ZORB

Data Theft Prevention

easy, powerful, affordable

Cloud Application Data Threats

Prevent data breaches from redirected outbound cloud services data

Most business are undergoing a shift in working patterns, as more services are outsourced to the cloud. This could simply be cloud-based data storage. Or it could be self-hosted cloud services on AWS. Or third-party services such as CRMs, ERP, project management, HR, finance, service desk ticketing, etc.

Today, over 60% of enterprise data is held in the cloud. This translates as over 90% of businesses with more than 11 employees using at least one cloud-based service.

Data breaches remain the biggest security concern for cloud-based services. These can arise for various reasons:

- vulnerabilities in cloud applications or infrastructures,
- compromised account credentials
- insider threats
- lack of encryption of data at rest or in transit.

With almost 45% of data stored in cloud services unencrypted, it comes as little surprise that in 2023, over 80% of data breaches involved data used in cloud services.

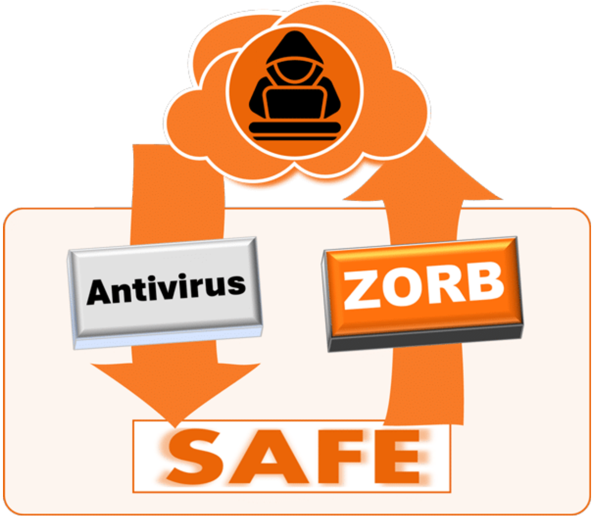
START TODAY

10 FREE licences

www.zorbsecurity.com/trial

There is an inherent degree of trust when using cloud services, that the data transferred to the application goes directly to the cloud vendor and it not intercepted on route. An estimated 10% of data transfer (application data and back-ups) remains unencrypted. The amount of data intercept or redirected by a bad actor (say via DNS rerouting) is not known but is still a breach.

Consider the magnitude of a business's activities that a hacker has visibility of by redirecting an Office 365 .OST file synchronisation.



Prevention

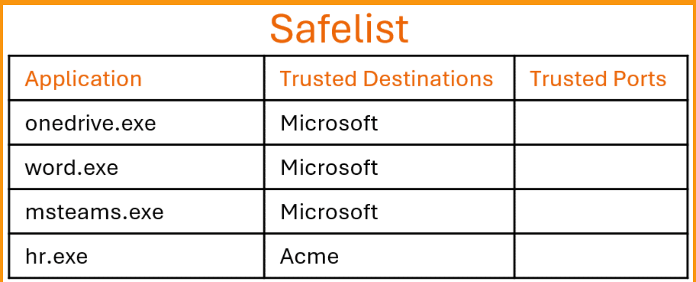
Often one is reliant upon the cloud service provider themselves to provide appropriate security measures.

The result is very little control over what security measures you can influence. At best this can be limited to account access control measures, such as strong passwords, multi-factor authentication and privilege restrictions. Zero-trust frameworks in cloud infrastructure lags significantly behind zero-trust uptake in corporate network.

One area that zero-trust can be successfully applied by the service user is data transfer. Classifying data to ensure the appropriate level of protection transfer, together with proactive, context-aware outbound firewalling on the network perimeter.

ZORB takes a much simpler approach to achieve a zero-trust framework for outgoing cloud application data transfer. ZORB challenges the destination of any outbound data flow to ensure it is being sent to the appropriate IP addresses. If not, the outgoing data flow is blocked.

Example - Preventing cloud data theft



Safelist

Application	Trusted Destinations	Trusted Ports
onedrive.exe	Microsoft	
word.exe	Microsoft	
msteams.exe	Microsoft	
hr.exe	Acme	

A primarily office-based HR employee uses a cloud-based ERP package from Acme.com. This has a local desktop application, called hr.exe, which synchronises in real-time with the cloud data. Malware on the user's PC tries to mirror the ERP data transfer to a service hosted in Azure.

The company list hr.exe as a trusted application in the company's safelist. The cloud application is also associated in the safelist with the vendors domain (www.acme.com). ZORB will identify two data streams. 1) The legitimate data transfer from hr.exe to the cloud provider (acme.com), which it permits as per the safelist. 2) The data transfer from hr.exe to a non-acme.com IP address, which is blocked as untrusted as this IP is not permitted in the safelist. If necessary, this data flow could additionally be queried, and blocked, at a protocol level.

The user goes home for the evening to complete the work on their home PC. The company allows BYOD, but enforces a VPN tunnel to the main office, from where all outbound data is sent. The user only has 5 minutes to work complete, so avoids the hassle of logging into the corporate VPN.

Whilst the hr.exe application is trusted on the user's home device, ZORB has been set up to ONLY permit data transfer over the VPN. The destination IP is NOT the VPN endpoint, so the data is blocked. Having been blocked, the user realises the error and connects to the VPN. ZORB now transmits the data.

On Monday, the IT department rolls out a new cloud-based CRM package to all of sales team.

The IT admin logged onto their ZORB cloud portal, removed the old SalesSpot.exe entry from the trusted list and replaced it with HubForce.exe and the name of the application vendor. This update to the safelist was automatically rolled out to each users device without IT having to do anything.