ZoneFox

Data Security by ZoneFox

Analyze. Detect. Respond.

ZoneFox

Powerful, intelligent, data security and threat protection

Identifying and responding to threats from innocent and malicious sources remains a complex challenge for organisations. This is not a challenge that can be ignored as regulatory requirements such as GDPR threaten large penalties for companies that cannot document, or do not have the capability to respond to, security events and data breaches.

ZoneFox is a unique data security and threat detection solution that delivers advanced threat hunting to help you spot, respond to and manage risky behaviours that put your business-critical data at risk. We combine powerful and flexible Machine Learning with detailed forensics around user actions to bring focus to the facts more rapidly that other solutions.

Our award-winning technology provides 360° visibility of activities around your data – the who, what, where and when – by monitoring user behaviour and data movement both on and off the network, and instantly alerting to anomalous activities. Security posture is strengthened, sensitive information is protected and regulatory compliance is supported.

Key Benefits of ZoneFox

- **Smart endpoint agents** result in a very low touch on system resources, with only endpoint meta-data collected.
- **Instant insights around your data activities** as agents collect data from the moment they are installed.
- **Real-time data processing and analysis** of user behaviour results in rapid incident response capabilities.
- **ZoneFox AI spots common and potentially unknown forms of malware and ransomware**, allowing rapid containment and clean up.
- **Compliance Reporting** linked with investigation tracking provides critical intelligence in one dashboard.
- **Rules-based engine eliminates false positives** and spots potentially dangerous user behaviour with even greater accuracy.
- **Learns what normal activity is at user, system and network layers** to provide 360 coverage of your environment and deep forensic capability.

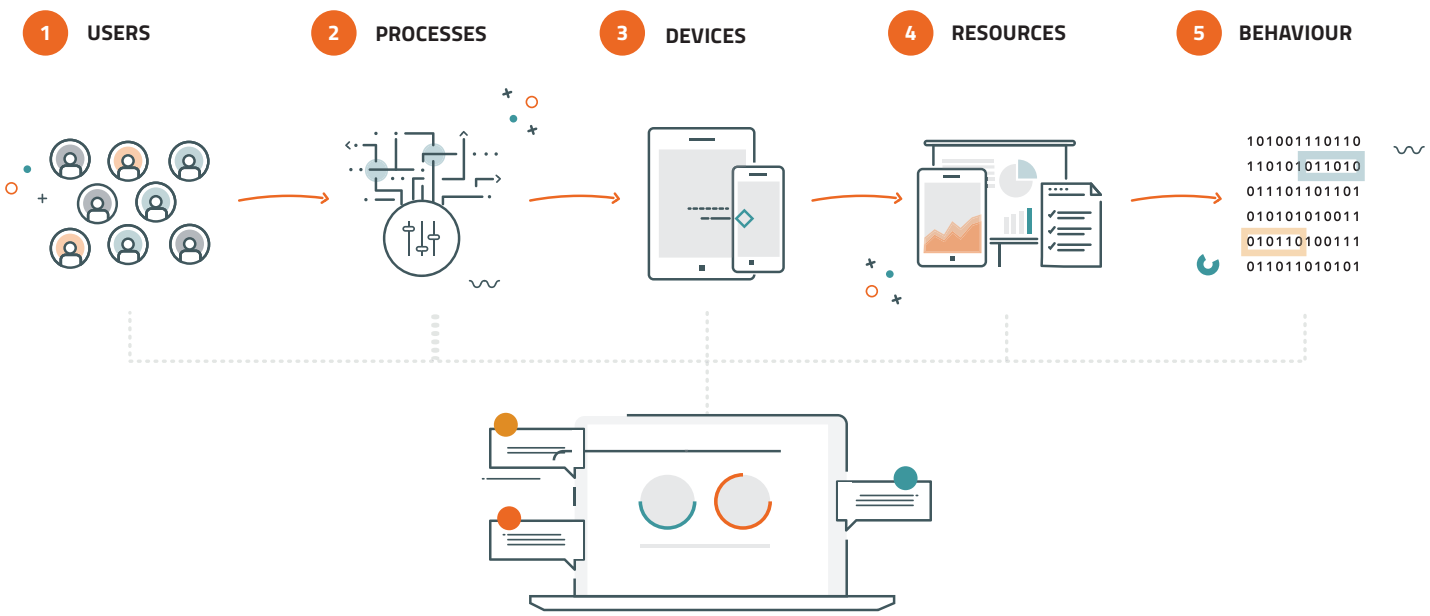
Key Features and Operating Information

- ZoneFox can be **deployed as a bespoke and customized solution on premises, private cloud or public cloud** as required.
- Smart Agent technology on the endpoint **provides visibility on files being moved through cloud storage applications,** Skype, Instant-Messenger, etc. complete with tracking of file names being moved through encrypted means.
- User and Entity Behaviour Analysis (UEBA), powered by rule sets and augmented with AI, **detects known and unknown threats** ranging from malicious insider activity to Advanced Persistent Threat Trojans and Malware.
- Recording of user, machine, application, file, behaviour and network destinations/source activities results in a **complete forensic level of detail for investigation and compliance** purposes.
- The big data storage architecture of endpoint meta-data allows for retroactive rules and the **ability to "go-back-in-time" to see past events** in the current context.
- The Smart Agent "store-and-forward" capability **reports on potentially suspicious activity when offline** eliminating network blind spots.
- Billions of endpoint events are collected, collated, and analyzed to provide **a complete timeline of user activity**, from patient "Zero" to the incident being investigated.
- ZoneFox uses the latest elastic search technology, giving you near **instant access to the information collected**. Who downloaded the payroll database? Has our company ever connected to that IP address before? How many people have a cloud sharing app installed? Rapid search capabilities gives a rapid response.
- Endpoint agents available for **Windows, Mac, Linux, SQL Server and Sharepoint** (local hosted version only).

How ZoneFox Works

The zero-config, lightweight agent installed on each system performs no analysis or preventative actions on the endpoint. Rather, the agent simply gathers and sends data for alerting or investigation. This 'smart agent' approach has significant advantages as it presents a smaller attack surface to sophisticated attackers, reduces performance drain on the endpoint, and allows configuration of each agent to send its data to a cloud-based service.

Unique Five-Factor Model



Best of Both Worlds

With ZoneFox, the sophisticated rules-based engine bolstered by smart machine learning ensures all activities are monitored on AND off the network. Rules are drawn up to agree what constitutes acceptable user activity. The rules are applied and if activity takes place that breaches these rules, an alert is sent to the administrator. This feature-set is also harnessed extensively to deliver insight into potential breaches around compliance regimes (such as GDPR) .

Our 'Enterprise' solution utilizes Machine Learning which examines behaviour around data - and data flow - to spot anomalies such as users who are acting out of character, for example, looking at files they don't normally seek out, or unusual changes in work patterns, compromised accounts or changes in peer group activities.

ZoneFox

	Core	Enterprise
Augmented Intelligence with Machine Learning Advanced UEBA platform, delivering real time, actionable insights into anomalous user behaviour around your business-critical data. Patented UEBA capabilities, plus Machine Learning (ML) enables your team to build comprehensive profiles of: ▪ Users ▪ Applications ▪ Peer Groups ▪ Files ▪ Endpoints ▪ Networks	●	●
Detailed Forensics Trail ZoneFox delivers a complete record of all user and machine activity so your team can respond rapidly to potential or actual breaches - essential for effective incident response, case-building, and of course, meeting regulatory compliance - particularly in complying with the GDPR 72-hour disclosure rule.	●	●
Endpoint Connector Gain complete visibility around data flow whether users are on OR off the network by creating a lightweight stream of user and machine behaviour from Windows, Mac, Linux, SQL Server and Sharepoint, as well as laptops and desktops.	●	●
Database Connector Track user access, data queries and database changes in real-time from your SQL server databases.	●	●
Visualisation and Dashboards Rapid set-up of ZoneFox charts, graphs, and dashboards the way your business needs them means visibility of the critical insights needed to manage your security operations workflow.	●	●
Standard Case Management Be ready to meet compliance. Forensics data at your fingertips when you need it - with no time frame on data storage. Gather alert and incident response data in case files which can then be used for thorough breach investigations.	●	●
Federated Security Assign multiple logins to different members of your team to assign alerts and incident response tasks.	●	●
Network Monitoring Gain valuable insights into where your data goes when it leaves your network. Find out what left your network, from where, and where it went to.	●	●
Compliance Reporting Dedicated Compliance Reporting to help support you to meet regulatory compliance such as GDPR, HIPAA, ISO27000 and FCA.	●	●

About ZoneFox

ZoneFox helps businesses around the globe protect their business-critical data against the insider threat. Our award-winning technology provides the 360 visibility of activities around your data – the who, what, where and when – by monitoring user behavior and data movement both on and off the network, and instantly alerting to anomalous activities.

Security posture is strengthened, sensitive information is protected and regulatory compliance is supported.

Like to Learn More?

zonefox.com

youtube.com/zonefoxvideo

@zonefox

alerts@zonefox.com

40 Torphichen Street

Edinburgh

EH3 8JB

0845 388 4999

ZoneFox