ZORB

Zero Trust: Safeguarding Your Outgoing Data

How to defend outbound data against theft and compliance violations.

It's 7pm on a cold, dark, miserable Friday evening. It's been a tough week. Your team has completed their work for the week and gone home.

And so can you, with the peace of mind that your company's sensitive, proprietary data is protected against theft from insider attacks, hackers, malware, cloud data transfer threats, and application update poisoning.

Executive Summary

Several common business strategies inadvertently expose company's proprietary data, intellectual property and application data. In ways that are not obvious, often overlooked, and increases the opportunity for theft.

Hackers are changing, ransomware is changing, and as a result data theft is increasing.

Organisations need to recognise that Data Theft Prevention (DTP) requires a different strategy to Data Loss Prevention (DLP). Furthermore, whilst firewalls can provide some mitigation, outbound firewalling for DTP is complex, risky and hugely resource intensive.

This guide explains how a zero trust stance is the only viable way to prevent data theft:

- which business processes are behind the increase in theft attacks
- why your DLP solution and firewall don't protect against theft
- how using zero trust outgoing data security, you can easily and affordably enhance an already strong cybersecurity defence posture, to eliminate data theft and further strengthen your data/privacy compliance framework.

Learn how to defend against:

Data theft from Bad Actors (hackers and insider threats)

Data theft from C2 malware (botnets, ransomware)

Data theft from Info Stealers (trojans, data stealers)

Data theft from transmission re-routing (vulns, data syncs, DNS poisoning)

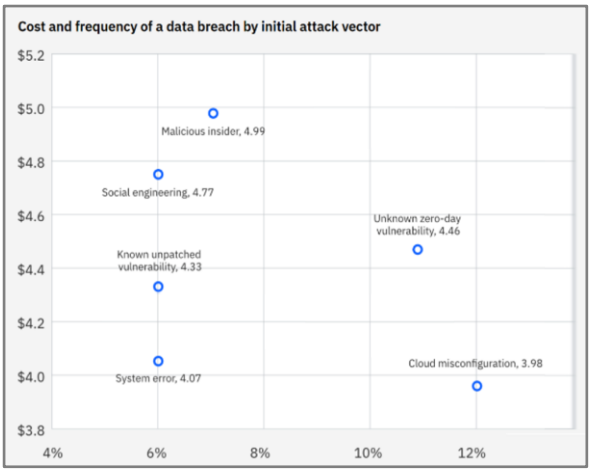
The reality of data theft.

Data theft attacks spiked in 2023. Experts estimate that attackers stole over 1 trillion digital assets last year. This figure includes personal data. But it also includes theft of business proprietary data - such as financial records, intellectual property, customer lists, etc.

The deliberate, intentional data exfiltration **from hacker attacks** is rising. State-sponsored attackers and other financially motivated external actors caused 83% of breaches. The most common method of gaining access was via OS vulnerabilities on endpoints.

Ransomware is changing. Ransomware used to just encrypt data. Today, ransomware steals data. In 2023, data exfiltration from ransomware jumped from 46% to 64%. 76% of victims paid the ransom to get their data back.

Nor is it all about financial gain. Attacks to deliberately disrupt businesses increased from 31% of people surveyed in 2022, to 51% in 2023.



Adapted from IBM's Cost of a Data Breach Report 2024

What is behind the increase in theft attacks?

Certain popular business processes significantly contribution to this spike in attacks:

- an increased **reliance on cloud services,**
- employees wanting to **work remotely** with full access to data,
- deeper **digital supply chain** relationships.

These processes share a common thread – they are all sending more of our sensitive business data than ever outside of the corporate network. In turn, exposing business-critical data to more threats.

Today, cloud services store more than 60% of the world's corporate data. Unsurprisingly, in 2023, cloud data featured in 80% of breaches. Providers have started to tighten up on the more obvious threats - unrestricted ports, account compromise, privilege abuse, and infrastructure security. But this still leaves vulnerable gaps.

Supply chain attacks rose from 44% to 55% of people surveyed, in 2023. Some 98% of organizations that have a vendor relationship have experienced a data breach within the last two years. But of course, people will remember 2023 for the MOVEit attack, which compromised 80 million users.

For more information about how these three business processes expose business data visit

https://www.zorbsecurity.com/blog/three-business-strategies-exposing-your-data/

Secure outgoing data to combat data theft.

An attacker can easily bypass incoming threat prevention tools, such as antivirus, firewalls, intrusion prevention, and identity management. Otherwise, data theft would not be a thing.

Today, securing outbound data focuses on **HOW** is my external data getting to its destination? We force data transmission via VPN and HTTPS to ensure data is encrypted and cannot be read if intercepted.

Data theft occurs stealthily. If you don't detect it happening, you can't prevent it. So, to fully protect business and application data against theft, we must look beyond the obvious security risks.

To be able to combat data theft, we need to question every data flow as to "**WHERE** are you going to?" Endpoint protection tools and firewalls can answer this question - maybe not easily and requiring considerable resource allocation. See *The Trouble with Firewalls...*

But knowing the destination of the data does not mean it is headed to the "correct" place. It is one thing knowing that data is going to IP address 10.10.10.10. It is a different story if you know a botnet is telling the data to go to this IP. So outgoing data security also asks, "**WHAT** told my data to go there?"

Outgoing data security enables you to detect unauthorised data removal. But you also need to stop the exfiltration before it turns into a data breach. Today, if you detect data theft, you trace the leak back to the infected machine. Then you quarantine the machine, possibly perform forensics, and re-image it. Then you start patching servers and other hardware devices. All of which takes time. Time in which more data might be being exfiltrated.

So, outgoing data security also requires the capability to isolate and end just the compromised outbound data flow – quickly, and without manual intervention such as the user or IT department.

Safeguarding outbound data against theft involves three elements:

1) **knowing where transmitted data is destined to,**
2) **knowing which application has requested to send it there,**
3) **isolating and stopping the compromised flow, without affecting users.**

COMPARE & CONTRAST

Outgoing Data Security is a protection mechanism to prevent the intentional, deliberate THEFT of business intellectual property and application data, by bad actors or malware.

Data Loss Prevention is a protection mechanism to prevent (accidental) leakage of Personally Identifiable Information (PII), by a user.

These two different protection mechanisms safeguard two distinct types of data. They protect against different attacks, which result in different business impacts.

For more information about these two different prevention methods visit

https://www.zorbsecurity.com/blog/differences-between-data-theft-and-data-leak/

Zero Trust: Safeguarding your outgoing data.

Zero trust is a security model that assumes **nothing, and no one, is trustworthy by default,** even if it is inside an organization's network.

Outgoing data security is a zero trust stance to data transmission. It starts from the viewpoint that:

Every data flow is untrusted until its integrity can be proven.
Only then can the data be sent to its onward destination.

In other words, prevent ALL outward-bound data from leaving its source device, unless the data flow is confirmed to be trusted.

This can be applied through a typical security rule-based approach, through two opposing methods:

1. **PERMIT ALL and DENY unsafe** destination IP addresses and protocols.
   Allow the entire IPv4/v6 address range. Deny the few million trusted destination IPs.
2. **DENY ALL and PERMIT safe** destination IP addresses and protocols.
   This is more manageable but still requires millions of safe IP addresses.

In outgoing data security, **trust** is achieved by querying each data flow on "Where is this data going to?" and "How is the destination related to the origin application?" This can be easily achieved by querying a list of **known** (i.e. trusted) applications that IT has installed on a device.

Now if malware installs, as it is not on the known application list, then any transmitted data is blocked. Suppose the malware masquerades as a known Microsoft application. We query the destination IP address. As this points to an IP address that is not associated with Microsoft, again, we treat this as untrusted and block any data from transmission. A belt and braces approach can be achieved through a third question – "**WHICH** comms channel will it use to get there?" Thereby blocking covert channels, such as TOR, SSH, etc. (unless specifically approved in the trusted application list).

Outgoing data security is a ZERO TRUST approach to data transmission:
By default, all data flows are untrusted and therefore not transmitted.
Until proven trustworthy.

Thereby making it extremely difficult to exfiltrate data via the network, internet or cloud.

Do you *really* know where your data is going?

If you cannot answer these questions, you need outgoing data security:

- Can I detect data being syphoned off to a compromised cloud server?
- Can I detect compromised synchronisation uploading of cloud data?
- Can I detect rerouting of application data on its way Microsoft 365?
- Can I detect a compromised application update request to a malicious server?
- Can I detect a compliance compromise of a user innocently storing data on Dropbox?

Even if you answered YES to all the above:

- Can I stop this in real time?
- Can I stop this proactively – without user, or IT intervention?

The trouble with firewalls…

Businesses have used firewalls as a staple network defence tool for decades. Firewalls are two-way devices, capable of restricting both outgoing as well are incoming traffic. They are a necessary element to prevent incoming attacks. Blocking open ports exposed to the internet. Blocking incoming traffic from compromised IP addresses. Content inspection of incoming data.

Less than 1% of businesses use firewalls to safeguard outgoing data from theft. Firewalls and Data Loss Prevention (DPL) solutions can inspect outbound email content or web forum data. Security professionals find it much easier to configure a system to protect against known incoming threats, than to block the myriad possible outbound threat combinations.

Yet, we implicitly trust our applications to send data to the correct place. Usually the vendor's cloud. In 2023, 91% of data theft attacks begin at an application, or device, vulnerability or misconfiguration that allows an attacker to redirect data.

When did you last investigate where your business apps send their data?

…FIVE reasons you do not currently block compromised egress traffic.

Complexity – firewalls and IPS can protect both inbound and outbound data. Administrators can configure inbound rulesets relatively simply. Today, firewalls automatically create new inbound rules when someone installs an application.
However, configuring outgoing rulesets is complex. Rulesets may need to cover hundreds of millions of rules. Microsoft alone has over 60 million possible IP addresses, each of which may require a rule. Even if you can create all these rules, a single misconfiguration on a perimeter firewall could expose your entire network infrastructure.

Resource – most IT teams are over-stretched. So, team members must be deployed where they have the most impact. Managing outgoing data rulesets is extremely resource intensive. Outgoing data rulesets change continually and require updating across all devices.

Cost – complexity and resource mean cost. Perimeter firewalls are expensive and lack flexibility. Blocking outgoing data on a perimeter firewall makes tracing the issue back to the offending device, or application, difficult. It's more effective to have a firewall for each device – to be able to implement rules at a user or department level. But this is expensive. How can this granularity scale across all your users? How do you bring hybrid workers into your posture? What about cloud services? What about supply chain data?

Situ limitations – network firewalls are typically perimeter devices. This makes it simple to applying blanket rulesets across a network. But makes it difficult to apply rules to an individual user level. For example, 3 people in Finance need to access the cloud-based QuickBooks app, but no one else in the business can. Only device-level firewalls can achieve such fine granularity. But these introduce configuration and ongoing management challenges.

Alert fatigue – Most SOCs are already overloaded with too many false positives. Rather than feed yet more alerts about data exposure into your SIEM, a device such automatically block any malicious exfiltration, without your staff, or user's intervention.

SEVEN key features of outgoing data security.

Data exfiltration prevention requires challenging the integrity of outbound flows: **WHERE** is data going, **WHAT** told it to go there? Asking - what application told this data flow to go to this IP address? Is the application trusted? Is the endpoint related to the application?

Often security is about risk mitigation. Outgoing data security shifts mitigation to **PREVENTION**. Preventing compromised data from leaving a device is preferable to mitigating damage after theft. Outgoing data security provides a zero trust stance: *Deny all outbound data. Only once the flow has proven to be from a TRUSTED origin to a TRUSTED destination, should it be transmitted.*

Key features for outgoing data security include:

1) Zero trust stance
Treat each data flow are untrusted for transmission, until proven otherwise.

2) Automated, proactive flow blocking
Most SOCs don't need more alerts. Nor should IT, nor the user, intervene to decide if a data flow is trusted. Just block the compromised flow at once before it can become a breach. And log it for later reporting.

3) Rule granularity
It must be easy to create powerful rules at both the application layer and the network layer. Rulesets require flexibility and granularity, so they can be applied to specific user groups and their applications. Thereby removing opportunities to exfiltrate data should an account or application be compromised.

4) Device based
A robust defence comes from deploying user/group specific rules on individual user devices, rather than the network. Especially if these devices are part of a hybrid working setup. Outgoing data security tools must scale affordably across the entire device estate, as well as being easy to push update rules to each device.

5) Integration
Outgoing data security should not require any upheaval to legacy equipment. It should have the ability to report to the SIEM, as part of threat intelligence gathering.

6) Visibility
A CISO wants to know that the risk profile across the entire company has been minimised. Outgoing data security should be able to provide a real-time snapshot of the outgoing data across all devices, without gaps an attacker could exploit.

7) Compliance
Outgoing data security is about both a) prevention against compromise and b) meeting compliance regulations. Outgoing data security is a control for frameworks such as Cyber Essentials, ISO27001 and the MITRE ATT&CK guidelines.

Who is in control of your outgoing data?

A strong outgoing data security stance protects sensitive, proprietary business data and application data from exfiltration. But what do you need to defend against?

Hackers & Insider Threats
Business data is subjected to multiple threats. Internal as well as external.
If your proprietary data (intellectual property, financials, M&A, product blueprints, cost prices, etc) is valuable to you, it has resale value for an attacker.

Ransomware & Botnets
C&C malware have an Achilles' heel - they communicate with a C&C server. Sever that link, you cut the malware's threat potency.

Data Stealers & Trojans
These malwares provide attackers with a backdoor to your network. Allowing attackers to exfiltrate data as they please. Would you know if your business has been compromised?

Cloud-App Data Transmission Rerouting
Has an app vulnerability allowed an attacker rerouted Outlook .OST synchs? Has the DNS request for an automatic update been poisoned?

Explore these use cases in more detail at https://www.zorbsecurity.com/use-cases

To arrange a trial, or understand more about ZORB, contact us at eliminate@zorbsecurity.com, or call +44 1223 603029.

About the Author

Dr Mark Graham has been involved in cyber security for over 40 years. He spent 7 years lecturing in information security in Cambridge, UK. He holds a PhD in novel ways to detect cyber incidents in small volumes of network traffic. He is an accomplished pen-tester. He regularly speaks at events about cyber security and data protection.

Frustrated by constant bad-news stories of attackers staying ahead of the game in data theft, he built ZORB to help companies achieve effective, yet affordable, protection from data theft, whoever the attacker might be.

ZORB Security Ltd

ZORB Security is a data theft prevention startup based in Cambridge, UK. The company was created to make it easy for businesses, of any size, to enhance their cyber defence posture by including outgoing data security. The ZORB team are all specialists in data protection at a network and application level.

Our mission is to democratise data loss prevention by making is easy, powerful and affordable.

www.zorbsecurity.com