Ziften Zenith Review

A Broadband-Testing Report By
Steve Broadhead, Founder & Director, BB-T

BROADBAND TESTING

Table of Contents

Broadband-Testing

Broadband-Testing is Europe's foremost independent network testing facility and consultancy organisation for broadband and network infrastructure products.

Based in Europe, Broadband-Testing provides extensive test demo facilities. From this base, Broadband-Testing provides a range of specialist IT, networking and development services to vendors and end-user organisations throughout Europe, SEAP and the United States.

Broadband-Testing is an associate of the following:

- Limbo Creatives (bespoke software development)
- Broadband-Testing Laboratories are available to vendors and end-users for fully independent testing of networking, communications and security hardware and software.

  Broadband-Testing Laboratories operates an Approvals scheme which enables products to be short-listed for purchase by end-users, based on their successful approval.

  Output from the labs, including detailed research reports, articles and white papers on the latest network-related technologies, are made available free of charge on our web site at www.broadband-testing.co.uk
- Broadband-Testing Consultancy Services offers a range of network consultancy services including network design, strategy planning, Internet connectivity and product development assistance.

Executive Summary

- Such is the lack of visibility within most IT infrastructures that securing that infrastructure is all but impossible. How can you secure what you can't see?
- The emergence of SysSecOps – combining systems and security operations – is a major step in the right direction, as it is founded on having complete visibility in the first place, then applying endpoint security.
- With its Zenith platform, Ziften has a product that ticks all the SysSecOps boxes and more. Since its definition of "endpoints" extends into the Data Centre (DC) and the world of virtualisation, it is true blanket coverage.
- The configuration/deployment options and architecture of Ziften allow for a very flexible deployment, on or off-premise (OnPrem/OffPrem) or hybrid. Agent deployment is simplicity itself with zero user requirements and no endpoint intrusion. Agent footprint is also minimal, unlike many endpoint security solutions. Scalability also looks to be excellent – the biggest customer deployment to date is in excess of 110,000 endpoints.
- Once deployed, everything is controlled from a single management user interface – the Ziften console, keeping life simple and training costs minimal.
- Integration options are extensive; existing data can be imported directly into the console (e.g. using a .csv file) and Ziften has developed external API functionality for mass integration with 3rd party products.
- Data analysis options are equally extensive. From the dashboard (completely customisable) you can continue to drill down into the captured data. There is also a very flexible search engine. Any object can be analysed – e.g. Binaries, applications, systems – and, from a process, an action can be defined as an automated function, such as quarantining a system in the event of a potentially malicious binary being discovered. Multiple reports are pre-defined covering all areas of analysis.
- Alerts can be set for any incident – based on definition – and delivered via a number of options, such as by email. Additionally, Ziften provides the concept of extensions; essentially these are for custom data collection or execution of actions and allow for the execution of PowerShell and Bash scripts, maintained and signed by Ziften.
- With its External API functionality, Ziften-gathered endpoint data can be shared with most 3rd party applications, thereby adding further value to a customer's existing security and analytics infrastructure investment.
- Overall, Ziften has a very competitive offering in what is a very worthy and emerging IT category in the form of SysSecOps.

SysSecOps and Ziften

Securing Contemporary IT Endpoint Infrastructures

Networking has got itself into an unholy mess.

The bolt-on approach to building networks over the best part of the past three decades has brought with it many problems, not least visibility. Many companies - regardless of size, geographical spread and status - simply do not know what applications, devices and even users are on their network. They don't necessarily even know where their extended network actually is, not least due to all forms of outsourcing over those decades, culminating in cloud-based deployments in the past few years.

Add in virtualisation in the form of Virtual Machines (VMs)/containers and the whereabouts of data and applications could require more than a digital Sherlock Holmes to locate them. Of course, that's the proverbial tip of the iceberg. It's not simply a case of not knowing which applications and browsers are loaded on a device, assuming you know that device exists, but also which versions thereof. More fundamentally, what Operating System (OS) versions are these running on; what patches have been installed, what Java versions are running on them, what Flash versions, Anti-Virus/Anti-Malware definition updates…? And then you have to secure all of this. The point here is - how can you secure something if it's not actually visible? In a recent Frost and Sullivan report, 38% of organisations admitted they are likely to have unaccounted for assets in their networks. For too long, IT has been creating islands of technology and resource, so tasks and data that should be shared are split between different teams and individuals who seldom communicate with each other. The result is a huge void in terms of visibility and understanding of what is on the network and how to manage it.

In a recent Frost and Sullivan report, 38% of organisations admitted they are likely to have unaccounted for assets in their networks.

A recent report from Technology Research outlined the concept of SysSecOps – that is to say combining systems and security operations into a single IT profile or categorisation. And it makes total sense as it's all about visibility and follows the aforementioned mantra - if you don't know what your systems are running – basically what is happening on an ongoing basis - then how can you possibly secure users, their data and applications? The report concluded that, at the heart of a SysSecOps approach are endpoint security integration and organisational coordination. More to the point, it suggested that many of the successful cyber-attacks over the past few years could have been prevented with such an approach in place. Integration appears to be the key challenge currently, when securing endpoints, as can conflicting security goals within an organisation – those islands of security administration.

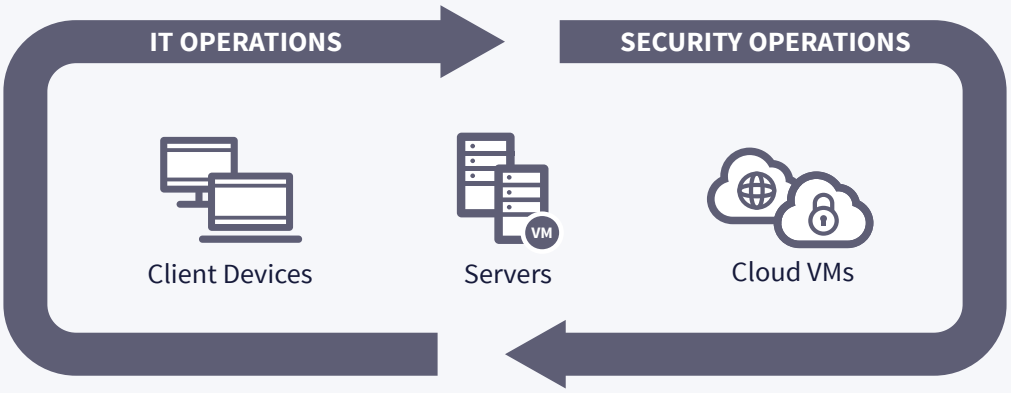


Figure 1 – SysSecOps

So the last thing you need is endpoint security that is neither integrated nor coordinated with the rest of the operations, but that is essentially what the report found with respect to many current endpoint security tools. To say this is proving costly is an understatement; it's already estimated that the recent WannaCry ransomware virus will likely cause more than $4 billion in economic damage. Key findings of the SysSecOps report were that integrated security visibility is a top challenge and that security starts at the endpoint. Several questions were raised as to a fundamental lack of knowledge within IT departments, including:

- What systems are connected to our network?
- What software is running on those systems?
- Are my systems compliant to our own policies?
- What vulnerabilities exist in our systems?
- Are there clear indicators of threats on my systems – internal or external?
- How did a threat get onto our systems?
- What actions did a threat take once it was in our environment?

A recent survey by the Enterprise Strategy Group (ESG) found security professionals are inundated with security incidents, averaging 78 investigations per organisation over the past year, with 28% of those incidents involving actual targeted attacks. And in almost every case, response to any alert, be it vulnerability, compliance or actual breach alerts, requires quick, coordination between both IT and security teams. Hence the requirement for endpoint control with coordinated systems and security operations, aka SysSecOps.

The report concluded that the needs for SysSecOps highlights the requirement to integrate existing systems management and security tools, coordinate budgeting and planning across organisational boundaries, and focus on using endpoint visibility data to drive analytics-based improvements for building predictive detection of security and system risks.

Ziften, whose Zenith product is the focus of this report, is in a prime position to drive SysSecOps, having all the components in place, unlike many EDR (Endpoint Detection and Response) vendors, whose focus is solely on threat detection. Now let us take a look in more detail at the aims of Ziften with its Zenith product, including a hands-on session evaluating the features and functionality of the product and how it integrates into existing infrastructures.

Product Overview

Ziften Zenith

With its Zenith platform Ziften has created a tool for what it describes as client-to-cloud visibility and security.

This includes access to user behaviour, system, application, and network data originating from user client devices, DCs and the cloud. What this translates into is continuous and look-back visibility, security posture assessment and enforcement, and real-time detection and response to security, operations, risk and compliance teams. Many security vendors talk about minimising a company's attack surface and that indeed is the aim here, while improving security and operational efficiencies which, in turn, will deliver real cost savings as well as a more secure and better-managed infrastructure. And to clarify, when Ziften talks about securing endpoints it means traditional client devices like laptops, desktops and VDI deployments, servers, VMs and containers running in a DC or in the cloud.

The Ziften architecture is designed to support both OnPrem deployments as a virtual appliance, and cloud-based deployments – the architecture is the same regardless. The two primary components in the architecture are the Kafka Message Broker and HP Vertica Analytics Database. With these components Ziften claims to achieve horizontal scaling while maintaining a high-performance data rate; the largest customer deployment currently is in excess of 110,000 endpoints. Redundancy is integrated, as is continuous feature delivery, in line with a SaaS-based product. On this basis, the product has broad appeal, designed to meet the demands of pretty well any company size, from remote/branch office, through mid-size and large enterprise, to governments, MSSPs (Managed Security Service Providers) and similar service/outsourced delivery companies.

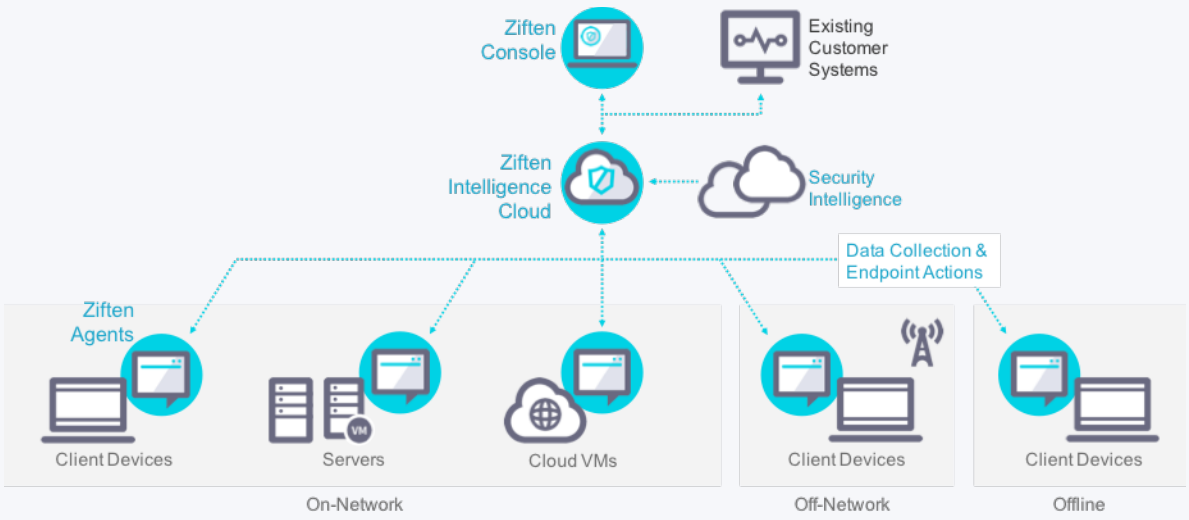


Figure 2 – Basic Ziften Architecture

So what are the basic aims of the technology?

- **System Analyses:** Continually assessing the device, its capability, the usage of the device, the user's experience with the device, the idea being to maintain the best possible performance for the end user.
- **On-going Risk Assessments:** Continually looking for unmanaged assets, the compliance of managed assets, while conducting detailed vulnerability assessments for each device.
- **Conducting continuous threat monitoring:**
  Detect, respond to, and remediation of both internal and external threats on the endpoints.

All of this is built on the basis of total visibility rather than simply data snapshots - continuously streaming data from the endpoints. There is no query or request required. Once that data is collected, it is continuously analysed, scored, alerted upon and correlated with associated work-flow. An asset can be on-network or off-network, connected or not connected and the visibility data can be retained for 12 months or more depending on customer/legal requirements.

As the visibility data is collected, it is augmented with what Ziften defines as security intelligence sources, such as the Reversing Labs analysis and report services that we have included in the test platform here (see next section). Once the endpoint data is collected, using the Ziften Console (see "hands-on" section) you can ask any question or query, searching across the entire data set - all historical data and all assets.

Typical Use Cases

Asset Discovery

This can be used to build a complete application inventory, so IT can look at detailed foreground and background usage statistics in order to gain accuracy in software license management, actual usage and related data. Ziften cites that many customers initially justify their purchase of Zenith from this capability alone.

Systems Management

IT uses Ziften for on-going systems management. This normally consists of monitoring for performance issues, looking for application hangs or crashes, or the classic "blue screening". This is designed to not only aid the helpdesk team to react to and fix performance issues faster (i.e. before the user calls them!) but, moreover, these issues are often indicative of a security issue requiring further investigation.

Security Hygiene Monitoring

Security hygiene functionality includes monitoring the overall state or posture compliance of each asset, and monitoring all applications and the OS for unpatched vulnerabilities. Once identified, they can be prioritised and corrected/updated accordingly.

The security operations teams use Ziften for monitoring and detecting both malicious threats and anomalous user behaviours. With access to the endpoint visibility data, they can conduct complex searches and analysis to identify malware, suspicious binaries, suspicious network connections, suspicious user behaviours, or other indicators of compromise. These investigations can be fully automated, or customised to investigate unique scenarios. Once an initial threat is dealt with, incident responders can conduct forensic investigations using historical data to find possible lateral threat movements and respond accordingly.

Ultimately the idea is to uncover the root cause of the initial intrusion, and appropriately address the root cause in the organisation's security procedures.

The desired end game from deploying Ziften is both increased security and efficiency. Existing customer examples have shown that, from a reliability standpoint, customers often cut their helpdesk calls for endpoint issues by 10% or more as the software identifies and fixes issues before they are recognised by the wider user community. Customers also learn to reduce the number of unknown devices in their networks, in some reported cases by as much as 98%. Ziften claims they also dramatically reduce the number of non-compliant assets connected to the network through continuous compliance monitoring, often by 80% or more.

Equally, they can dramatically reduce the number of unpatched critical vulnerabilities in environments, drastically lowering their overall security risk in the process – remember, reducing that attack surface is all-important. Tying in with this is reducing the mean time to respond to identified security threats and/or suspicious communications or behaviour. In some cases, customers have reported reducing their response times by 96% or more – going from several days to just hours to successfully respond to security incidents.

Existing customer examples have shown that, from a reliability standpoint, customers often cut their helpdesk calls for endpoint issues by 10% or more.

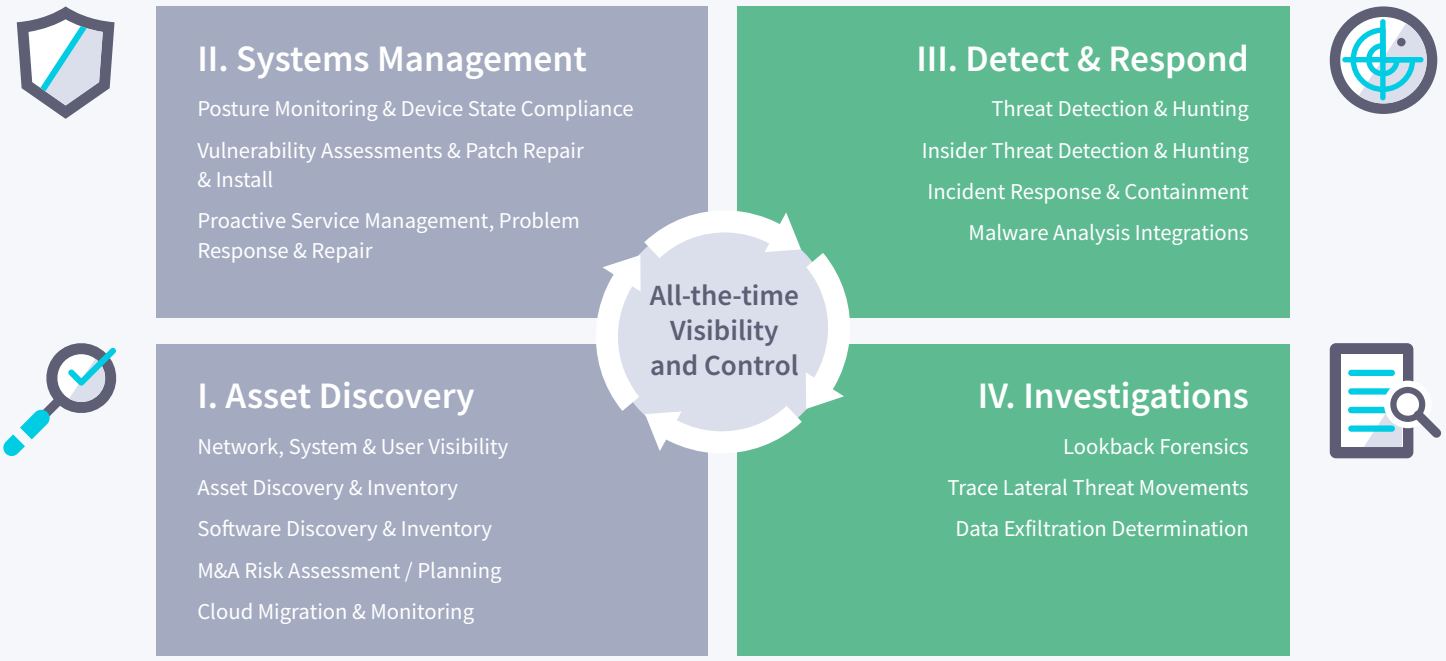


Figure 3 – Typical Use Cases

Ziften Features and Functionality: Hands On

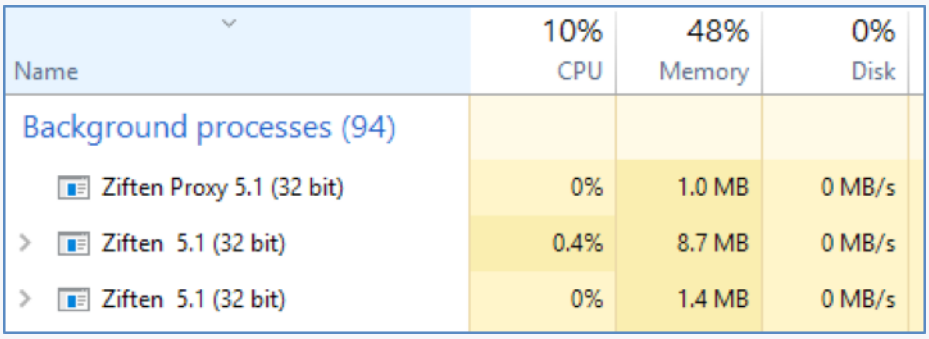
Deployment and Configuration

As we mentioned earlier, there are two basic deployment options – On Premise (OnPrem) or Off Premise (OffPrem).

With the massive shift towards OffPrem deployments nowadays – which is where someone like Ziften really adds value to the Operating Expenses (OpEx) element – our focus here is on the Ziften-hosted solution which can be cloud-based or a SaaS model. Deployment in this OffPrem scenario really is as simple as it gets; simply install the relevant endpoint agent, depending on what combination of endpoints you have, given that these can be a mix of Windows and Mac clients, servers, Linux, VMs and containers, including VMs in a cloud environment.

For the testing, we simulated a remote office, with our Windows-based endpoints reporting back to a cloud-based host - an environment typically open to attack and with little or no human security intelligence onsite. Our entire deployment consisted of simply downloading and installing Windows agents (1.94MB .msi files), then responding to an email with our console login details – and we were up and running. Ziften claims a rapid deployment rate, plus the ability to discover all devices or systems connected to the network, and get full visibility of those systems, is realistic and there is no reason to doubt this. Existing endpoint data can be directly imported into the system via a .csv file.

So a lightweight Ziften agent is deployed to the endpoints. As soon as the agent is installed, visibility data starts to be streamed back to the Ziften Intelligence Cloud. The agent runs as a service under the System user in Windows and as a daemon in macOS and Linux. The agent has no user interface or any visible components to the user – it is totally transparent, both during installation and in use. The Windows agent service, as tested, runs three processes (Ziften.exe, Ziften.Proxy.exe, and Ziften.Updater.exe), with minimal footprint – see example captured from a Windows 10 laptop endpoint on the test network:



Name	10% CPU	48% Memory	0% Disk
Background processes (94)			
Ziften Proxy 5.1 (32 bit)	0%	1.0 MB	0 MB/s
Ziften 5.1 (32 bit)	0.4%	8.7 MB	0 MB/s
Ziften 5.1 (32 bit)	0%	1.4 MB	0 MB/s

Figure 4 – Windows 10 Agent Footprint

Likewise, the macOS and Linux agent daemon run three processes ("Ziften Agent," "Ziften Proxy," and "Ziften Updater"). The agent runs in system mode so there is no driver to install, no kernel impact, and no reboots required! These processes can be observed by an admin user with native tools. The agent collects information about currently running processes, services, DLL files, and the system itself. Agents cache information in a locally stored database. This data is encoded and compressed into Google Protobuf format and sent over a secure connection to the server. By default, Ziften will provide a self-signed 2048 bit RSA SSL for agent to server communications. However, customers can provide Ziften with a comparable PKCS12 certificate to use if preferred. As noted, each agent has a Ziften Updater process, so once installed agents automatically update when a newer version is available from the server. Users can also select to manually update agents if preferred.

The Ziften agent does not collect or submit information from within applications themselves, document names opened by an application, emails or passwords. It collects system and user names, process names, metrics (memory utilisation, CPU usage, I/O, network), sockets and network connections (type, port, IP addresses, associated process), the processes username that it runs under and a processes full command line, including arguments. It also collects all client-side IP addresses, MAC addresses, hardware information, selected Windows system event logs, user state (active or inactive based on mouse or keyboard activity) and – optionally - all remote IP address, port numbers, and the associated PID (Process Identifier). Despite the wealth of data being captured, daily traffic levels are very low – around 2MB maximum, as observed and, as recorded by Ziften itself.

The agent runs in system mode so there is no driver to install, no kernal impact, and no reboots required!

Passive "Fingerprinting"

Ziften defines its data discovery approach as passive, in that it is non-obtrusive. The agents discover and effectively "fingerprint" every physical or virtual device connected to the network from day one. That "fingerprint" of device manufacturer, hostname/MAC address helps identify the device type and beyond – essentially it's the endpoint's passport. This device discovery is maintained through continuous monitoring, rather than a snapshot-based approach. The fundamental problem with the latter is that, by definition, it misses events and incidents and related cause/effect implications. Murphy's law dictates that those very instances that are missed will be the key ones!

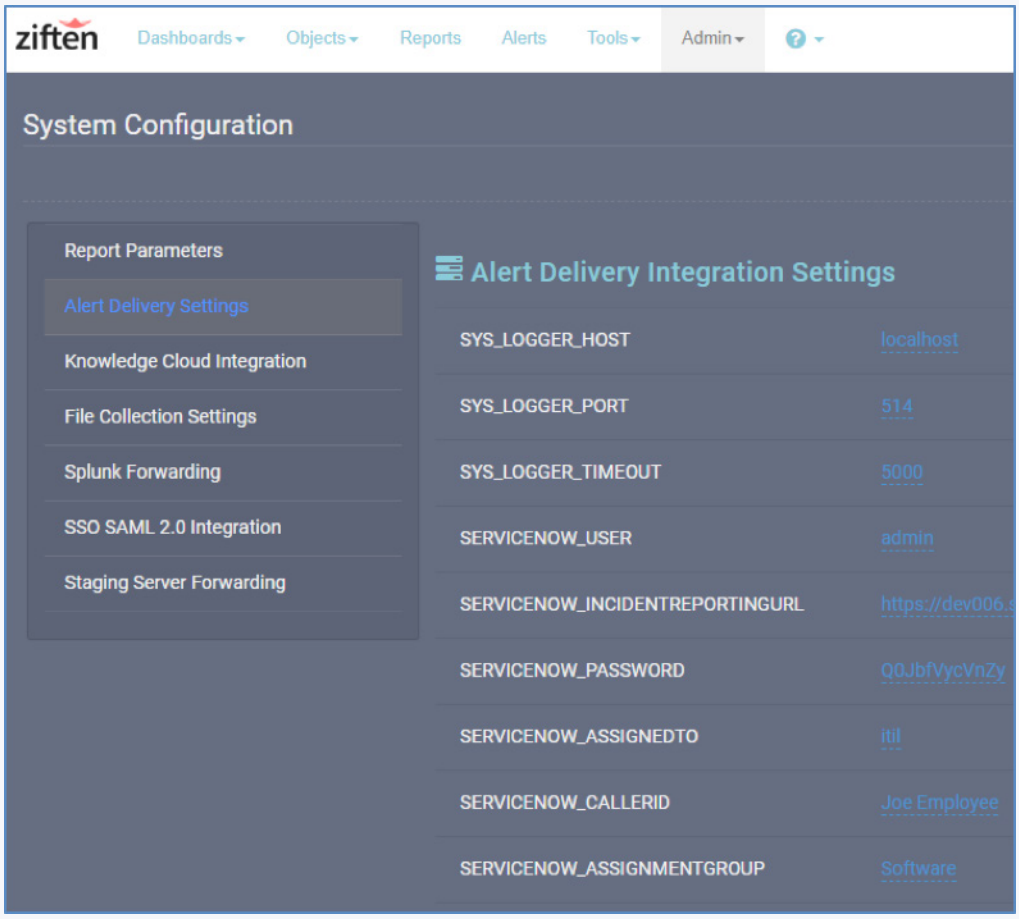


Figure 5 – System Configuration From Ziften Console

Since data collection starts the moment an agent is installed, you can make use of the Ziften Console immediately and start to configure the system to your own requirements (see next section for examples), such as setting up alerts and alert respondents, custom dashboards, reports etc, though Ziften provides a wealth of pre-defined options that will satisfy the needs of many users, straight from the off.

Features and Functionality

All the features of the Ziften solution can be accessed from the browser-based console.

There are six basic menu options, set out along the top of the browser – Dashboards, Objects, Reports, Alerts, Tools and Admin. Each option drops down to reveal more choices. In the case of Dashboards and Reports, this reveals a large number of pre-formatted examples. More than a dozen dashboards are pre-defined, any of which can be designated as the default one that opens on the console, but you can also create custom dashboards, as we did to focus on two key aspects we perceived within our remote office simulation test – application sprawl and unlicensed application usage, selecting a layout then adding "widgets" – data views – from a very broad selection spanning all the elements available in the Reports section:

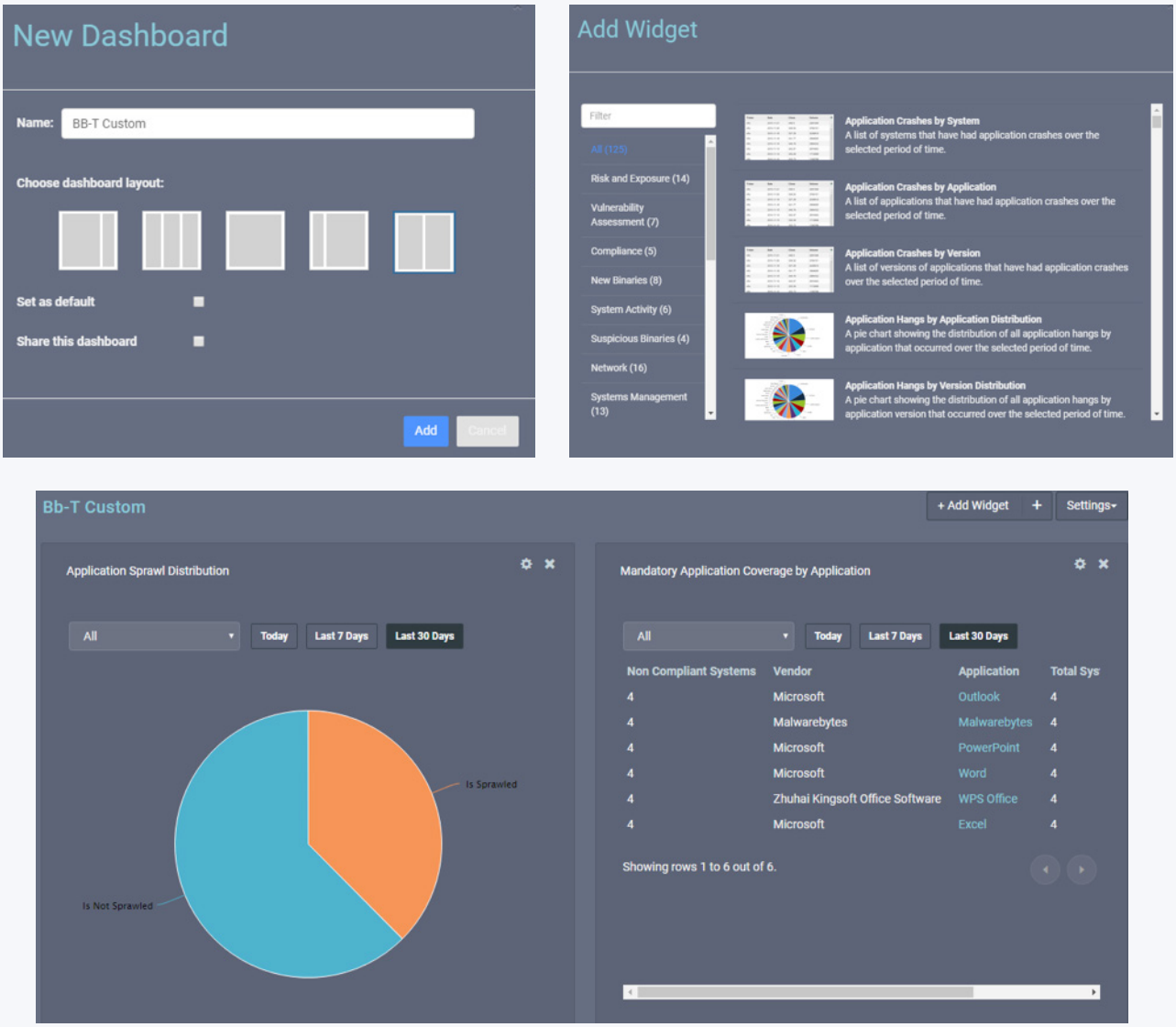


Figure 6 – Creating A Custom Dashboard

For example, here – left-hand graph - we are looking at binaries that are only seen running on one system or 0.1% of the total systems in the environment (whichever is greater) that being the application sprawl. We want to minimise this sprawl as it could a) lead to serious update/patching problems and/or b) indicate illicit application usage.

This is being supported by the table on the right, showing mandatory applications, but equally can be used to show use of non-compliant/unlicensed applications. Tied in very closely with this is “attack bloat” - binaries from the attack surface that are not the latest version of the application seen on the network (environment), also known as version proliferation. This clearly increases our attack surface – an obvious negative we need to respond to.

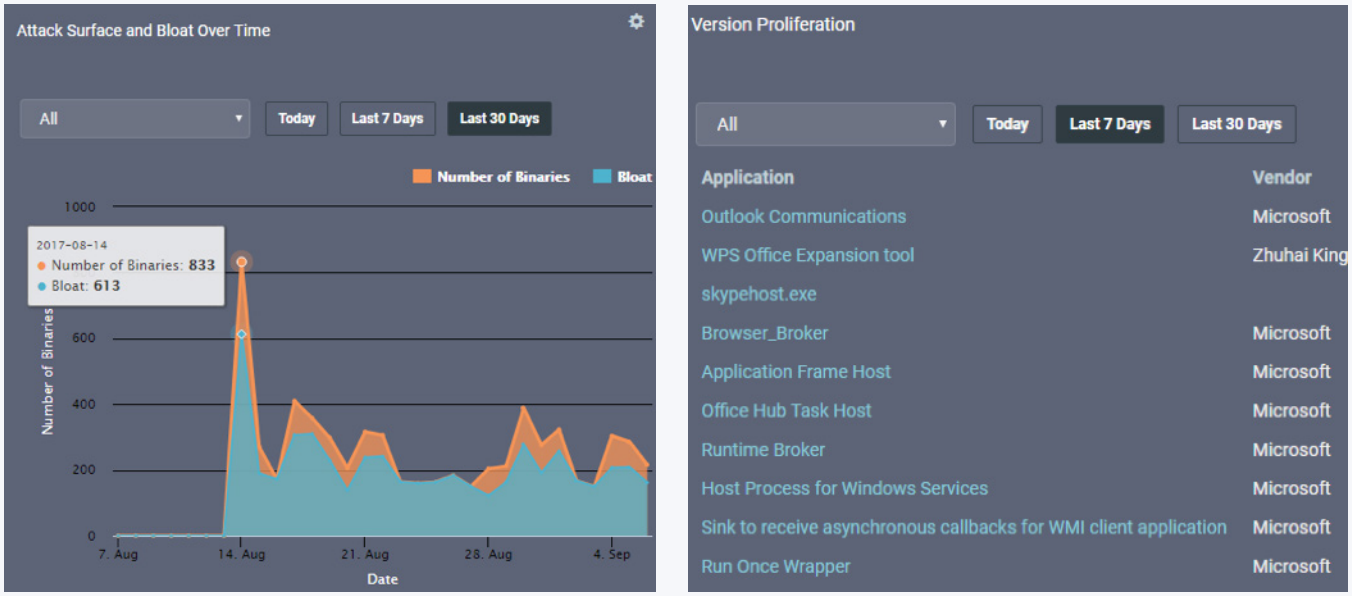


Figure 7 – Attack Bloat And Application Version Proliferation

Here is a good example of how we can continue to drill down with Ziften and extract more details. If, see above, we click on Outlook Communications, we are presented with the binary details and whether that binary is suspicious or not. Clicking on an individual binary would then take us to all related information concerning that binary – for example, network connections, client failures, security issues, utilisation and usage. From here we can even go to one of our defined intelligence sources, as we explained earlier in the report; in this case Reversing Labs, log in and get a complete report on that binary.

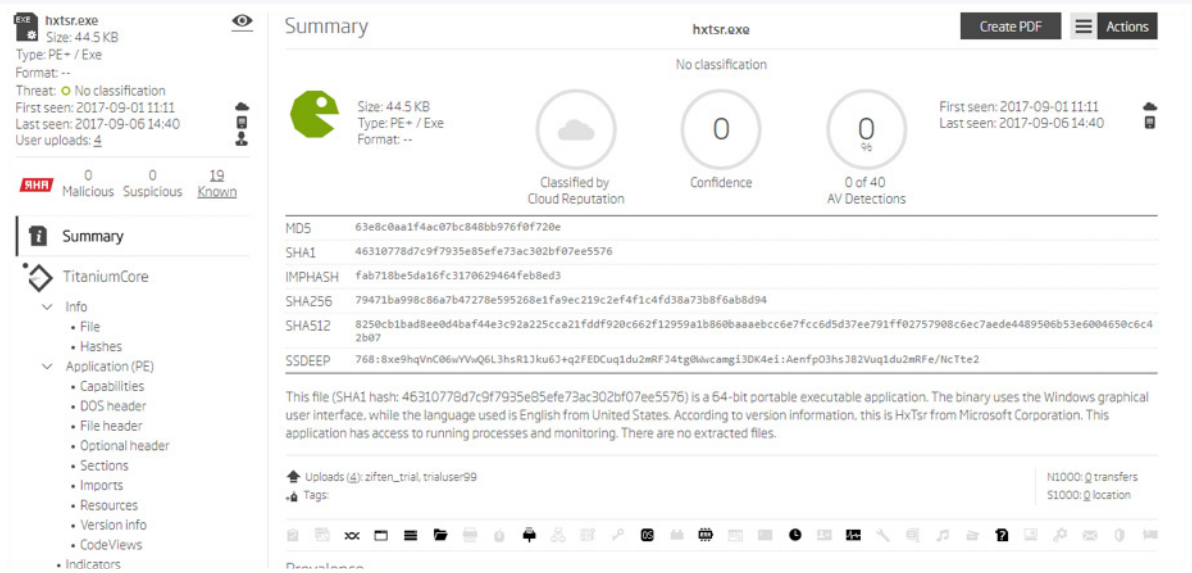


Figure 8 – Reversing Labs Report

Similarly, from the Reports screens, we can start with a high level view and continue to drill down into minute detail, such as with binaries flagged up as suspicious. Here we can also subscribe to that report, designating an administrator to receive that report on regular basis – for example, daily, weekly, or monthly, and at what time of day.

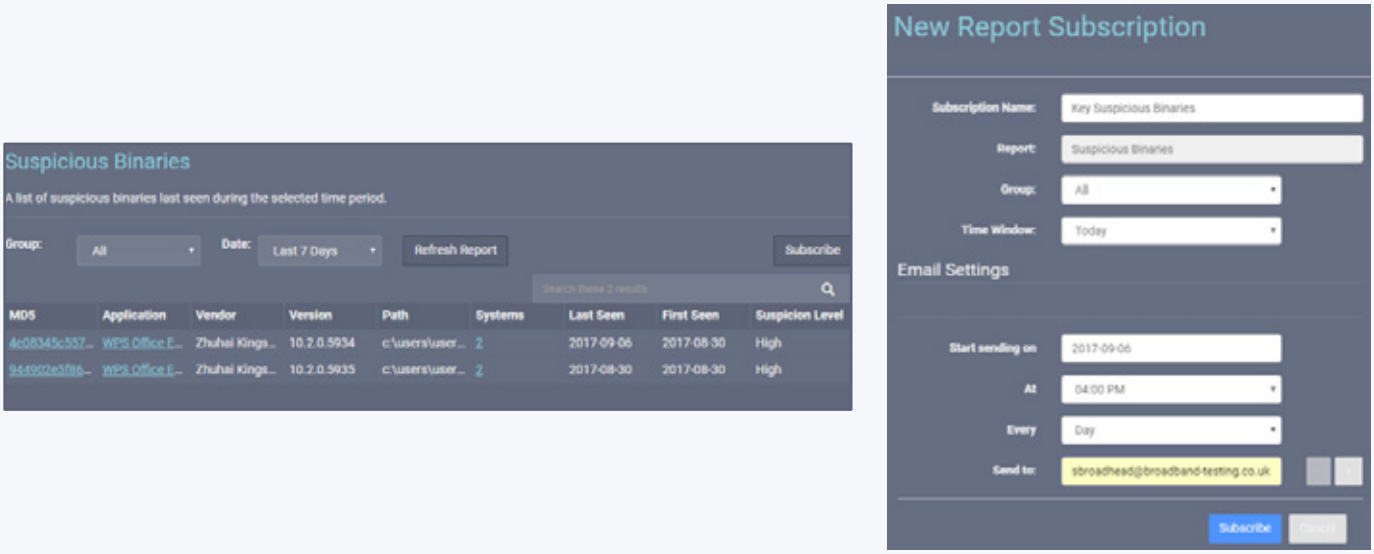


Figure 9 – Subscribing To A Report

Similarly we can sign up to receive alerts by email based, for example, on severity. A large number of alert rules are pre-configured (within the Tools Section) which can also be customised. As part of the test, we created GET URL lists to generate potentially dangerous websites, notably with an https connection, so we had all "443 Destination Suspicious" alerts routed to the administrator's email inbox:

Application	Destination IP	Direction	Is Connection Successful	Source IP	Version
Compatibility Telemetry	40.77.226.249	outcoming	true	192.168.1.162	10.0.15156.1008
Host Process for Windows Services	40.77.226.249	outcoming	true	192.168.1.162	10.0.15063.0
Edge Content Process	151.101.62.2	outcoming	true	192.168.1.163	11.0.15063.483
Host Process for Windows Services	40.77.226.249	outcoming	true	192.168.1.162	10.0.15063.0
Outlook Communications	13.107.13.88	outcoming	true	192.168.1.163	16.0.8400.0

Figure 10 – Receiving Alerts By Email

Under the Objects menu option, you can access all captured data for: Binaries, Applications, Systems, Users, Destination IPs, Hostnames and Client Failures. Here is where the integrated, interactive search and filter engines can clearly come in extremely useful, not just for ad hoc searches, but because you can also save any filters you create, which use Boolean logic to generate sets of rules:

Figure 11 – Creating Search Filters

The general search engine uses similar logic and also enables you to save and reload search definitions. Within the Objects sub-menu, under Systems, here is where you can get pro-active. Part of the extensive data provided here is a table of processes. Clicking on a Process ID produces a Process Tree view, from which you can specify actions on a particular process. Actions options are relevant to the particular case, but can include, killing a process, deleting a file, restarting a service, editing a registry key, quarantining an entire system from the network or ejecting/disable a USB drive. Each of these actions can be automated or implemented manually.

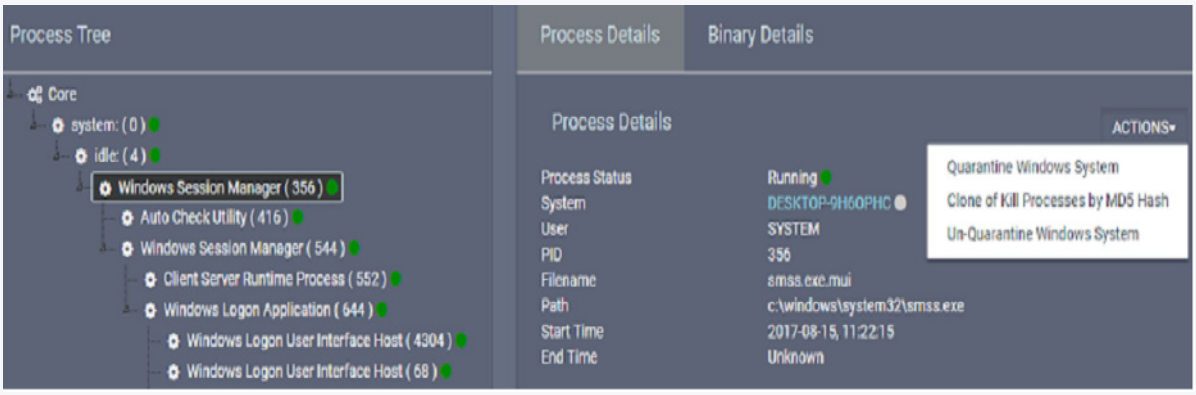


Figure 12 – Actions Example

Additionally, Ziften provides what appears to be a unique concept within the genre of extensions; essentially these are for custom data collection or execution of actions and allow for the execution of PowerShell and Bash scripts, maintained and signed by Ziften. A number of extensions are available by default but a customer can create their own and make them all actionable, so extending the pro-active element of the Ziften solution. Overall, a wealth of information is available, and with the means to act upon potential issues, as well as investigate historical problems.

ZFlow

ZFlow is a separate element of the Ziften offering, specifically for customers that already use NetFlow analytics, either for network performance management or security management. ZFlow provides extended NetFlow data from each endpoint at the edge of the network, designed to significantly improve existing NetFlow analytics, eliminating dangerous blind spots in the process. The primary problem here is that because NetFlow is typically collected at network choke points, it leaves lots of blind spots at the edge of the network, and in the DC.

With ZFlow, Ziften is able to generate extended NetFlow feeds from the edge of the network – or each deployed endpoint agent – to augment and extend the visibility of these existing NetFlow analyses. It provides traditional network flow data in the IPFIX format, ZFlow extends the data fields provided and adds contextual data such as, the application that initiated the flow, the actual process executable and its hash, the process identifier, parent process, command line entry and the logged in user, and user launching the executable.

Importantly, this gives a user fast access to data they normally have to chase down manually, which is excessively time consuming. In addition, because ZFlow data is looking at all network connections from the edge of the network and not from these internal choke points, ZFlow provides NetFlow analytics users additional visibility such as what's happening in local network domains and wireless domains, and at the edge of the DC, meaning all east-west traffic is easily viewed and analysed. Additionally they can see all cloud network traffic with their existing NetFlow tools.

Ecosystem Considerations

A point we need to make is that Ziften isn't designing itself to be a complete, self-contained security solution from an analytics standpoint; that would be frankly unrealistic.

Realising that customers have many existing elements in place, the focus is to be completely open with its collected endpoint data, with the ability to share it with any other analysis tools already in use. In other words, the product is designed to integrate with an existing security ecosystem to extend the capabilities of those existing tool and be wholly complimentary. The Ziften focus is on conducting endpoint-based analytics so, given that many customers will have other threat detection tools and higher level analytics tools in place, the aim is t o incorporate Ziften into that existing security and analytics ecosystem and add value in doing so. For example, this might involve data sharing with the likes of ticketing and orchestration systems for workflow management, 3rd party vulnerability assessment and patch management systems, SIEM tools for analytics, malware analysis and sandboxing tools for real-time, dynamic binary inspections, and endpoint firewall tools for quarantine and response duties.

To this end, Ziften provides a complete External API functionality, which can be managed from the console. Ziften allows you to share raw data, not just metadata. The overall idea is to help customers get more value from their existing security investments through access to the endpoint visibility data Ziften provides access to.

Realising that customers have many existing elements in place, the focus is to be completely open with its collected endpoint data

Ecosystem Customer Feedback Examples

Vulnerability Scanners

- Ziften has seen several customers planning on/replacing their vulnerability scanning solutions with Ziften due to its "just enough" approach being sufficient without over-complexity.
- In the tested version of Ziften Zenith (v5.1), the product detects vulnerabilities for the top 150 (but this number is growing rapidly) applications across its supported OSs in real-time, as applications are seen on their endpoints. So there is no scanning or waiting for an alert required.
- Ziften reports that in Zenith v5.2, the product continuously detects vulnerabilities for all installed applications. The company reports it has completely reversed its vulnerability detection technique such that all known vulnerabilities in NVD are continuously detected on all installed applications.

SIEM Integration

- While general SIEM integration (sending alerts) is valuable, Ziften has seen significant interest in integrations where it sends all or most of its data to the SIEM. Examples include: Splunk (all data, including ZFlow) and QRadar (a large subset of its data, including ZFlow). This has been of great interest to its MSSP customers, not simply native Splunk/QRadar users.
- Rather than have to pivot from their "single pane of glass" view of the network, customers using those advanced SIEM integrations get to stay within their SIEM console realm, as the Ziften data is already there.

Network Visibility

- Ziften's view into endpoints (using both Zenith and ZFlow) provides a unique perspective into network visibility that its customers are using for incident response (IR), forensics, compliance, and network monitoring.
- Whether directly integrated or living side-by-side with network solutions (firewall, netflow, DDoS appliances, etc), Ziften's "last-mile" visibility provides the context that network technologies natively cannot.
- IR teams use Ziften for alert triage of their network solutions; the Ziften endpoint context helping to reduce the false positives that are typically caused when only looking at the network alone, without the context of what caused that network alert. Example: customers are flooded with command and control (C2) IP alerts. However, in reality a large portion of these are IPs with many (often thousands) of hosts and, when looking at the endpoint process responsible for connecting to the C2 IP and identifying it as a browser, the alert can be lowered in priority as it is far less likely to be due to a threat, rather than an IP collision and poor IP threat intelligence (which is extremely common).

Malware Analysis / Sandboxing

- One of the key Ziften integrations involves its file collection capabilities with various malware analysis/sandboxing solutions. Examples: Palo Alto Networks WildFire, Blue Coat (now Symantec) Malware Analysis Appliance, VirusTotal, Fortinet's FortiSandbox, and ReversingLabs' A1000.
- Since Ziften is on the endpoint, it sees many files that are not observed by the in-line network tools. Example: It sees files that are sent via encrypted traffic, files that come in via a USB connection and files that are sent while the endpoint is offline and therefore invisible to in-line tools.

In Conclusion

The emergence of SysSecOps – combining systems and security operations – is a rare moment in IT; a hype-free, common sense approach to refocusing on how systems and security are managed inside a company.

Key to Ziften's endpoint approach in this category is total visibility - after all, how can you secure what you can't see or don't know is there in the first place? With its Zenith platform, Ziften has a product that ticks all the SysSecOps boxes and more.

Deployment is simple, especially in a cloud-based scenario as tested. Scalability also looks to be excellent – the biggest customer deployment to date is in excess of 110,000 endpoints.

Data analysis options are extensive with a huge amount of information available from the Ziften console - a single view of the whole endpoint infrastructure. Any object can be analysed – e.g. Binaries, applications, systems – and, from a process, an action can be defined as an automated function, such as quarantining a system in the event of a potentially malicious binary being discovered. Multiple reports are pre-defined covering all areas of analysis. Alerts can be set for any incident. Additionally, Ziften provides the concept of extensions for custom data collection, beyond the reach of most vendors.

And with its External API functionality, Ziften-gathered endpoint data can be shared with most 3rd party applications, thereby adding further value to a customer's existing security and analytics infrastructure investment.

Overall, Ziften has a very competitive offering in what is very valid, emerging IT category in the form of SysSecOps and one that must be on the evaluation short-list.

Ziften-gathered endpoint data can be shared with most 3rd party applications, thereby adding further value to customer's existing security and analytics infrastructure investment.