Where ZoneFox Can Support Your Security Ecosystem

ANALYSE. DETECT. RESPOND.

Contents

01 **Robust security** isn't an island

03 The security **Triad**

06 An Example **Deployment**

14 **Conclusion**

Robust security isn't an island

Robust information security is not delivered by a single product or vendor-provided technology. A strong security posture is, however, established through a combination of technical solutions, a clearly defined process, and employee awareness and training - all working together to provide defence against the full spectrum of threats, from advanced malware to social engineering attacks.

Your security strategy starts with the measurement of risk undertaken through the analysis of threats and vulnerabilities that are specific to your business. Once these threats and vulnerabilities are understood, mitigation is achieved through a range of countermeasures.

There are a plethora of different products and vendor offerings on the market. All of these need to work together in order to provide your organisation with a layered defence to reduce business risk to an acceptable level.

This white paper will provide insight into how ZoneFox is deployed alongside existing business security solutions to detect, audit and report on events which may have compromised an organisation's security.

The security **Triad**

Information security at a strategic level is commonly defined by the "CIA" Triad - Confidentiality, Integrity and Availability.

Depending on the nature of the business, various risks are mapped against CIA. Is a theft of Intellectual Property the most damaging? What about tampering with a critical system? Or, perhaps a Distributed Denial of Service attack on your E-Commerce site? Depending on what the identified risks are, a business looks to technological products alongside process and awareness training to deliver information security that's essentially tailor-made for the organisation's unique risk profile. In information security, one size does not fit all.

There are a number of frameworks and ways of defining information security requirements, some of which are very complex, such as the US National Institute of Standards (NIST) 800 series, and others that are very straightforward, such as the UK Cyber Security Essentials.

The following list outlines the main capabilities you require in your organisation in order to provide effective information security:

Assessment Creating a robust information security solution to address business risks comes from understanding the business data. Mapping the data processes - including the systems and people that store, process and transmit data - will provide insights into what solutions are required. Significant penalties from regulatory agencies exist for failing to protect certain kinds of data. Assessments determine what data is most important and, by association, what systems are most important ... and, by extension again, which people interacting with that data and those systems may require enhanced protection.

Prevention All too often in information security through technology, solutions become the central fixation within the organisation, commanding the most significant portion of the information security budget. Clearly, cybercrime statistics, stories of insider threats and armies of botnets blasting DDoS attacks tend to feed this fixation. Preventative technologies and information security best practices are vitally important, but crucially need to be aligned with mitigating the business risk.

Detection & Investigation Data breach detection and investigation appears to be the most neglected component of robust information security. Placing too much faith in the preventive solutions, including awareness training, frequently fails to provide the organisation with adequate protection.

Verizon's 2016 Data Breach Investigations Report indicates that in 93% of cases where data was stolen, systems were compromised in minutes - or less. But, in over 80% of cases, victims didn't find the breach for weeks or more. Giving the cybercriminal unfettered access to the entire infrastructure for weeks is less than optimal for information security.

Reaction Reaction can only occur only after an incident has happened - and is discovered - and the "Who, What, Where, When and How" of the security incident are known. There is, after all, always a danger in reacting without understanding the full scope of an incident. Over-reaction could call into question question the credibility and capabilities of the security team. Under-reaction could lead to accusations of negligence, or worse - a cover up. Either way, when the organisation is plunged into a security crisis, the folks involved have only one chance to react appropriately and to react properly. Vital information about the incident is needed, and it tends to be needed very quickly.

Recovery Recovery from a data breach or security incident is completely multi-faceted, and perhaps involves a much wider audience than just the business. If the discovery and reaction are linked, then recovery provides the "lessons learned," , and a vital plan of “how we insure the incident never occurs again.” Perhaps the failure was a user mistake, or a technology gap. It's important to address the internal aspect, but if the incident was reportable, or notification to clients was necessary, they need to understand what happened and what steps are being taken to make sure it does not happen again.

An Example **Deployment**

The architecture depicted below shows the information security configuration of an example organisation. In this example, a number of typical security solutions found in many organisations are described. The business may select any number of vendor products to mitigate the risks unique to the business.

1 Vulnerability Scanning
2 DDoS Protection
3 On-Host application whitelisting
4 Endpoint backup
5 Managed anti-malware
6 Data loss protection
7 Authentication and encryption
8 Email filtering
9 Network segmentation and firewalls
10 Malicious Activity Detection and Digital Forensics with ZoneFox
11 Security Information Event Manager (SIEM)
12 Identity Access and Access Management (IAM)

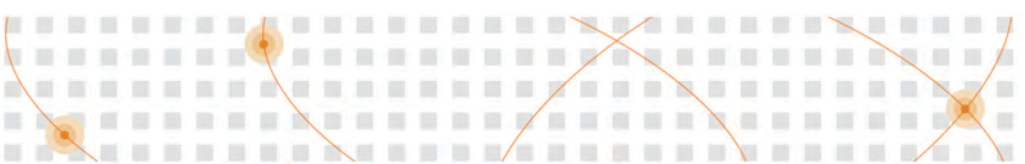
1 **Vulnerability Scanning** Always found in the top mitigations against cybercriminal drive-by downloads, malicious adverts and web links, is patch management. Finding and patching out-of-date software is a perfect opportunity for an automated tool. Exploit kits, a type of cybercriminal software, rely on out-of-date software to infect endpoints. Given recent SMB V1 attacks, vulnerability management has become an organisational priority.

2 **DDoS Protection** Many business are now investing in technology to protect from a DDoS attack, which renders external access to the Internet, or access to hosted or cloud services, impossible. If the business can't survive a prolonged outage from the Internet, DDoS protection is highly advised. Cybercriminals are using vast armies of compromised IoT devices and hijacked systems to flood businesses with unwanted traffic. Frequently, attempts to extort a ransom are made in advance of a DDoS attack.

3 **On-host application whitelisting** This technology has been included in the Windows Operating System since Windows 7 and Server 2008. Microsoft calls this technology 'AppLocker,' and there are other similar technologies available in the market place. The concept is to expressly authorise applications to run on endpoints and prevent anything else from running. This is also one of those technologies that have been highly effective against cybercriminal Trojans and credential stealing-malware - frequently installed on endpoints as a result of compromise.

4 **Endpoint backup** Backup is the "must-have" business security solution. With the rise of crypto-locker payloads, robust backup has become the primary and last-ditch way of avoiding to pay a Bitcoin ransom. Backup provides a business with a wide range of recovery options due to user mistakes and contractor/staff error. More sophisticated products also include virtual recovery options to bring the business systems online if physical hardware is damaged.

5 **Managed anti-malware** This has been the de facto go-to standard for business information security. Sadly, even with advanced sandbox, heuristic and behaviour-based capabilities, it would appear from industry analysis of cybercrime that these products as a risk mitigation strategy leave a business wanting and minimally protected. Clearly, some vendors are better than others, but the consensus opinion is that more layers are required than even the most advanced anti-malware products.



6 **Data loss protection** Data Loss Prevention (DLP) technology sets up many rules about how users can interact with files and data in the organisation. Although the technology has advanced over the years, with the advent of cloud services and cloud storage DLP has struggled to manage these remote locations. Perhaps the most difficult part of a DLP solution is the initial configuration and identification of where the data is located in the organisation. Adjustments to the rules of a DLP system can be an extremely arduous task.

7 **Authentication and encryption** Robust user identity services such as Multi-Factor Authentication go a long way in ensuring integrity of the systems, and provide a detailed audit trail of authenticated access. These are must-have features in the case of regulated finance or healthcare industries. When combined with a password manager these technologies make it difficult for cybercriminals to leverage stolen user IDs and passwords. Ubiquitous encryption for data at rest remains a strong risk mitigation strategy against the loss or theft of mobile devices. Given it has been included in the full version of Windows Vista and Windows 7 forward, it seems negligent to encounter an unencrypted laptop.

8 **Email filtering** Email filtering is one of the fastest-growing security technologies, and rightly so. It's estimated that 60% to 70% of data breaches and ransomware outbreaks are directly attributed to a malicious phishing email. Although the technology is not flawless, it extends the perimeter of defence - often to the cloud or a dedicated appliance - and provides a good chance of intercepting malicious email before it arrives at an endpoint and tempts a user to click.

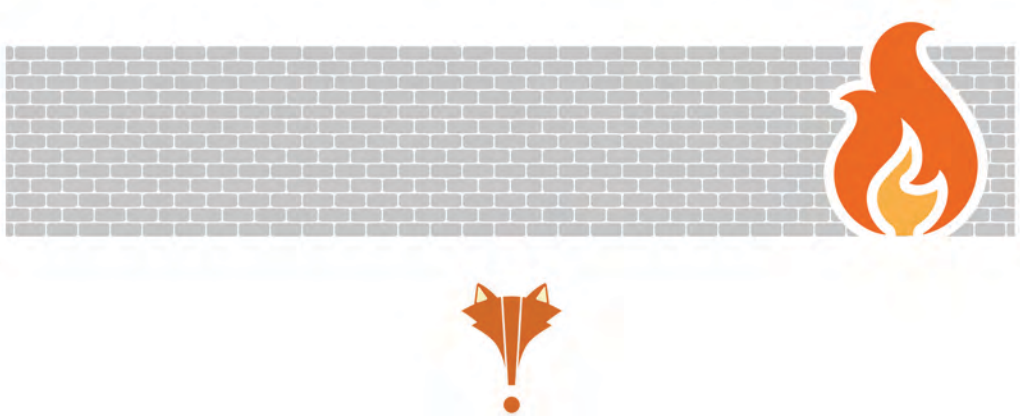
9 Network segmentation and firewalls

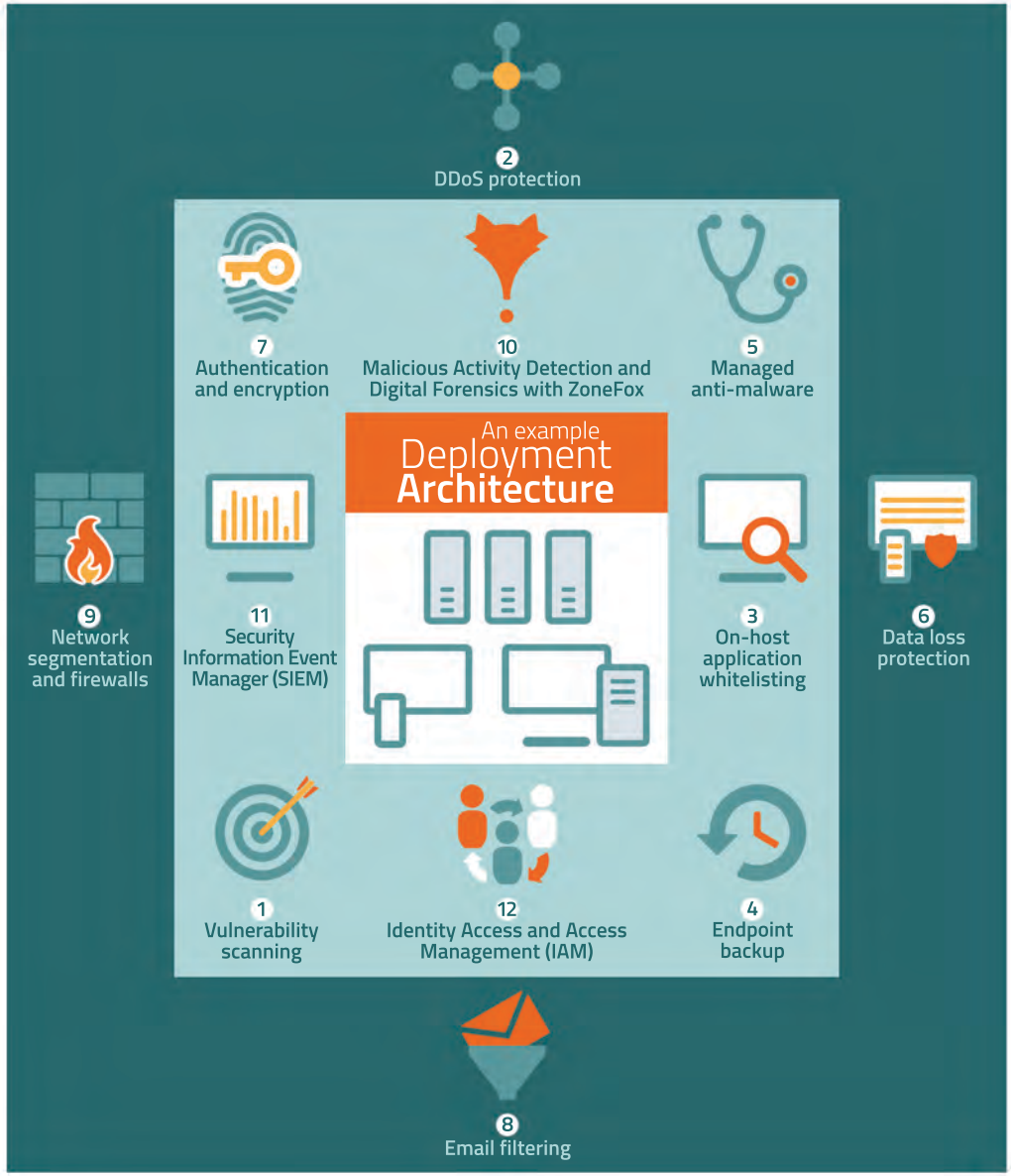
Network segmentation to prevent lateral movement by cybercriminals who have gained unauthorised access to a workstation, or to contain the spread of ransomware, has become a necessary mitigation step found in many organisations.

Due to the arrival of IoT devices, personal devices, and requirements to isolate protected environments such as finance, development or human resources, VLANS remain an excellent way of controlling access to network resources.

The traditional role of firewalls was to prevent bad things from making their way into the network. Now the emphasis is on controlling what can make it out to the Internet from i*nside* the network. This is due to how cybercriminal Remote Access Trojans (RAT) work. Once established, the RAT tunnels out to the Command and Control infrastructure. As such, taking an aggressive approach to controlling outbound data on ports and services, in addition to restrictions on inbound data flows, establishes the firewall as another security layer.

Interestingly, the firewall's logging and alerting capabilities can be used to detect attempts to exfiltrate data. As an example, if FTP or IRC protocols are not used in the business, attempts by these known protocols to move across the firewall from inside the network to outside would be blocked (if, of course, there is a rule), the attempt logged and an alert sent.




2
DDoS protection
7
Authentication and encryption
10
Malicious Activity Detection and Digital Forensics with ZoneFox
5
Managed anti-malware
An example
Deployment
Architecture
9
Network segmentation and firewalls
11
Security Information Event Manager (SIEM)
3
On-host application whitelisting
6
Data loss protection
1
Vulnerability scanning
12
Identity Access and Access Management (IAM)
4
Endpoint backup
8
Email filtering

10 Malicious Activity Detection and Digital Forensics with ZoneFox

Malicious activity or risky behaviour can manifest in many ways. ZoneFox's capabilities provide the business with the assurance policy that procedures are being followed and the deployed security technology is working. Frequently, users can and will make mistakes and ZoneFox assists an organisation by making sure users are following the established rules. As an example: if the business has decided that USB drives are not authorised for use, ZoneFox will detect when files are written to such a device and alert immediately.

ZoneFox takes an incredible leap forward when it comes to understanding what normal activity is. Utilising Artificial Intelligence (AI) with Machine Learning, an organisation can quickly spot a change in user, endpoint and network behaviour. From the AI perspective, the download of a new program never seen before, or the creation of a large .zip file using data not normally interacted with, will trigger an alert - which needs to be investigated.

The value of ZoneFox in an organisation is simply this: ZoneFox will give you the "Who, What, Where, When and How" of a security incident, providing a powerful digital forensic investigation capability. This capability quickly allows the business to respond appropriately by having clarity around the facts of a security incident. And, by knowing the facts, you can make smarter security decisions that strenghten your security posture and support the meeting of regulatory compliance.

11 **Security Information Event Manager (SIEM)** The SIEM aggregates and correlates log information from devices and systems in the network making it a powerful tool for examining a stream of data for activity that indicates a potential security incident. Unfortunately, due to network bandwidth limitations and complexity of modern enterprise networks, the high signal-to-noise ratio potentially creates many false positives.

Unless a true commitment to responding to the SIEM alerts is mandated by an organisation, this technology tends to be ignored in favour of more AI and Machine Learning based SIEM solutions.

SIEM solutions do have a powerful role in an organisation both for compliance purposes and for identifying sudden changes in network behaviours. If the organisation has a multitude of business-critical IoT devices, then a SIEM collecting firewall and switch information may be the only way to ensure the integrity of those IoT devices. The SIEM provides a single location where these events can be collected and analysed, with alerts being generated if any behaviours are correlated from the multiple sensors that have been deployed.

12 **Identity Access and Access Management (IAM)** These technologies provide an excellent integrity layer, as they're primarily focused on "who" is accessing "what" - and apply rules to this access. This becomes important under compliance regimes applicable to healthcare, such as the HIPAA legislation in the U.S.

Certainly, this is a data-focused approach driven by a users "need to know" requirement for data access. These systems do a great job of access control, but provide little assurance the data is not being misused in other ways.

The technology is driven by data classification, and in larger organisations the classification process alone could take a significant amount of time and effort. In smaller organizations where individuals are cross-functional, the role of the individual may need almost complete access to all the organization's data.

Conclusion

As you can see from this brief survey of the security ecosystem, analysis of the more-common technological solutions suggests that they all have merit when it comes to security, with many of the technologies discussed provided by vendors who may cover more than one risk mitigation strategy.

ZoneFox stands apart as one of the few detective technologies that can tell the whole story when it comes to the "Who, What, Where, When and How" around your data, enabling you to determine the appropriate response. If you'd like to find out more about how ZoneFox can help you to work smarter, secure sensitive data and meet regulatory compliance, **contact us!**

Like to Learn More?

zonefox.com
youtube.com/zonefoxvideo
@zonefox
alerts@zonefox.com

40 Torphichen Street
Edinburgh
EH3 8JB
0845 388 4999