ziften
WHITEPAPER

Ziften's Client-to-Cloud

Adaptive Security Model

"Adaptive security is a continuous state of improvement and corrective actions that includes discovery, prevention, detection & response, and investigative efforts. It requires continuous visibility of users, systems applications and network behavior."

Why Adaptive Security

"Enterprises are overly dependent on blocking and prevention mechanisms that are decreasingly effective against advanced attacks. Comprehensive protection requires an adaptive protection process."[1]

Adaptive security implies an on-going process that incorporates multiple cyber security functions that can be used in a concerted effort to continuously learn, and improve the ability to stop breaches and minimize risks. In the recent past, too many organizations have focused primarily on blocking and prevention techniques, and policy based controls to block threats. However, one hundred percent prevention is impossible.

Organizations must operate with a mindset that they are in a state of continuous compromise. With this mindset, organization must implement a balanced approach to security that includes constant and continuous IT asset discovery, security posture monitoring, threat detection and response, and deep data forensics capabilities. Thus, adaptive security is a continuous security process that requires:

1. Continuous visibility and analysis of users, systems, applications, and network behavior.
2. A continuous state of improvement and corrective actions including Discovery, Prevention, Detection & Response, and Investigative efforts.

Approaching Adaptive Security From the Endpoint

The endpoint is the front line when it comes to cyber security per Forrester[2]. Why? Because user endpoints and servers are targeted more than any other enterprise assets in cyberattacks, which is why Forrester recently stated that endpoint security is the front line when it comes to cybersecurity.

"[E]mployee client devices, and servers are targeted more by cyber-attackers than any other type of asset."

- The Forrester Wave™: Q4 2016

What is an Endpoint?

Traditionally, endpoint brings to mind laptop and desktop personal computers, and perhaps personal mobile devices. But in today's enterprise networks, the term endpoint means much more. Enterprise networks have thousands of connected devices. These might include the following to name a few:

- User devices such as laptops, desktops, workstations, virtual desktop systems, bring your own devices (BYOD), smart phones, and tablets.
- Data center and cloud devices such as servers, virtual machines (VM), orphaned VM's, containers, and storage systems.
- Networking devices such as routers, switches, firewalls, load balancers, and WiFi access points.
- Other devices such as printers, and more recently – Internet of things (IoT) devices.

Why Adaptive Security from the Endpoint?

If the endpoint is the front line in cyber security, organizations must maintain an awareness of what's happening on that front line. They must understand their endpoint environment. In fact, SANS Critical Security Controls for effective cyber defense lists developing an inventory of authorized and unauthorized devices number one on their list. Once the landscape is understood, organizations must also build a strong security posture to defend their endpoints.

Second, while organization may rely on network based security tools, they often struggle to understand the user, device and application context for network-based security tool alerts. Quite simply, much of the data necessary to respond to, investigate, and contain threats or breaches resides at the endpoint.

So, adaptive security models have to start with a powerful understanding and management of the endpoint environment.

Challenges Adaptive Security Can Address

Many organizations simply lack the visibility and security they need. This is true at the network level, with traditional endpoints, in data center environments, and even more so in cloud deployments, which the following data points illustrate.

- **Unknown Assets**
  Ziften's deployments find that as much as 30% of all connected assets or VMs are previously unknown to the organization.
- **Lack of Cloud Visibility**
  The 2016 Netwrix Visibility Report shows that as many as 75% of companies have little to no visibility into their enterprise cloud environments.
- **Undetected Breaches**
  On average enterprises take 21 weeks to find a breach, according to the 2016 Mandiant M-Trends EMEA report. That duration of "dwell time" is simply unacceptable.
- **No Look-Back Forensics Data**
  PwC's cybercrime research indicates that most organizations lack the data and analytics needed to adequately investigate breaches they find.

Figure 1: Ziften Client-to-Cloud Adaptive Security Model

Client-to-Cloud Adaptive Security Model

Ziften helps organizations protect their client devices, data centers and cloud deployments from cyber-attacks. We do this using an integrated security solution that helps organizations implement an adaptive security process from an endpoint perspective that enables the following.

"Ziften uses an integrated security solution that helps organizations implement an adaptive security process from an endpoint perspective"

- **Unmanaged IT Asset Discovery**
  Ziften enables organizations to discover and fingerprint all assets, with no additional network or processing overhead, and no disruptive network activities that set off security tool alerts.
- **Threat Detection and Response**
  Ziften provides a complete picture of suspicious activity and threats within your environment, and an improved ability to co mitigate threats reducing incident response times by up to 96%.
- **System Monitoring and Hardening**
  Ziften provides the visibility and tools required to understand your organization's current security posture, and to identify and make improvements, often reducing in the number of non-compliant endpoints by up to 80%.
- **Deep Lookback Forensics**
  Ziften stores up to 12 months of rich endpoint intelligence giving incident responders the forensics data to dig until they find the root cause of a breach, and to implement corrective actions preventing future failures.

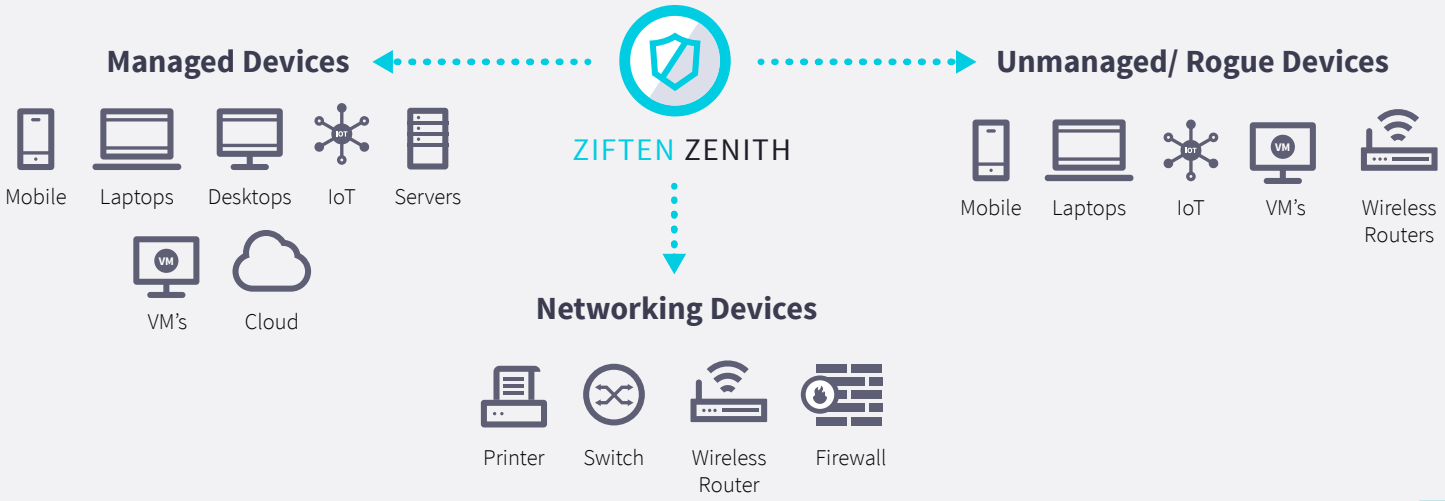

Figure 2: Unmanaged IT Asset Discovery

"SANS recommends that the number one task in creating effective Cyber Security Controls is to develop an inventory of authorized and unauthorized devices."

1. **Discover**

Most enterprise IT organizations have a limited understanding of their attack surface because they are unable to understand the full range of devices that are on the network. SANS recommends that the number one task in creating effective Cyber Security Controls is to develop an inventory of authorized and unauthorized devices. Unfortunately, understanding the device inventory has become even more challenging with the advent of dynamic virtual networks, bring your own device (BYOD) policies, and Internet of things (IoT) devices appearing at the office.

As a key aspect of understanding an organization's security posture, Ziften includes passive and continuous asset discovery.

Every Ziften Agent in the network takes on the task of passively monitoring for Ethernet announcements that are required for any network device to operate in the same network. This information is evaluated and changes in the list of connected devices are captured. For each discovered device, an administrator can quickly identify each device that is not under management by IT, and evaluate the product details on that connected device provided by Ziften.

As the solution discovers network devices passively, obtrusive network scans are not required, avoiding unwanted network traffic and device impacts. This eliminates unwanted security tool alerts from the asset discovery process. Since the agent is constantly assessing the device health and monitoring for new devices, the Ziften console always provides a current view of any devices that have accessed the protected network.

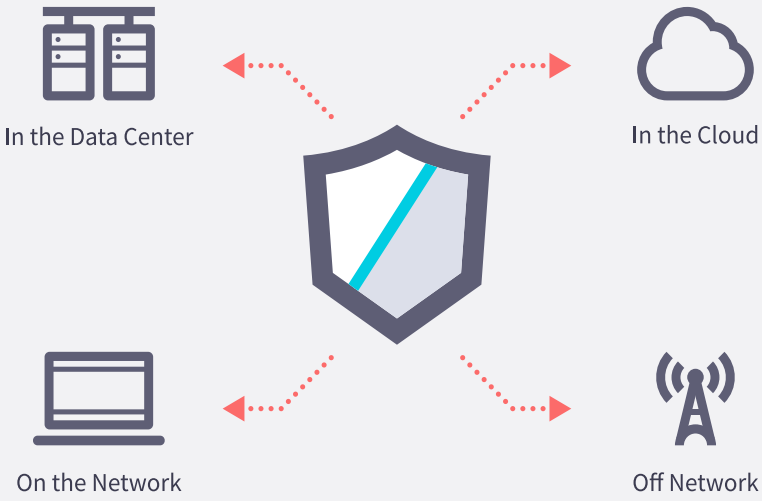

Figure 3: Posture Monitoring and Hardening Across the Enterprise

"The Ziften Zenith solution provides IT organizations with the truth about their security posture. The combination of external intelligence with the constant flow of device state intelligence provides administrators with a unique view into the risks their current devices represent."

2. Prevent

Most cyber security professionals indicate that the first step in understanding and improving your cyber security posture is to identify and evaluate the devices that are on your network.

The Ziften solution provides IT organizations with the truth about their security posture. The Ziften Agent collects all important device state information and provides security teams with the intelligence and reporting to understand which devices pose an increased risk to their organization, enabling enterprises to take action and improve their defenses to prevent cyber-attacks.

Continuous posture monitoring allows Ziften to alert on policy infractions in real-time. The process works both on and off the network, and integrates with existing third-party workflow components including SIEM tools, systems management platforms, ticketing systems, and orchestration platforms. With Ziften, administrators can understand the most critical aspects of their security posture, including:

- Device inventory
- Attack surface over time
- Encryption deployments
- Application usage and version proliferation
- System and application vulnerabilities
- System and application patch status
- Application usage and compliance
- Software license rationalization
- Network usage and suspicious behavior
- Suspicious binaries and applications
- Suspicious client (host) behavior
- WinSAT scoring

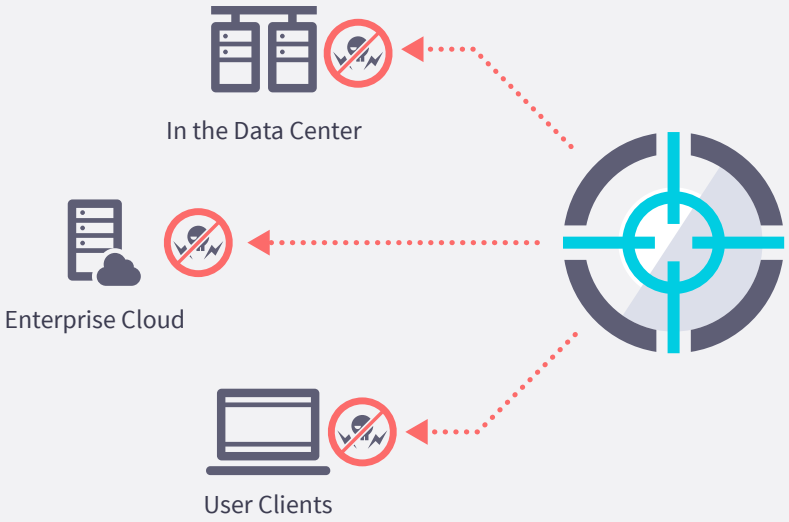

Figure 4: Threat Hunting and Incident Response

"For every device that is confirmed to be infected, Ziften can be used to contain and eliminate the full scope of the threat."

3. Detect & Respond

Given the current state of the Internet, it is impossible to completely avoid the barrage of attacks that have now become commonplace. When an organization's defenses are penetrated, Ziften provides the features needed to detect threats that are resident on the host.

Ziften also supports the integration of global threat intelligence from many third party partners. Threat intelligence further enhances the detection of suspicious behavior on all devices. In addition, Ziften supports the integration of open source and proprietary customer intelligence feeds, allowing organizations to integrate intelligence from their favorite sources.

Using Ziften, administrators get a complete picture of suspicious binaries, applications, network, and user activity within their environment – from user devices, to data center servers and virtual machine endpoints, to cloud based virtual machines and even containers.

Once a threat is discovered, it is critical to quickly ascertain how many devices are impacted. Ziften response and forensics features can be used to investigate the breadth of the attack, illustrating which devices the infected host has contacted over a historical period.

For every device that is confirmed to be infected, Ziften can be used to contain and eliminate the full scope of the threat. Administrators can kill processes, adjust registry keys, and restart system services directly from the Ziften Console. If these measures are insufficient to mitigate the threat, administrators can disable network operations on the affected device, quarantining it until the threat can be properly remediated.

Figure 5: Lookback Forensics, Investigation, and Threat Elimination

4. **Investigate**

After the immediate response to contain new threats, Ziften enables look-back investigations to discover and correct the entire set of actions the threat has created in the environment including:

- Performing forensic look-back analysis going back up to 12 months
- Pinpointing possible data exfiltration attempts
- Tracing lateral movement of threats over time
- Determining root cause vulnerabilities used throughout the chain of events
- Performing thorough breach clean-up

Consider the example of a system on the network that has been compromised. If undetected, the threat will likely attempt to spread to other systems across the network, extending the damage it creates. The threat may ultimately infect many systems by the time it is detected and contained.

Unfortunately, many security tools stop once they have found and quarantined a single compromised system. Ziften, by contrast, uses its historical monitoring data to enable look-back forensic analysis. This allows IT security teams to find all systems affected by the threat, along with associated incoming traffic that could indicate the attack's point of entry (for instance an unpatched system) and outgoing traffic that could reveal data sent to locations off the network.

"Unfortunately, many security tools stop once they have found and quarantined a single compromised system. Ziften, by contrast, uses its historical monitoring data to enable look-back forensic analysis."

Summary

The Ziften client-to-cloud adaptive security model enables a truly adaptive approach to finding and fixing issues and threats, and to implementing corrective actions from the learnings over time. In general, adaptive security is a continuous state of improvement and corrective actions that includes discovery, prevention, detection & response, and investigative efforts that requires continuous visibility of users, systems, applications, and network behavior.

"In general, adaptive security is a continuous state of improvement and corrective actions that includes discovery, prevention, detection & response."

Below is a summary of today's challenges and the adaptive security recommendations organizations should consider.

Key Challenges[3]

- Existing blocking and prevention techniques are insufficient to protect against motivated, advanced attackers.
- Most organizations continue to overly invest in prevention only strategies.
- Security capabilities from vendors have been delivered in nonintegrated silos, increasing costs and decreasing effectiveness.
- Information security doesn't have the continuous visibility it needs to detect advanced threats.
- Enterprise systems are under continuous attack and are continuously compromised. An ad hoc approach to "incident response" is the wrong mindset.

Recommendations[3]

- Shift your mindset from "incident response" to "continuous response", wherein systems require continuous monitoring and remediation.
- Adopt an adaptive security process for protection from advanced threats.
- Favor context-aware network, endpoint and application security protection platforms that provide integrated adaptive security capabilities.
- Develop a security operations center that supports continuous monitoring and is responsible for an integrated continuous threat protection process.
- Architect for comprehensive, continuous monitoring at all layers of the IT stack: network packets, flows, OS activities, content, user behaviors and application transactions.

1. "Designing an Adaptive Security Architecture for Protection From Advanced Attacks", Gartner, Neil MacDonald and Peter Firstbrook, Refreshed January 28, 2016.
2. "The Forrester Wave: Endpoint Security Suites, Q4 2016", Chris Sherman, October 19, 2016.
3. Adopted from a similar set of challenges and recommendations in "Designing an Adaptive Security Architecture for Protection From Advanced Attacks", Gartner, Neil MacDonald and Peter Firstbrook, Refreshed January 28, 2016.

WHT-10001-1AEN, Dec 2016

ziften