- Symantec / Blue Coat

The Ziften Difference

Unlike other “next-gen” vendors that provide closed, patch management or threat detection and response; we provide a unified systems management and security platform. Our solution (1) supports on-premise or cloud delivery, (2) supports on- and off-network client devices, data center, and cloud, (3) provides continuous and 12 months or more historical intelligence, (4) enables unified risk management, and (5) provides open data sharing with SIEM, firewall, data analytics, ticketing systems, and more.

CONTACT US



<https://ziften.com>



sales@ziften.com