ZORB

Data Theft Prevention

easy, powerful, affordable

Hackers & Insider Attacks

Prevent data breaches from hackers, insiders & disgruntled employees

The likelihood of data theft from external hackers and internal bad actors has increased. Bad actors can easily acquire sophisticated attack tools, many of which are starting to incorporate AI to automate finding weak spots within an organisation. Fuelled by the ease of selling data on the dark web, or holding a business to ransom.

Attacks are increasingly becoming state-sponsored. Large hacking teams with access to state provided budgets are attacking businesses of all types and sizes for data and IP theft, or simply to cause disruption.

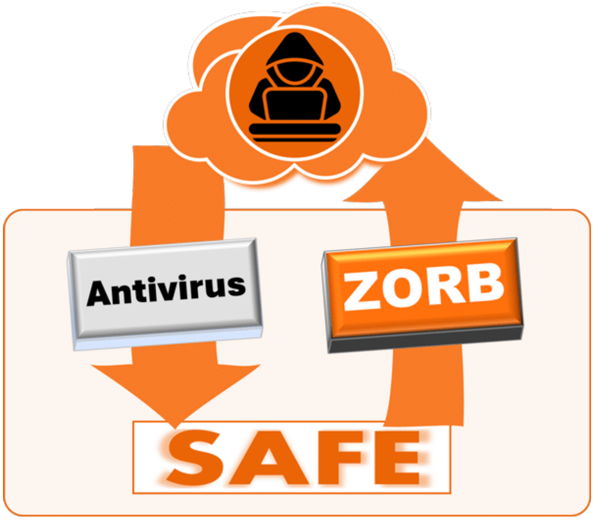
An insider attack is malicious activities initiated by trusted individual within an organisation. This might be a disgruntled employee, an opportunist contractor, or even lack of policy outlining a third-party's responsibilities.

The risk posed by insider threats is growing at an even faster rate than from hackers. So much so, that the threat of insider attacks now features in many CISO's top 5 concerns. Recent data indicates that more than half of organisations have encountered an insider threat within the past year, with 8% experiencing more than 20 incidents. 74% of organisations are believed to be vulnerable to insider attacks.

START TODAY
10 FREE licences
www.zorbsecurity.com/trial

Both external and internal actors are often motivated by financial gain. These bad actors aim to exfiltrate sensitive business data to either resell on the dark web or to hold the business to ransom. Insider threats can originate from various sources, such as employees, vendors, contractors, or partners who have access to internal systems and data.

Often, it is a trusted person with legitimate access to sensitive information during their normal course of work that perpetrates an attack. Some of the most common scenarios involves departing employees or contractors who steal confidential data, intellectual property, or trade secrets before leaving the organisation.



Prevention

It may not be possible to totally eliminate the likelihood of attack from a determined adversary. The correct strategy is to mitigate the opportunity for attack. An attacker only requires one vulnerability in the infrastructure, whilst a defender needs to plug every gap.

Effective mitigation of the risks form external hacker attacks and insider threats requires a comprehensive set of measures, including access control, data encryption, employee cyber awareness education, and more.

Despite best efforts in mitigating the likelihood of incoming attacks, at some point, a bad actor with access to the system will attempt to exfiltrate information. Now, the strategy can shift from mitigate to prevent.

Again, the attacker has the upper hand due to the multiple ways in which data can be extracted. Physical data extraction could involve a USB drive, or printed material. Digital extraction means transferring data over the internet to cloud storage.

ZORB specialises in preventing unauthorised digital exfiltration. By applying a zero-trust framework to outbound data, ZORB blocks the manual or software-based extraction of data to unknown or untrusted destinations.

Example - Preventing unauthorised data transfers

Safelist

Application	Trusted Destinations	Trusted Ports
Onedrive	Microsoft	
Excel	Microsoft, 192.168.1.62	
Outlook	Microsoft	
Word	Microsoft, 192.168.1.62	

Before resigning to establish a competing business, an employee tries to save confidential Word documents to external cloud storage.

The company's safelist identifies "Word" as a trusted application. However, the safelist is also configured to only permit data transfer from Word to either the company's internal server or to Microsoft's managed services.

Upon realizing they cannot save documents externally due to these restrictions, the employee installs Dropbox on their laptop.

IT have not locked down the laptop so Dropbox installs successfully. However, Dropbox is not included in the company's safelist of trusted applications. Consequently, any attempt to transfer data using Dropbox is automatically thwarted.

Finally, the employee attempts to establish a SSH connection to a personal AWS instance.

ZORB prevents data transfers via covert channels such as SSH, TOR, FTP, SFTP, and others unless explicitly permitted in the company's safelist. Hence, the employee was unable to make an SSH connection with the external server.