SOLUTION BRIEF

Fortinet and Ziften Integrated Security Solution

Security Without Compromise with Comprehensive Endpoint Visibility and Analytics

The ongoing mobility revolution has resulted in significant benefits for organizations and individuals, but also brings security risks and challenges to IT organizations. Flexibility in where, when, and how employees conduct business, as well as the proliferation of a wide variety of mobile phones, tablets, laptops, and other endpoints greatly increases the attack surface for new and sophisticated cyber-threats. Employees often conduct business from outside the office, from home, or while travelling, and these locations are typically not covered by a firewall. Attackers can breach these endpoints and systems and often hide for months at a time, traversing through the network to high-value business systems and critical infrastructure within the enterprise. IT organizations face growing stakeholder security demands, and have to deal with securing a rapidly-proliferating range of networking gear, mobile devices, and other endpoints.

Fortinet and Ziften have partnered to deliver an industry-leading security solution that addresses these challenges. Ziften provides end-to-end visibility and analytics to provide security teams with endpoint context to rapidly detect, remediate, and respond to both known and unknown threats. Fortinet's award-winning FortiGate

Key Benefits

- Rapidly decrease time to identify, investigate, and respond to breaches and malicious user behavior.
- Improve and harden Security Operations Posture.
- Gain greater understanding of host behavior
- Improve Total Cost of Ownership.
- Get unparalleled security protection with the industry's best validated security protection.
- Leverage Global Threat Intelligence to protect individual customers, using Fortinet's FortiGuard Security Subscription Services.

Enterprise Firewall Platform provides the industry's highest-performing firewall capabilities, and Fortinet's FortiGuard Security Subscription Services provide the industry's highest level of threat research, intelligence, and analytics. Bringing the Fortinet and Ziften products together into one integrated solution delivers comprehensive endpoint and network security protection.

How Does it Work?

The lightweight Ziften ZDR agent continuously records all endpoint activities (whether good, bad, or unknown) and sends all data to a central Ziften server for real-time detection as well as historical forensics. ZDR monitors activities including: processes, registry, network, file, user, event log, hardware profile, patch levels, vulnerabilities, and more. In addition to detecting threats, ZDR also mitigates threats with its robust response capabilities. Based on the type of threat that is detected, actions can be performed, such as: kill processes, ban files from executing, eject USB devices, block USB devices, and many more.

The Ziften ZFLow™ endpoint network sensor monitors any endpoint (laptop, desktop, VDI/virtual, datacenter, or cloud) for its network activity. It creates IPFIX flows with standard IANA fields plus custom fields that include the context behind the network activity (including information such as the process that made the connection, parent process, hash, user, hostname, OS information, and more). This enables the solution to address typical use cases such as east-west traffic visibility, off-network traffic visibility, public cloud visibility, network visibility in virtual/VDI environments, and last-mile network forensics.

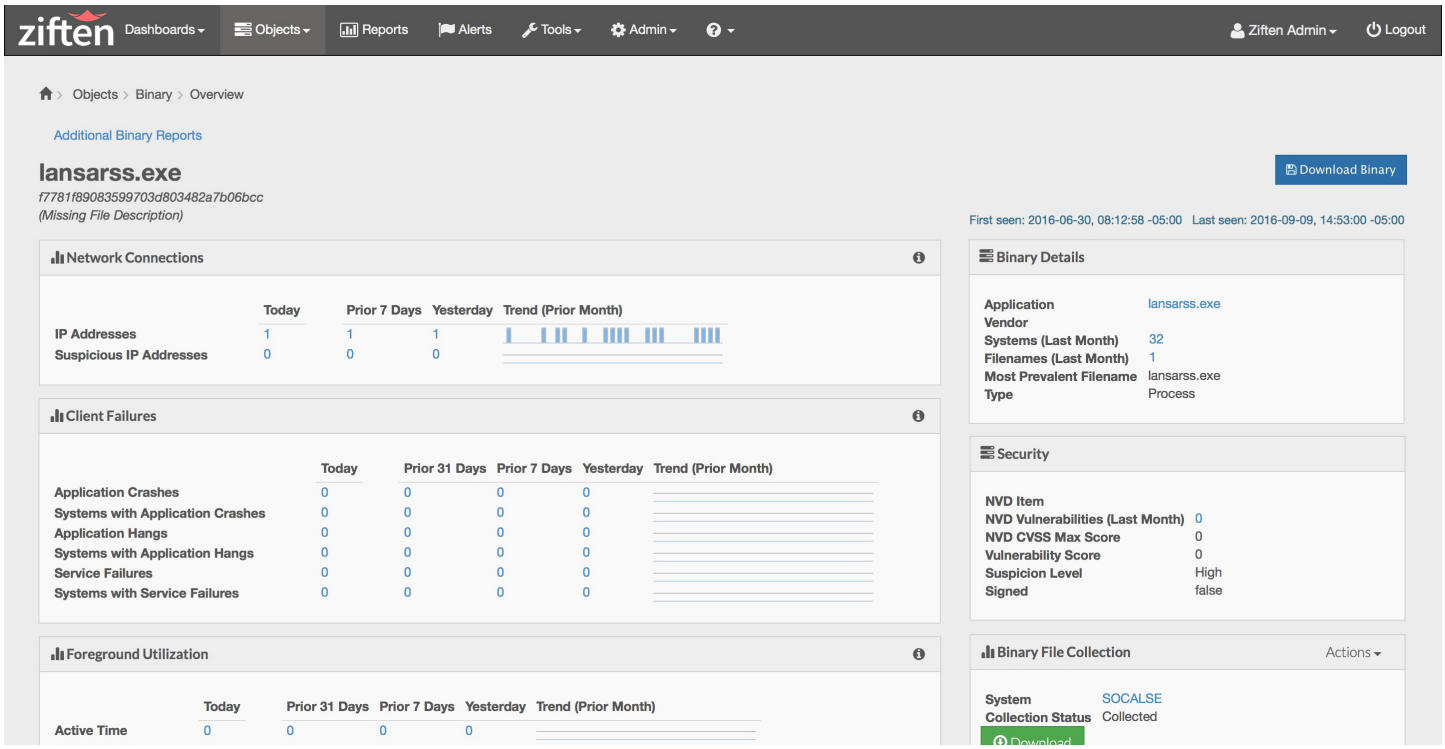
Complementing Ziften's endpoint security capabilities in the solution is Fortinet's award-winning FortiGate Enterprise Firewall Platform, which provides end-to-end security services across the entire network. This is strengthened by Fortinet's FortiGuard Security Subscription Services which provide the industry's highest level of threat research, intelligence and analytics. The solution leverages Global Threat Intelligence, to protect individual customers, by using FortiGuard to enable visibility and control for next-generation protection against advanced threats, including zero-day attacks.

FortiGate integration with Ziften enables the following functionality:

- Operationally pivot from any FortiGate log or alert to Ziften for additional context.
- Pivot on IP (source/destination) and/or port to understand which process was responsible for making a network connection on that specific system that generated the alert. Find out what other network connections that process made on the system that generated the alert, and also determine what other systems have that process/file to get the full scope of an infection.
- Determine what other systems have connected to that same destination IP, even when they may have connected while off-network.
- Pivot from FortiGate to Ziften based on source IP address to get the user and hostname details.
- Once Ziften has identified a system as being infected, one can operationally pivot to FortiGate to quarantine or limit the device.

FortiSandbox integration with Ziften enables the following functionality:

- Operationally pivot from any file analyzed by FortiSandbox to Ziften to get the details for every system that has ever run that file (regardless of whether or not the file still exists on that endpoint).
- Operationally pivot from FortiSandbox to Ziften to understand what network activity any file has made. Quickly stop dynamic/polymorphic malware by using FortiGate to block network activity for similar files (making the same malicious network connections).
- Ziften will automatically collect files from endpoints — no need to wait to determine something might be malicious or suspect to collect it.



COMPREHENSIVE ENDPOINT VISIBILITY AND ANALYTICS

Solution Benefits

Rapidly decrease time to identify, investigate, and respond to breaches and malicious user behavior.

- Improve and harden Security Operations Posture. ZFlow allows for highly specific alerting. These alerts reduce false positives as well as shorten attribution and remediation cycles when compared to older tools.
- Gain greater understanding of host behavior. ZFlow provides the highest resolution on patterns of a host's behavior. With modern endpoint flow data, behavioral detection modeling is more comprehensive and detailed than ever before.
- Improve Total Cost of Ownership. Endpoint flow opens access layers for end-to-end visibility to a part of the network previously too expensive to monitor effectively.
- Get unparalleled Security Protection. Leverage the industry's best validated security protection.
- Leverage Global Threat Intelligence. Protect individual customers using Fortinet's FortiGuard Security Subscription Services.

About Ziften

Ziften is a visionary provider of the ZDR platform for real-time endpoint security and management, offering unprecedented access to endpoint, user, application, and network data originating from user devices, data centers, and the cloud. Combined with Ziften's patented ZFlow technology, the company delivers real-time data, context, and relevance to security, operations, and risk and compliance teams. Ziften helps enterprises efficiently deal with unexpected threats and issues that get through their preventative measures, saving them money, minimizing cyber security risks, and improving productivity and end user experience. Learn more at www.ziften.com.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
Valbonne
06560, Alpes-Maritimes,
France
Tel +33 4 8987 0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel: 011-52-(55) 5524-8428

Sep 14, 2016