Fortinet and Ziften Zenith Integrated Security Solution

Security Without Compromise with Comprehensive Endpoint Visibility and Control

End-user mobility and the cloud have forever changed the way we work, communicate, and support customers – delivering great business value, but often at the expense of our cyber-security posture. Employees and their devices operate off-net and even offline greatly increasing the attack surface of the organization. Application workloads are virtual and operate in the cloud where traditional monitoring and security controls are limited or non-existent. And without thorough visibility and security controls in place, attackers can breach these endpoints and cloud systems and often hide for months at a time, traversing through the network to high-value business systems within the enterprise. Organizations face growing stakeholder security demands and have to deal with securing this growing user device and cloud infrastructure.

Fortinet and Ziften have partnered to deliver an industry-leading security solution that addresses these challenges. Ziften provides all-the-time visibility and control for client devices, servers, and cloud VM's so security teams can immediately detect, investigate, and respond to both known and unknown threats. Fortinet's award-winning FortiGate 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 Ziften Work?

With Ziften Zenith a lightweight, non-kernel agent continuously records all endpoint activities (regardless of whether those activities are good, bad, or unknown) and sends all data to a central Ziften server for real-time detection of threats, risky behaviors/ configurations, and compliance or policy violations. System activities monitored by Ziften include: running process, network activity, user behaviors, installed applications, file activity, system baseline configuration and changes, vulnerabilities and missing patches, and more. In addition to visibility into all activities in real-time, Ziften also provides visibility into past/historical activities to investigate a potential threat and identify the initial point of infection (patient-zero), the full scope of the infection, and any endpoints which may have previously been compromised but no longer show signs of the infection (but are still potentially vulnerable or still infected).

In addition to threat detection, Ziften also includes robust threat response capabilities, both automated as well as analyst-approved (configurable based on settings). Response actions include the "standard" response actions (process kill, file deletion, quarantine, and registry change) as well as less common actions (USB control, push out patches, install applications/ tools, forensic memory dumps, change firewall settings, disable services used to spread ransomware, and more). In addition to out-of-the-box actions, Ziften also offers custom action capabilities through the powerful Extensions platform, a custom scripting tool that allows organizations to operationalize running and controlling scripts on their endpoints. Not only can Ziften Extensions be used for taking actions, but also for the collection of any custom data from any endpoint.

Solution Benefits

- Rapidly decrease time to indentify, investigate, and respond to threats and compromised or malicious users
- Improve and harden overall security posture through integrated endpoint and network security
- Gain greater understanding of host and user behavior with lastmile network visibility, allowing Fortinet customers to get complete visibility from their network into their endpoints
- Get unparalleled security protection – leverage the industry's best validated security protection Leverage global threat intelligence – protect your organization with Fortinet's FortiGuard Security Subscription Services

FORTINET Fabric-Ready

Extending Fortinet's Security Fabric to the Endpoint

Ziften Zenith integrates with Fortinet's FortiSandbox by automating the collection and submission of files from endpoints (whether client devices, server devices, or cloud VM's) to FortiSandbox's malware analysis solution. Once a file has been submitted and malware analysis has been completed by the FortiSandbox, Ziften will automatically feed the analysis results into the Ziften console for automated alerting of any detected threats. When a threat is detected, Ziften and Fortinet will coordinate response efforts to mitigate the threat on the endpoint (Ziften) and network (Fortinet). In addition, with the power of Fortinet's Security Fabric, response is automated across all Fortinet solutions to provide a comprehensive mitigation of detected threats.

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, using FortiGuard to enable visibility and control for next- generation protection against advanced threats, including zero-day attacks.

Together Ziften Zenith and Fortinet FortiSandbox enable:

- Automatically collecting files from any endpoint, including client, server, and cloud endpoints
- Automatically submitting files to FortiSandbox for deep file analysis, leveraging real-time analysis and FortiGuard Labs intelligence
- The inclusion of deep file analysis results in the Zenith console for visibility and alerting of threats detected by FortiSandbox
- Automatically coordinating threat response across both endpoints and the network for complete protection
- Automatically sharing threat detection and response actions across the entire Fortinet Security Fabric

Ziften Zenith integrated with Fortinet FortiGate enables:

- Correlating endpoint and network based alerts to improve and speed overall threat detection efforts.
- Quick triage of FortiGate alerts by pivoting to Ziften from any alert for additional last-mile context from the endpoint.
- Guaranteed user and host attribution for any alert, regardless of whether endpoint is tied to Active Directory or not.
- Understand the responsible process and file behind any network activity.
- Search for other endpoints with similar behaviors, regardless of whether activity occurred on-premise or while the endpoint was remote / off-premise.

Reducing false-positive alerts by understanding the endpoint activity related to FortiGate alerts, helping to provide additional context.

About Ziften

Ziften delivers all-the-time visibility and control for any asset, anywhere - client devices, servers, and cloud VMs – whether onnetwork or remote; connected or not. Our unified systems and security operations (SysSecOps) platform empowers IT and security operations teams to quickly repair user impacting endpoint issues, reduce their overall risk posture, speed security threat response, and increase operations productivity. Ziften's secure architecture delivers continuous, streaming endpoint monitoring and historical data collection for large and mid-sized enterprises, governments, and managed security service providers (MSSP). And Ziften helps extend the value of incumbent tools, and fill the gaps between fragmented, siloed systems.

FORTINET®

www.fortnet.com

February 6, 2019 9:14 PM

123456-0-0-EN

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:Egnyte:Shared:CREATIVE SERVICES:Team:Susie-Hwang:2018:Collateral-Refresh-2018:Solution-Brief-Template:sb-template-gray Folder:sb-template-gray