# ZoneFox

# ZoneFox Sample Proof of Value (PoV) Report

Valuable, actionable insights to help protect your business-critical data

**During your 15 day PoV, we identified:**

**130K** individual events

**6.4M** user actions

**3** cloud services used by 16 users

**5** tools associated with hacking in use

**14** high-risk users making use of removable storage

**110K** AI alerts that rules failed to trigger

www.zonefox.com

# EXECUTIVE SUMMARY

ZoneFox helps organisations around the globe protect their business-critical data against the insider threat. Our award-winning technology provides 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, business-critical information is protected and regulatory compliance is supported.

Our zero-configuration agent means the solution is plug-and-play, allowing for breakneck-speed deployment, and instant protection. In the past 15 days we have:

- ✅ helped you achieve elements of compliance with GDPR and DPA

- ✅ provided a full suite of tools to conduct security investigations quickly and effectively, offering a high-value, demonstrable ROI

- ✅ demonstrated that proactive alerts can help identify breaches, and highlight where potential breaches may occur - often allowing for prevention rather than cure

- ✅ worked across your entire suite of device profiles, offering blanket coverage and reliable, audit-friendly data

## ACTIONABLE INSIGHTS GENERATED BY AUGMENTED INTELLIGENCE



**Leaking your data?**
1 user zipped the contents of a networked shared drive, which is a common sign of data about to be leaked or sold to a third party.



**Playing Games**
AI has detected 3 users installing games using the Steam platform, and playing games on company machines during working hours.
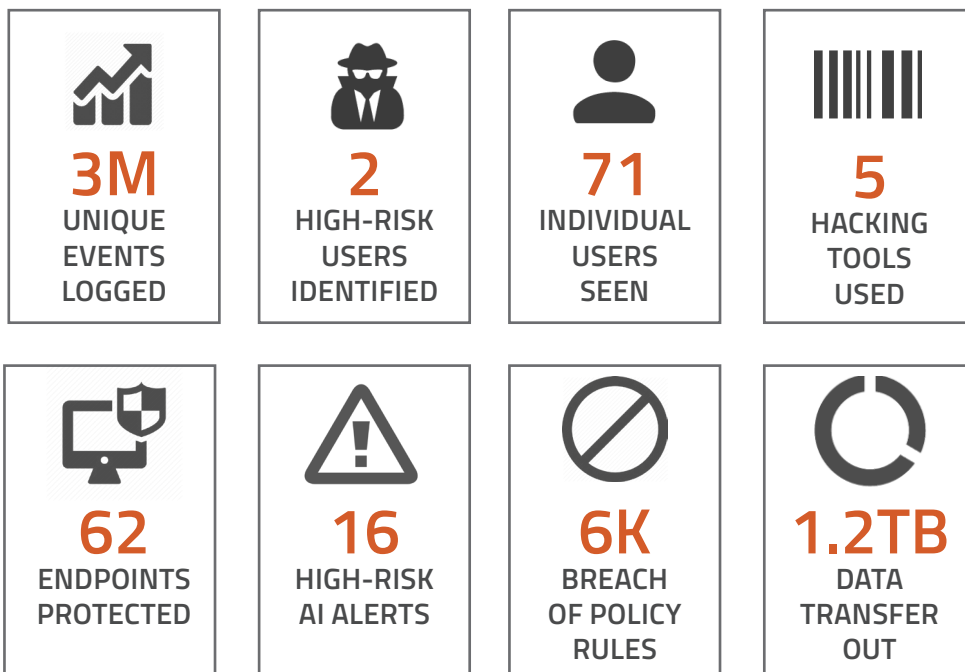


**Illicit movies**
7 users watched pirated movies on their computers during the PoV study, loading the films from USB sticks. Pirated movies can contain viruses.

Analyze. Detect. Protect

# YOUR PoV IN NUMBERS

ZoneFox is constantly monitoring your network and endpoints, with no need to manually "switch on" logging. All you have to do is install a zero-config connector, and ZoneFox does the rest.

During your PoV, ZoneFox discovered the following:

**3M**
UNIQUE EVENTS LOGGED

**2**
HIGH-RISK USERS IDENTIFIED

**71**
INDIVIDUAL USERS SEEN

**5**
HACKING TOOLS USED

**62**
ENDPOINTS PROTECTED

**16**
HIGH-RISK AI ALERTS

**6K**
BREACH OF POLICY RULES

**1.2TB**
DATA TRANSFER OUT

"If you don't know when your business critical data is moving around, you can't know that it's safe. ZoneFox solved this problem for us – quickly and efficiently."

Lisa Kerr
CEO Angelincore

## REDUCE YOUR COSTS

51% of medium-sized UK businesses have experienced a data breach in the past 12 months, at an average cost per breach of £36,500. With ZoneFox you can investigate and resolve in hours, not days - saving time *and* money.

Source: Cyber Security Breaches Survey 2016, HM Government/IPSOS MORI/University of Bournemouth

# ALERTS

Alerts are generated by the rule engine in ZoneFox, and are a key tool for identifying when security policies have been broken.

Below are some key statistics around the alerts fired during your PoV, and the rules created for you by the ZoneFox security experts.

## Top Rules broken during your PoV
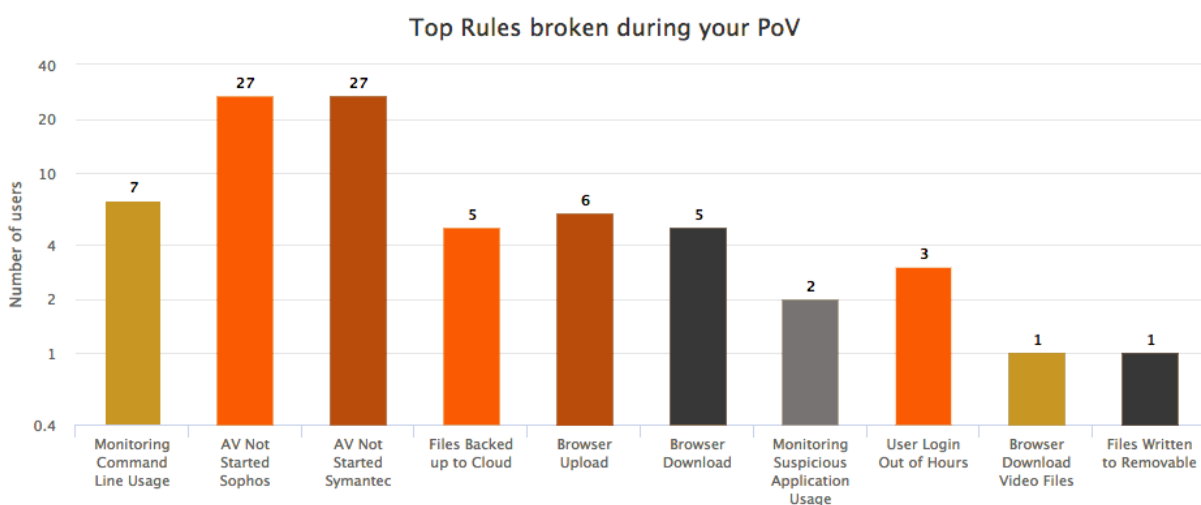


## INSIGHTS BROUGHT BY ZONEFOX ALERTS
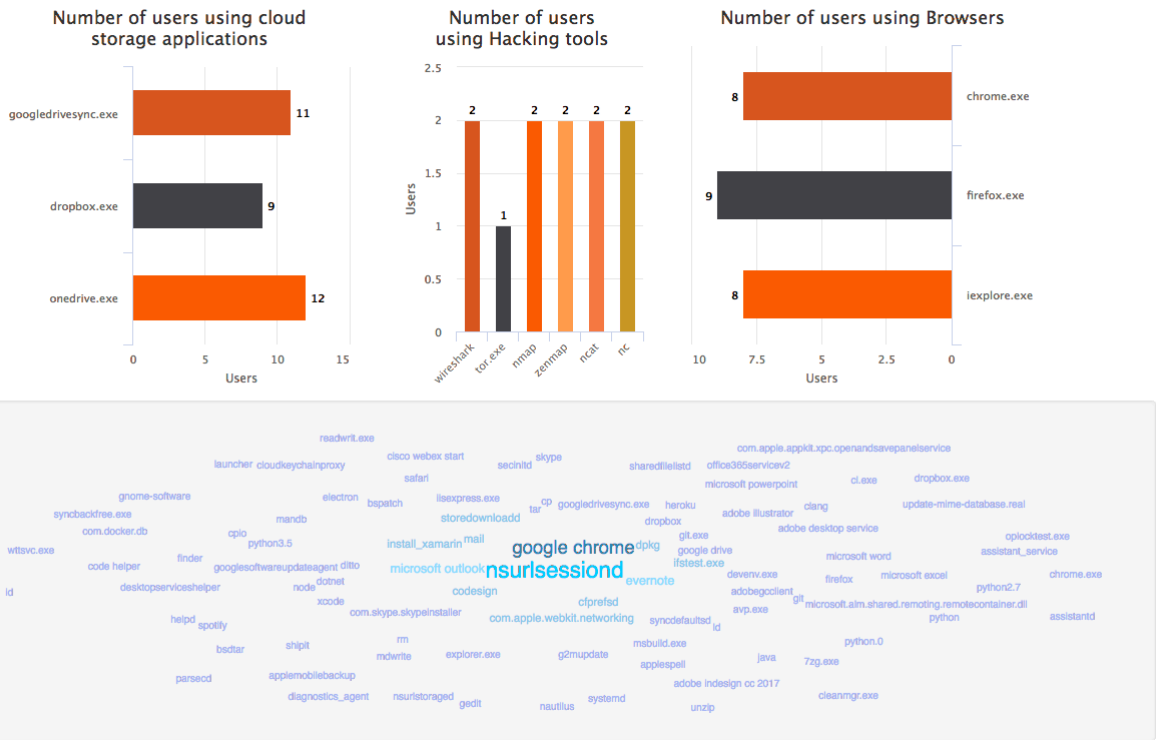
**6**
HIGH-RISK
USERS

**2**
HIGH-RISK
APPLICATIONS

## FOCUS YOUR RESOURCES

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. This allows you to focus your resources where it counts, reducing unnecessary and costly investigations.

Analyze. Detect. Protect

# APPLICATIONS

ZoneFox provides crystal clear visibility of activities around your data, whether users are on *or* off the network. Although alerts are powered by rules, rules aren't necessary for statistical analysis and incident investigation.

For example, during the course of your PoV, ZoneFox observed the following application usage, including some that fall outside of typical IT Security policies.



Number of users using cloud storage applications

Number of users using Hacking tools

Number of users using Browsers



**3**
CLOUD STORAGE
APPS USED

**1**
HACKING
TOOL USED

**3**
DIFFERENT
BROWSERS

**6**
USERS HAVE
FILES ASSOCIATED

# DATA FLOW

Increasingly, data flows across the globe in fractions of a second. A file that sits on a computer inside your secure network can be on the cloud, or shared by email, or sent via Skype ...

ZoneFox provides full visibility of where data has flowed from and to, without the need to install any additional hardware or configure extra proxies for web traffic. During your 15-day PoV ZoneFox protected your business by recording the flow of data in and out of your organisation.



Data Flowing In or Out of Test



Extensions
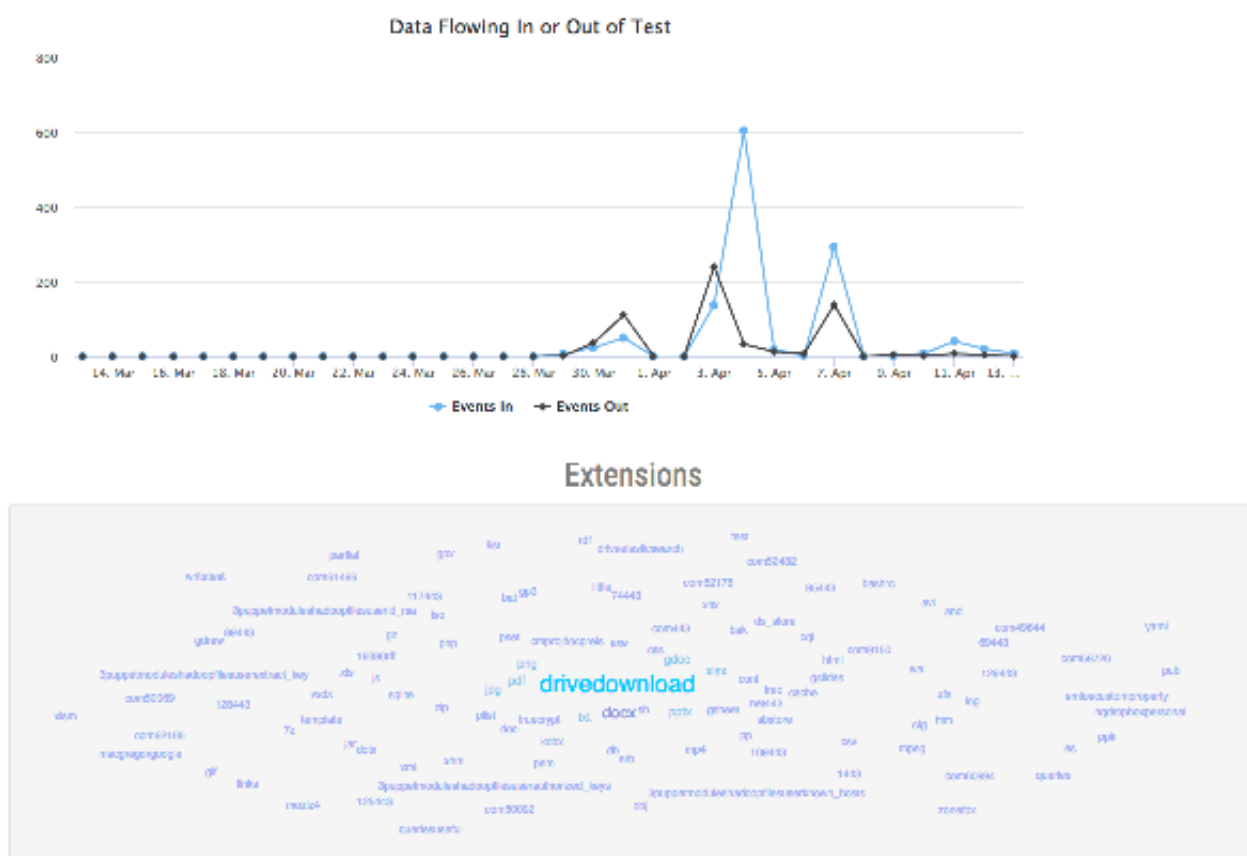
> ❝ If you don't know the movements of your business-critical data, you can't know that it's safe. ZoneFox solved this problem for us – quickly and efficiently. ❞

Analyze. Detect. Protect

# NETWORK ACTIVITY

Knowing that data is leaving your network is useful, but knowing where it's gone can be crucial if you're to keep hold of your intellectual property, protect confidential records, and ensure compliance with privacy, data-handling, and security legislation.

ZoneFox provides a suite of tools that help you monitor and track data movement across the world, so you can clearly identify where your data has gone.



| 24.88 GB | 12.49 GB |
|----------|----------|
| HAVE BEEN UPLOADED | HAVE BEEN DOWNLOADED |

## KNOW WHAT GOES WHERE
Gain valuable insights into the When, Where, Why and What when it comes to data flow around your network - no more guesswork.

# FORENSIC ACTIVITY

One of the downsides of typical solutions for monitoring use of IT systems is the need to create rules. Technology and software can iterate at a tremendous rate, making it difficult to keep rules up to date all the time.

ZoneFox negates this issue by using a Zero-Configuration Connector which collects and stores all activity, allowing for later forensic analysis and exploration in the event you need to get to the detail of what happened.

Take a look at a selection of the metrics ZoneFox gathered during your PoV below:



Frequency of users logging in or out

— user logins   — user logoffs
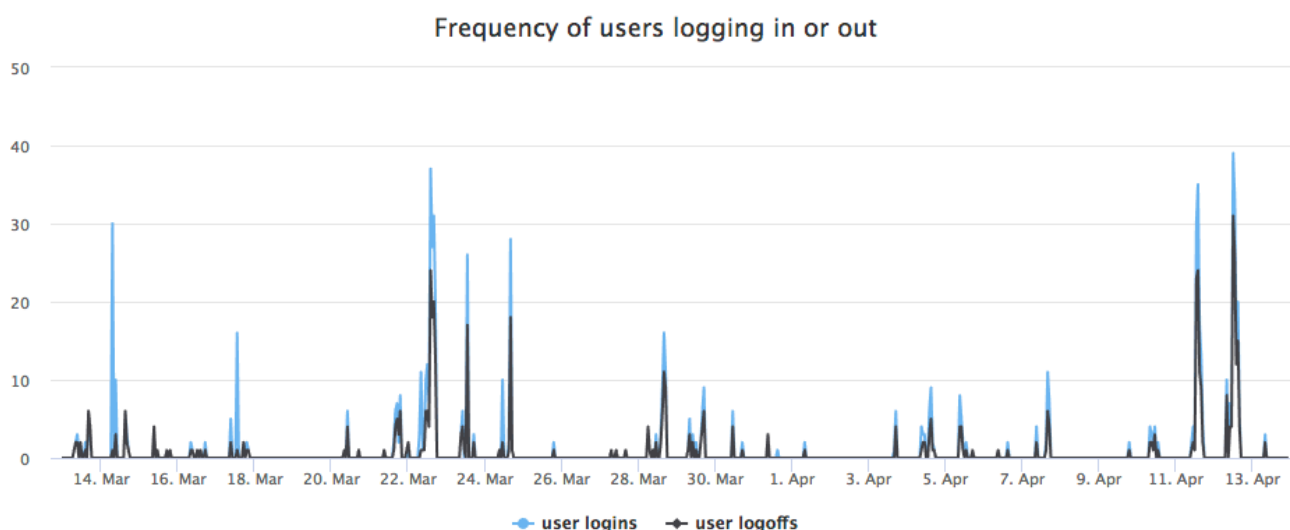
**AUDIT AND COMPLIANCE**
Gather alert and incident response data for case files which can then be used for thorough breach investigations and compliance reporting.

Analyze. Detect. Protect

## 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, business-critical information is protected and regulatory compliance is supported.**

## Like to Learn More?

ZoneFox.com

Youtube.com/ZoneFoxVideo

@zonefox

alerts@zonefox.com

Argyle House,

Edinburgh,

EH3 9DR

0845 388 4999