ZoneFox

Whitepaper

How ZoneFox Fits into your Security Ecosystem

Overview

Information Security is not a single product or vendor, nor is it just a set of technologies. Fundamentally, security involves the measurement of risk through understanding threats and vulnerabilities that are specific to your business, and deploying suitable countermeasures to mitigate them. Information Security is a process requiring technical; policy; business; awareness; training; and other factors to work together.

Similarly, there are a number of different products and vendor offerings on the market that need to work together in order to provide your organisation with complete coverage. The aim of this whitepaper is to provide you with an insight into the types of technology solutions and products that can be deployed alongside ZoneFox as other vital pieces of your organisation's completed security puzzle.

The Security Triad and Information Security Capabilities

Before we outline the main product areas, we need to fully understand the main aims and objectives of deploying any information security product. These objectives are covered by the classic triad of security principles which are; Confidentiality, Integrity, and Availability of Data.

In order to achieve the objectives of the information security triad we require a range of products and capabilities. The following list outlines the main capabilities you require in your organisation in order to provide effective information security.

Assessment

How do you know what you need to protect and what you need to protect it from, if you don't know what the baseline is in the first place? This is where assessment tools fit in, allowing you to understand exactly the broad range of hardware, software, users, networks, and other assets in your organisation.

Prevention

This capability allows you to keep people out of your network and systems, as well as ensuring that Bob from HR isn't accessing Alice's documents in Engineering.

Detection and Investigation

Without adequate detection, you won't know when or where an intrusion occurs, or whether your organisation is currently free-from compromise, or the degree of the compromise. Both detection and investigation capabilities need to be timely and comprehensive. If a breach is detected but the alert isn't sent in a timely manner, providing the key data (for example which user or machine caused the incident) then the incident will go unnoticed. Similarly, if an organisation cannot fully uncover all the necessary data quickly and easily, the investigation will take too long and become expensive.

Reaction

Reaction is the ability to do something about a security incident. The reaction your organisation undertakes can include a wide range of strategies, from an immediate response automatically removing a malware infection, to an incident response plan involving multiple parties.

Recovery

Now that you've identified what went wrong, it's time to bring the system back to a known-good state. However, it's important to ensure that this configuration does not contain the same flaw that lead to the incident in the first place. For example, did the malware get backed up? Did the error in the system's controls get duplicated? This capability is benefitted by the work done by the others in this list, in the best case, they prevent the need for a recovery, in the worst cases, they help expedite the time it takes to get your data back and to start operations again.

An Example Deployment

The architecture shown in this section (Figure 1, Page 4) shows the information security configuration of an example organisation. The configuration takes into account each of the capabilities highlighted in the previous section.

Each of the different products deployed aid the organisation by providing capabilities to help them achieve their information security goals. The technologies in the example configuration include:

1 Vulnerability Scanning

In order to plug the holes in your system, you need to be aware of them in the first place. Vulnerability scanning allows you to scan the software and networks in your organisation to find weaknesses. For example, a scan may reveal that there's a flaw in a web server, which can be fixed through patching.

2 DDoS Protection

A denial of service will reduce or wipe out the availability of the services you offer. Protecting against this form of attack is therefore crucial.

3 On-Host application whitelisting

There are more types of application that could be deployed on your system than one can count. So, why not let users run the known, good, applications? This also allows you to ensure that running software is running the latest patch level, as well as keeping out malware.

4 End point back-up

How can you recover from a disaster if you haven't backed up your systems? Back-up tools are essential for this. Data and configuration backup form the foundations of a good strategy.

5 Dynamic Malware analysis

Modern malware is smart and hard to detect. Signature-only based approaches are no longer effective. This is why you need a capability that combines signature-bases approaches with real-time analysis of behaviour. Included in this mix is the ability to understand what files, apps, and webpages are trying to do to your end-points.

6 Application-layer firewall

This stops documents from leaving your organisation, and potentially going to unauthorised recipients.

7 Authentication and Encryption

These are two key approaches to ensuring the right people have the right access to the right information, and ensuring that those without authorisation are unable to view sensitive data.

8 Email Security

Email is a highly effective way to lose information from your organisation, as well as receive malicious files or software.

9 Firewalls

Perimeter access control ensuring no unauthorised access can occur in or out of the organisation. A classic yet essential requirement to maintain an effective border.

10 Data-level behaviour monitoring with ZoneFox

ZoneFox provides key insights into how critical data is used, drawing from Identity Management and Access controls in order to ensure that the right people are accessing the right data. ZoneFox can verify existing security deployment and policies by providing you with reports and alerts on actual behaviours that may be contrary to existing policies. Finally, if a breach occurs your organisation will have a full forensic timeline of all user behaviours that's easily and quickly accessible to provide rapid answers to reduce the cost of a breach and to stop it from happening.

11 Security Information Event Manager (SIEM)

Over the past few years a new class of product has emerged that allows an organisation to properly integrate and associate the many different outputs from the many different products on their systems. 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 you have deployed.

12 Identity Access and Access Management (IAM) technologies

These technologies allow you to properly configure and control user access to data.

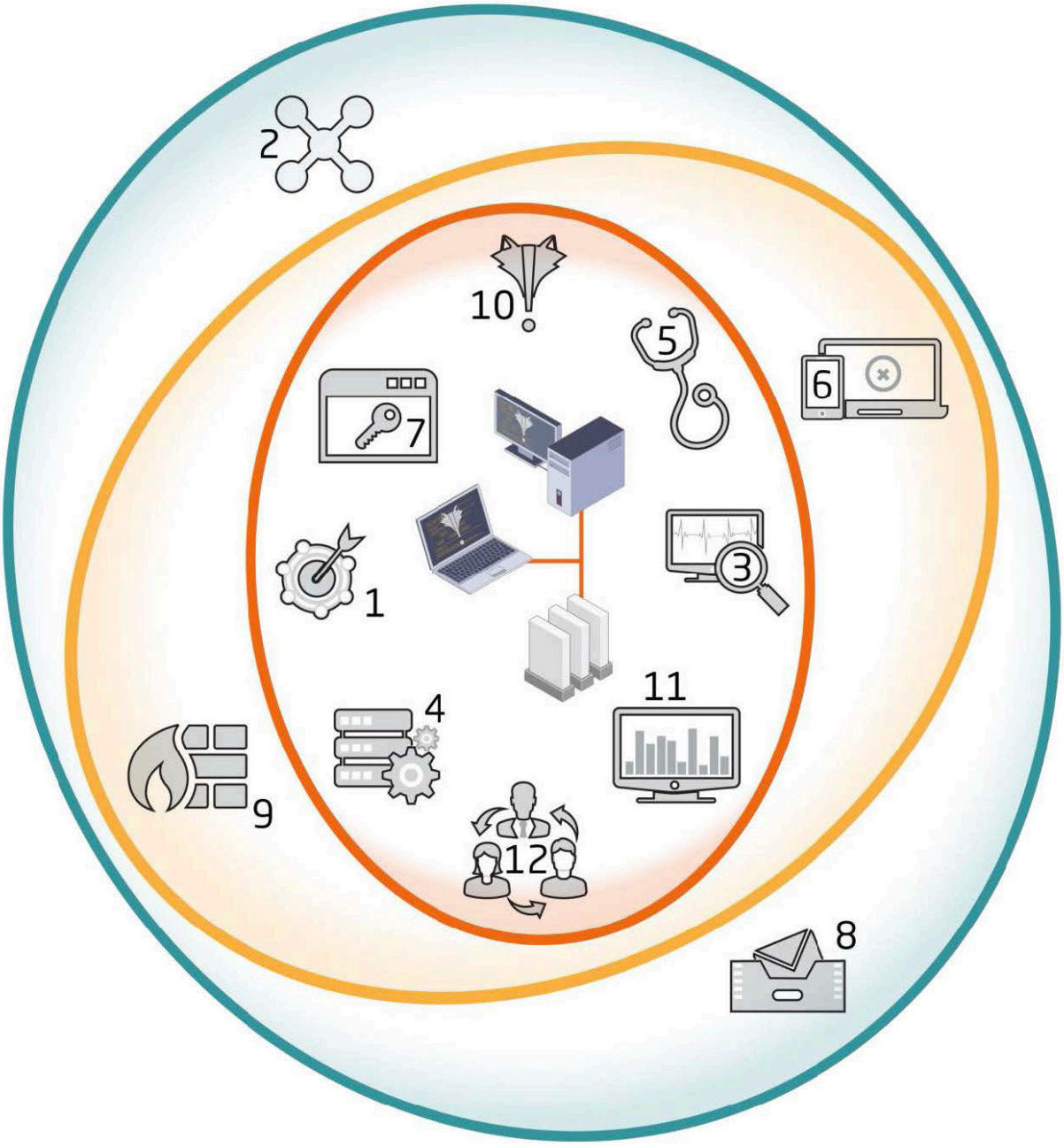

FIGURE 1 - EXAMPLE DEPLOYMENT

About ZoneFox

ZoneFox is a highly innovative Endpoint Monitoring & Threat Detection solution that helps our customers protect their business-critical assets: data and intellectual property (IP) from malicious and accidental insider threats. ZoneFox has a proven track record of protecting reputation, sales revenue, and competitive advantage by providing next generation data monitoring, security analytics and endpoint security.

Through its continuous monitoring capability, ZoneFox provides a unique perspective on user activity tracking. Our lightweight software agent, resident on each machine under surveillance, monitors user behaviour as a series of fine-grained events in real-time. This provides timely threat detection of data breaches, informing and facilitating a relevant response and enabling:

- Policy compliance monitoring
- Monitoring the effectiveness of security controls
- Protective monitoring of user risk
- Data and IP Protection