ziften
WHITEPAPER

What to Look for in a Scalable, Adaptable Endpoint Security Architecture

Accommodate the Demands of Enterprise Networks

Enterprise IT departments are faced with immense challenges in deploying security measures to protect dynamic endpoint environments. In addition to identifying products that provide strong security features, security teams must also ensure that selections have adaptive, scalable and resilient architectures that deploy without negative side effects.

Given the pervasive nature of endpoint security deployments, with agents throughout the enterprise, products have a unique capacity to wreak havoc upon devices and networks. It is imperative that endpoint security solutions are designed, from the ground up, to account for the dynamic nature of endpoints and robust enterprise requirements for scale and availability. Solutions that are not architected to account for challenging enterprise class environments will provide significant management headaches as they scale in customer environments.

"Ziften has extended performance, scale and resiliency to a level that surpasses the needs of enterprise networks."

Ziften's Zenith architecture is the first endpoint security solution that is truly designed to adapt to the dynamic nature of endpoint devices while accommodating the demands of enterprise networks of any scale. Within the architecture, Ziften has extended performance, scale and resiliency to a level that surpasses the needs of enterprise networks. Combined with industry leading discovery, prevention, detection and response features, Ziften Zenith provides enterprises with an ideal solution for endpoint protection.

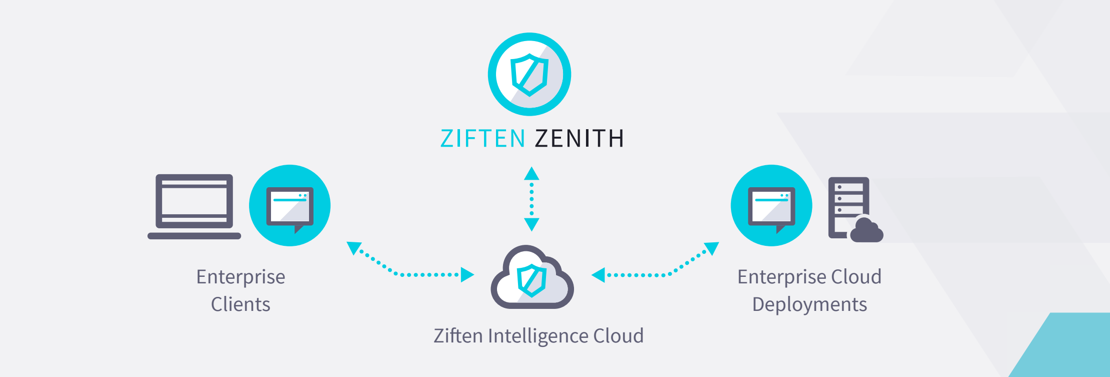

Figure 1 - Ziften Architecture

At the highest level, the primary components of the Ziften solution shown in Figure 1 are described below:

- **Ziften Agent**
  The agent is an installable executable for Windows, Mac or Linux. The agent has the task of collecting endpoint system information, forwarding to the Ziften Intelligence Cloud and taking specific action to protect the device, if required.
- **Ziften Intelligence Cloud**
  In cloud-based deployments, the intelligence cloud is delivered and supported as a hosted service. In on-premise deployments, the intelligence cloud is delivered as a virtual or physical appliance.
- **Zenith User Console**
  The Zenith console provides a web-based user interface allowing Host, Network, Security or Risk Operations team members to discover, and manage endpoints, and to detect, respond to, and investigate threats.

With any endpoint security deployment, it is critical to understand the features that define how those parts will interact with each other and with the network. Ziften's architecture is designed to provide features that protect the enterprise without negative side effects for hosts or the network, regardless of scale or topology. Table 1 provides an overview of the key architectural features covered in this white paper.

> "Ziften's architecture is designed to provide features that protect the enterprise without negative side effects for hosts or the network, regardless of scale or topology."

Architectural Features	Description
ENDPOINT FEATURES	
Broad Host Support	Support for all popular operating systems
Mobility and Transience	Support for local, remote, and offline client devices
Network Traffic Impact	Network impact of less than 4MB per day
Performance Impact	User-mode agent designed to protect the end-users experience
MANAGEMENT FEATURES	
Deploy Anywhere	Support for both cloud and on-premise management
Dramatic Endpoint Scale	Single instance scales to 1,000,000 endpoints
High Performance Backend	Vertica analytics database provides Exabyte scale and incredible speed
Always-on Management	All components support redundant deployments
Deep Data Storage	Support for up to twelve months of historical data
Data Safety Measures	Server storage deployed in high availability configurations
Continuous Feature Delivery	Both agent and management support continuous feature delivery

Table 1 - Ziften Zenith Architectural Features

Endpoint Security Starts with the Endpoint

Regardless of whether an enterprise is trying to manage a mixed environment of company provided hosts for it’s employees or trying to jump on the wave of companies supporting BYOD models[1] , one thing is certain -- all IT groups must support the reality that network endpoints are becoming more varied and mobile. Endpoint solutions must support various models that account for the mobility of all protected devices and take steps to minimize the impact the solution has on endpoint processing and network traffic.

The Ziften Agent is designed to provide the highest level of security, while still taking into account key deployment considerations, such as:

- Broad host support
- Mobility and transience
- Network traffic impact
- Performance impact

Broad Host Support

Enterprises require support for the wide array of operating systems that are commonly used, going beyond typical Windows operating systems. The Ziften Agent provides full support for Windows, Mac OS X, and common Linux operating systems.

> “The Ziften solution is designed to support all three agent communication models; local, remote and offline collection of events.”

Microsoft	Apple	Linux
Windows XP Windows 7+ Windows Server 2003+	Mac OS X 10.6+	Red Hat Centos 5.5+ Scientific Ubuntu Fedora

Figure 2 - Operating System Support

The agent is provided as a native installation package, that can be easily installed manually or distributed and installed via a package management solution. The installation package installs as a system service (or daemon) that quietly collects information, interacts with the Ziften Intelligence Cloud and protects hosts, without any interaction from the endpoint’s user.

[1] http://www.gartner.com/newsroom/id/2466615

Mobility and Transience

Enterprises are continuing to see employees vary the locations that they work from, with 61% of workers reporting that they work outside the office, at least part of the time[2]. Endpoint products must take on the challenge of providing security, regardless of whether the endpoint device is on the enterprise network (local), on another internet enabled network (remote), or completely inaccessible to the management server (offline).

The Ziften solution is designed to support all three agent communication models; local, remote and offline collection of events.

The local communication model is the most commonly used model for agent-server communication. In this model, the agent is located within the same network boundaries as the intelligence cloud and would generally be considered to be within the enterprise's network.

> "In a typical deployment, the total amount of traffic sent by an agent averages less than 4MB each day – lower than an endpoint's normal traffic levels for common tasks such as email and Internet browsing."

In the remote model, the agent is allowed to operate normally when it is outside of the enterprise's network boundaries. In this model, the agent can function as long as the agent's host has any network path to reach the intelligence cloud, typically over the Internet. In order for this model to be supported, the intelligence cloud must either be delivered as a hosted cloud service, or be deployed with Internet access if it is hosted on-premise.

While the Ziften Agent's normal operation allows for constant communication with the intelligence cloud in local or remote mode, it also supports a feature-set that allows it to easily adapt to offline operation. Offline operation is designed to allow the agent to collect all relevant endpoint data and events, storing them for delivery to the intelligence cloud when the agent reconnects. The agent supports transitioning from offline operation to either remote or local connectivity.

The combination of flexible intelligence cloud deployment models and the agent's offline feature-set allows the agent to provide the highest level of visibility and protection achievable, regardless of where the device is located or how often it transitions between networks.

Network Traffic Impact

A common concern for network administrators, when deploying an agent-based solution, is the impact the deployment will have on network performance. It is critical that an endpoint security agent is designed to limit the impact it causes on the network. This is especially important as the total number of endpoints continues to grow within a network.

[2] https://www.citrix.com/articles-and-insights/workforce-mobility/jun-2015/7-enterprise-mobility-statistics-you-should-know.html

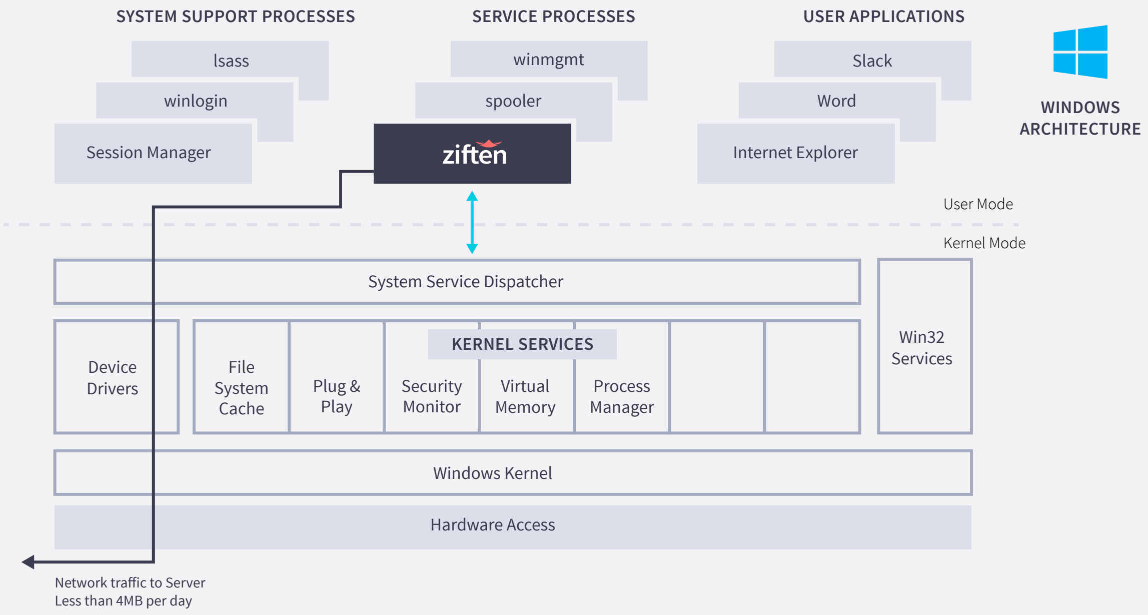

Figure 3 - Ziften Windows Architecture

The Ziften Agent is designed to be safe, lightweight and to minimize the amount of traffic generated. The agent sends traffic continuously (can be configured to send traffic only during endpoint idle times) to update the intelligence cloud on system and behavioral activities that have occurred on the endpoint. The Ziften Agent employs proprietary techniques to ensure that the data sent represents the minimum amount of traffic possible, while transmitting all required high value content. In addition, the agent employs enhanced compression techniques to further minimize the total traffic level.

> “Having an adverse impact on user experience is generally found to be unacceptable and must be accommodated by the endpoint agent’s architecture.”

In a typical deployment, the total amount of traffic sent by an agent averages less than 4MB each day. By comparison, the Ziften Agent’s traffic normal level is lower than an endpoint’s normal traffic levels for common tasks such as email[3] and Internet browsing.

Performance Impact

While providing excellent security, it is also important that an agent does not impede the user’s ability to normally use a device. Endpoint security agents have long had the reputation of monopolizing system resources and imposing additional latency on typical user activity. Having an adverse impact on user experience is generally found to be unacceptable and must be accommodated by the endpoint agent’s architecture.

The Ziften Agent is specifically designed to minimize any impact on the end user. As shown in Figure 3, the agent’s architecture imposes the unique requirement that the agent runs in the operating system’s User Mode as a Service Process. User Mode is one of two distinct execution modes for the CPU. It is a non-privileged mode in which each process (i.e., a running instance of a program) starts out[4].

[3] Office365 estimates email daily traffic levels vary from approximately 2MB to 10MB (for power users). https://blogs.technet.microsoft.com/educloud/2012/02/13/how-much-bandwidth-do-i-need-for-my-users-connecting-to-exchange-online/

[4] http://www.linfo.org/user_mode.html

By running in User Mode, the agent's processes are not provided with the same level of full system control as kernel mode processes. As a result, the agent does not have the capacity for it's processes to interfere with normal operations. Read more about User Mode versus Kernel Model deployments in the Ziften whitepaper titled "Endpoint Security in Today's Threat Environment: User Mode versus Kernel Mode Installations."

As the Ziften Agent goes about its normal business of evaluating and collecting data on system resources, it takes steps to ensure that non-critical housekeeping activities are only performed when the host would otherwise be idle. This constraint ensures that normal user activity is rarely in competition with the agent for system resources.

Endpoint Management that Scales with the Enterprise

As described in Gartner's latest Endpoint Detection and Response Market Guide, a key architectural consideration in a top solution is the support of a highly scaled centralized management server[5]. The Ziften Intelligence Cloud provides this functionality, with the right features to support an enterprise's increasing need for scale, such as:

- Deploy anywhere architecture
- Dramatic endpoint scale
- High performance backend
- Resilient, always-on management
- Deep data storage
- Data safety measures

"To provide support for the varied needs of each enterprise, Ziften supports the deployment of the intelligence cloud in the cloud, or on the enterprise's network (on-premise) in a physical or virtual form."

Deploy Anywhere Architecture

To provide support for the varied needs of each enterprise, Ziften supports the deployment of the intelligence cloud in the cloud, or on the enterprise's network (on-premise) in a physical or virtual form.

Cloud deployments of the Ziften Intelligence Cloud are fully supported by Ziften, including hosting services and upgrade support. This model allows for the service to be turned up very quickly and allows the Ziften Agents to connect from anywhere that an Internet connection might be available.

Conversely, it is sometimes necessary for an enterprise to have full control of all internally generated data often due to external regulatory requirements. To support this requirement, Ziften also supports the deployment of the intelligence cloud as a virtual image or physical appliance. Using this model, the enterprise can deploy an instance of the intelligence cloud within the protected network, outside on an unprotected network or within a hybrid/cloud deployment.

[3] 5 Gartner – Market Guide for Endpoint Detection and Response.pdf, Page 7 – Architectural Considerations

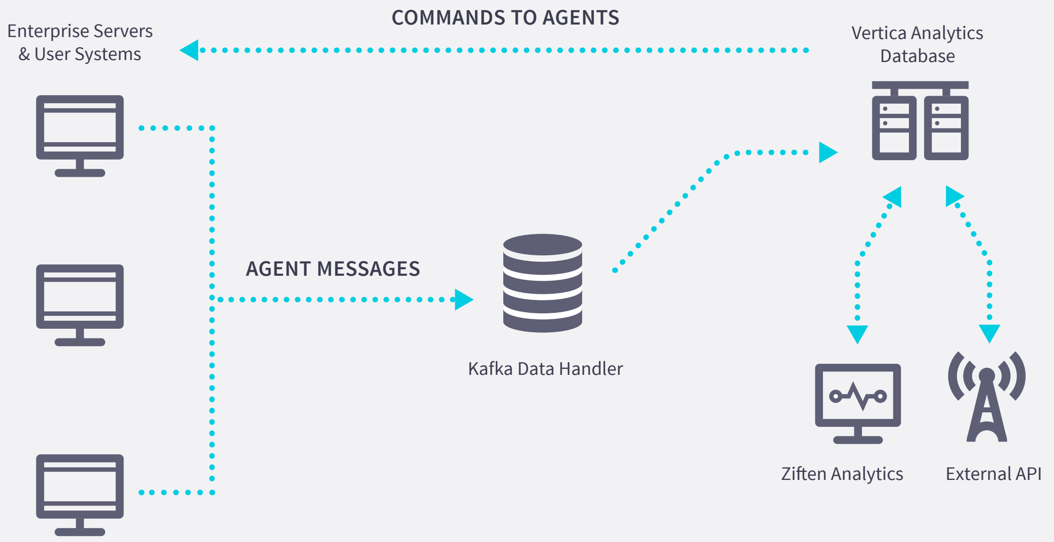

Figure 4 - Internal Intelligence Cloud Architecture

> “Ziften required a high-performance backend to support their end-to-end architecture. The Vertica analytics database was the perfect fit. It provides Exabyte scale, incredible speed, and the flexibility necessary to handle massive volumes of data.”
>
> - Hewlett Packard Enterprise

Dramatic Endpoint Scale

In deploying an endpoint solution, it is critical to have confidence that the solution is architected to support a wide range of endpoint counts, from a handful on a small network to hundreds of thousands for the largest scale of enterprises.

Ziften has taken specific steps within the architecture to allow a single instance of the intelligence cloud to easily support up to at least 1,000,000 endpoints. This level of scale is unique within the industry and promises to provide strong support, regardless of the growth in numbers of devices.

Ziften has achieved extreme endpoint scaling by enhancing its event collection algorithms to allow for highly paralleled receipt of messages from the agent, rapid processing, and immediate queuing for storage with the database. The server architecture, depicted in Figure 4, allows for the use of multiple instances of key message processing components and includes the ability for distributed processing of those messages. As a result, the overall architecture continues to scale, even if the resources of a single system are consumed, by adding additional systems with the appropriate server components.

High Performance Backend

In order to support enterprise scale requirements, while allowing for expedited UI updates and reporting, each intelligence cloud deployment includes an instance of the Vertica analytics database. The resulting architecture provides highly parallel and efficient insert and query times, allowing the intelligence cloud storage to scale dramatically, without negatively impacting insert performance or user interface response times.

With enhanced message processing algorithms, combined with support of the Vertica analytics database, the Ziften Intelligence Cloud architecture achieves near real-time insertion of critical alerts generated by the endpoint agents. Further, the UI architecture is designed for rapid response across the highly scaled database.

Resilient, Always-on Management

Endpoint security is not effective without an always-on management system. To achieve a high level of availability, each component of the must be architected with redundancy and robustness built-in.

In on-premise deployments, the Ziften Intelligence Cloud is able to be delivered with multiple instances, deployed across several virtual or physical appliances. The internal algorithms are designed to support distributed processing of inbound messages and alerts. With multiple instances of server components configured, the architecture is capable of continued operation if a single instance goes down for some reason. A redundant deployment model allows for the continued operation of management console, even in the case of system failure.

Cloud-based deployments of the Ziften Intelligence Cloud are implemented to support redundancy. If an enterprise elects to deploy in the cloud then redundancy is supported by default. If deploying the intelligence cloud on-premise, then it will be required to setup and configure multiple instances of each intelligence cloud component to achieve the ultimate level of redundancy and resiliency.

> “The Ziften Intelligence Cloud supports the storage of six months of historical data, providing sufficient storage for most investigatory and forensics efforts - additional months of data-storage can also be acquired and configured.”

Deep Data Storage

A key feature of any endpoint security solution is the capability of evaluating historic events and system information, supporting the investigation of specific security incidents. It is imperative that the solution’s management platform supports a deep data storage mechanism, allowing for extended research efforts to yield useful results.

In typical deployments, the Ziften Intelligence Cloud supports the storage of six months of historical data in the included Vertica analytics database, providing sufficient storage for most investigatory and forensics efforts. Additional months of data-storage can also be acquired and configured for use in the intelligence cloud, if an organization requires addition data depth.

Data Safety Measures

Securing the integrity of agent data is a key requirement for any management solution. The Ziften architecture is deployed with key measures to ensure the integrity of all stored data. All Ziften Intelligence Cloud instances are required to be deployed on hardware or virtual instances that are capable of supporting RAID 10, in order to ensure that sufficient mechanisms are in place to maximize speed and availability of storage.

Architected to Deliver Continuous Value

Given the rate of change of exploits and threats, it is imperative that any security solution be designed to allow for continuous improvements. It is no longer sufficient for users to wait until the next quarter for updates that might be required to detect and respond to current-day threats.

Both the Ziften Agent and Intelligence Cloud are architected to allow for safe and seamless upgrades and continuous feature delivery. The Ziften development team employs an Agile Continuous Delivery Process, allowing for rapid updates to sub-components of active deployments, without experiencing downtime or loss of visibility or security. Using a rapid delivery model, Ziften can supply feature updates as soon as they are available, instead of waiting for pre-defined release schedules.

> “Both the Ziften Agent and Intelligence Cloud are architected to allow for safe and seamless upgrades and continuous feature delivery. Ziften can supply feature updates as soon as they are available, instead of waiting for pre-defined release schedules.”

Summary

The Ziften architecture delivers unparalleled scale and resilience, while adapting to the dynamic nature of the endpoint devices. Built upon a strong framework, Ziften speeds endpoint security feature delivery, without the issues that hamper traditional and competing next-generation endpoint security products.

ziften

WHT-10001-1AEN, Dec 2016