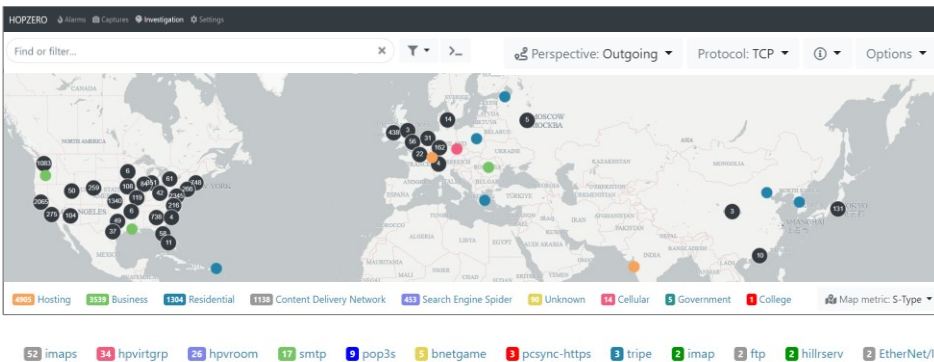


SaaS Auditor

It is an overwhelming task and burden to know where your data is going. With HOPZERO SaaS Auditor you can know with absolute certainty that your data is safe in just a few minutes.

The SaaS Auditor is an online tool that lets you upload a packet header capture file to our portal and in minutes receive access to a graphical representation of where your data is traveling. SaaS Auditor's easy point and click filters provide valuable information and advanced filters may be saved for reuse. One click produces a security compliance Block Report, providing a map of where application connections are leaking out firewalls. Click a session dot and detailed Deep Security DataTravel™ research pops up, delivering cogent information that saves hours of security research.

"A picture is worth a thousand logs"



Graphical geo maps of internal and Internet IP locations show every session traveling from inside of your network to the Internet. Predefined filters show perspective from External to Internal, Internal to External and Internal to Internal. Optional filters like Data Attributes Application types are included.

Client IP	Client Country	Client Domain	Client Type	Client Fraud Score	Client GDPR	Client Org	Peer Sessions	App Port	App Name	Server IP	Server Type	Server Hosting	Server EU	Hop Policy	Hop Severity	Risk Score
192.168.1.10	United States	example.com	Business	0.01	FALSE	Example Corp	1	1433	ms-sql-s	192.168.1.2	Hosting	TRUE	FALSE	Block	Critical	100.01
192.168.1.10	Turkey	example.com	Residential	0.01	FALSE	Example Corp	1	1433	ms-sql-s	192.168.1.5	Unknown	FALSE	FALSE	Block	Info	1
192.168.1.10	United States	example.com	Hosting	45	FALSE	Example Corp	1299	80	http	192.168.1.10	HVAC	FALSE	FALSE	Warn	Warn	490.16
192.168.1.10	Vietnam	example.com	Residential	0.01	FALSE	Example Corp	6	25	smtp	192.168.1.10	Exchange	FALSE	FALSE	Warn	Info	2.79
192.168.1.10	Portugal	example.com	Cellular	0.01	TRUE	Example Corp	3	25	smtp	192.168.1.10	Exchange	FALSE	TRUE	Warn	Info	2.1
192.168.1.10	Germany	example.com	Residential	0.01	TRUE	Example Corp	6	25	smtp	192.168.1.10	Exchange	FALSE	TRUE	Warn	Info	2.79
192.168.1.10	Unknown	example.com	Unknown	0	FALSE	Example Corp	1	135	epmap	192.168.1.10	Business	FALSE	FALSE	Block	Critical	100
192.168.1.10	Unknown	example.com	Unknown	0	FALSE	Example Corp	1	135	epmap	192.168.1.10	Business	FALSE	FALSE	Block	Critical	100
192.168.1.10	Unknown	example.com	Unknown	0	FALSE	Example Corp	31	22	ssh	192.168.1.10	Business	FALSE	FALSE	Local	Critical	44.34
192.168.1.10	Unknown	example.com	Unknown	0	FALSE	Example Corp	30	22	ssh	192.168.1.10	Business	FALSE	FALSE	Local	Critical	44.01
192.168.1.10	Unknown	example.com	Unknown	0	FALSE	Example Corp	30	22	ssh	192.168.1.10	Business	FALSE	FALSE	Local	Critical	44.01
192.168.1.10	Unknown	example.com	Unknown	0	FALSE	Example Corp	2	22	ssh	192.168.1.10	Business	FALSE	FALSE	Local	Critical	16.93

Fast security research at your fingertips. Export filtered data to table format to create your own custom reports.

- ✓ Upload Snapshot Audit Data
- ✓ Exfiltration Visualization
- ✓ Point & Click Navigation
- ✓ Access to Continous Recorder Data
- ✓ Point and Click Filters
- ✓ Map Investigation Sharing
- ✓ Portal Account Management
- ✓ Auto-send to Syslog
- ✓ CSV Export

Learn more about Exfiltration Prevention and Data Containment at <https://hopzero.com/Auditor>

Cybic - Australian Distributor

Suite 2, 65-71 Whiting Street,
Artarmona NSW 2064
Angus Button
Phone 0414-266-999
angus@cybic.net.au

About HOPZERO

HOPZERO is an Exfiltration Prevention solutions developer. Audits and proactive security solutions allow companies to protect their private data. HOPZERO products are managed with a unified SaaS management platform providing enterprise wide visibility and safe data containment policy enforcement. HOPZERO security systems eliminates complexity and training gaps normally associated with enterprise systems.

HOPZERO DataTravel™ Security

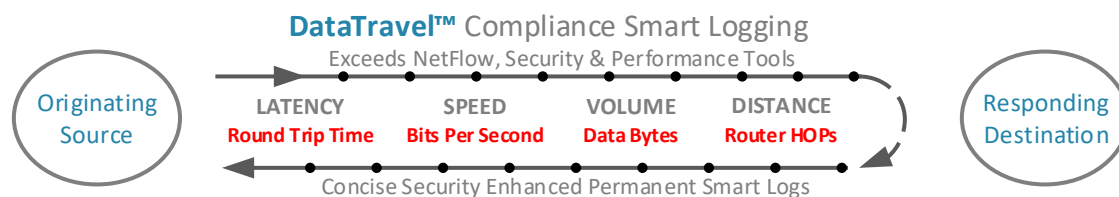
Smart Session Recorder

Knowing where your data is going at all times of the day or night is your ticket to peace of mind. The Smart Session Recorder puts eyes on every server session, continuously auditing where your data is traveling.

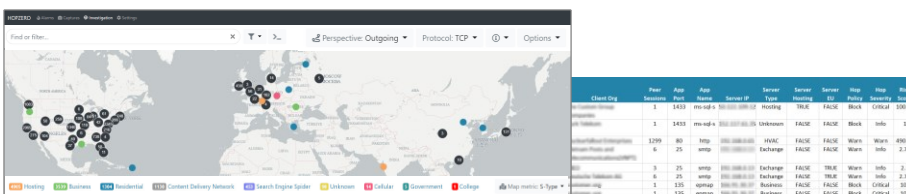
The Smart Session Recorder (SSR) is an on premise or cloud virtual security appliance with licensing that includes the SaaS Auditor product. HOPZERO's SSR provides unattended real-time operation for compliance standards logging and actionable exfiltration alarms. Alarms can be configured to send to central security consoles, making visualization map viewing optional – however, seeing where data is traveling enables rapid understanding, and HOPZERO's deep security research tools provide motivation to use it regularly. The SSR renders graphical presentation of the current attack surface and "a picture is worth a thousand logs".

"Smart Logs Improve Compliance"

Logging every communication session provides compliance with NIST, GDPR, HIPAA, PCI, DoD, and all security standards. Concise logs add security research enhancements, building smart logs to include the Who, What, When, Where and Why. Smart logs help differentiate a sophisticated state sponsored actor from a lone script kitty hacker. Speed, distance, latency and volume combined with threat intelligence lookups, build a powerful risk score, zeroing in on material risks. DataTravel™ Compliance Logging exports to Excel, Splunk, LogZilla or ELK Elastic Search. Integrating raw device event logs brings user session context with HOPZERO's enhanced smart security & performance session metrics. Actionable alarms notify of an attempt made to access vital data from outside the Sphere of Trust™. The system integrates with other vendors and has features to collaborate across organization lines.



Only IP address meta-data is collected or stored by our products. SSR with Auditor rapidly validates actual or potential exfiltration proving an organization's effective security or reveals data leaks. All meta-data is encrypted in transit and at rest.



Smart Session Recorder requires SaaS Auditor and purchased as a bundle. Get real time graphical geo maps and export data to create custom reports.

Learn more about Exfiltration Prevention and Data Containment at <https://hopzero.com/Recorder>

Cybic - Australian Distributor

Suite 2, 65-71 Whiting Street,
Artarmon NSW 2064
Angus Button
Phone 0414-266-999
angus@cybic.net.au

About HOPZERO

HOPZERO is an Exfiltration Prevention solutions developer. Audits and proactive security solutions allow companies to protect their private data. HOPZERO products are managed with a unified SaaS management platform providing enterprise wide visibility and safe data containment policy enforcement. HOPZERO security systems eliminates complexity and training gaps normally associated with enterprise systems.

HOPZERO DataTravel™ Security

Sphere of Trust™ Enforcer

When you realize it isn't enough to know your data has been compromised, you're ready for the HOPZERO Sphere of Trust™ Enforcer.

The Sphere of Trust™ (SoT) Enforcer is an on premise or cloud virtual security appliance that includes the Recorder and Auditor products. The Enforcer uses information provided by both the Recorder and Auditor to recommend DataTravel™ limits on server communications to keep data within a Sphere of Trust™.

Actionable alarms are generated to notify of any attempt to access vital data from outside the Sphere of Trust™. No data is allowed to travel beyond its security policy. Rapid validation of actual or potential exfiltration proves an organization's effective security or reveals data leaks requiring mitigation. The Enforcer is the proactive way to identify if data is being exfiltrated out of your organization and put limits in place to keep it from leaving the Sphere of Trust™. The Enforcer integrates with other vendor SIEM, SOAR and Archiving systems and includes features to collaborate across organization lines.

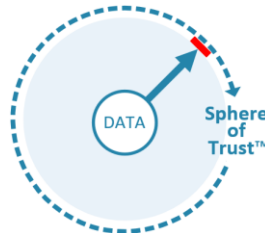
"Keep Vital Server Sessions Inside the Data Center"

HOPZERO provides greater than a 99% Attack Surface reduction, building a powerful Sphere of Trust, keeping data inside your network and out of the wrong hands.

Inside the Sphere of Trust™



- Data Center Devices
- Safe Communications
- Vital Server Protection

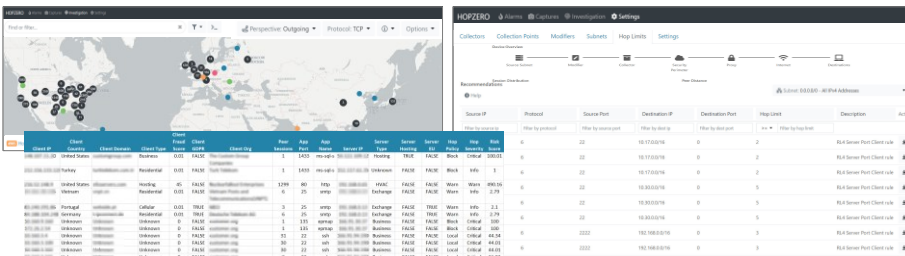


Outside the Sphere of Trust™



- User Insider Threats
- Phish & Ransomware
- Internet Risks

The Enforcer learns the Attack Surface of every device, creating numerous SoT policies to Block and Limit DataTravel™. An administrator's click authorizes an enforcement recommendation, limiting how far a vital server may communicate – keeping it safe inside the Sphere of Trust™. Enforcement works even if a firewall would allow exfiltration – even if access credentials to the server were lost and in the wrong hands – nothing can connect to the server from outside the Sphere of Trust™. This prevents command-and-control plus many other exploits, keeping vital data safe.



Source IP	Protocol	Source Port	Destination IP	Destination Port	Flags	Description	Action
192.168.1.100	TCP	80	192.168.1.1	80	SYN	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	ACK	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	FIN	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	RST	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	URG	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	PSH	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	ACK	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	FIN	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	RST	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	URG	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	PSH	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	ACK	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	FIN	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	RST	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	URG	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	PSH	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	ACK	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	FIN	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	RST	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	URG	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	PSH	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	ACK	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	FIN	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	RST	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	URG	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	PSH	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	ACK	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	FIN	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	RST	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	URG	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	PSH	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	ACK	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	FIN	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	RST	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	URG	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	PSH	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	ACK	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	FIN	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	RST	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	URG	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	PSH	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	ACK	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	FIN	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	RST	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	URG	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	PSH	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	ACK	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	FIN	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	RST	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	URG	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	PSH	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	ACK	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	FIN	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	RST	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	URG	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	PSH	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	ACK	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	FIN	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	RST	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	URG	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	PSH	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	ACK	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	FIN	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	RST	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	URG	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	PSH	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	ACK	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	FIN	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	RST	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	URG	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	PSH	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	ACK	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	FIN	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	RST	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	URG	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	PSH	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	ACK	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	FIN	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	RST	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	URG	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	PSH	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	ACK	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	FIN	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	RST	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	URG	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	PSH	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	ACK	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	FIN	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	RST	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	URG	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	PSH	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	ACK	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	FIN	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	RST	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	URG	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	PSH	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	ACK	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	FIN	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	RST	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	URG	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	PSH	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	ACK	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	FIN	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	RST	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	URG	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	PSH	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	ACK	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	FIN	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	RST	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	URG	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	PSH	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	ACK	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	FIN	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	RST	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	URG	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	PSH	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	ACK	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	FIN	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	RST	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	URG	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	PSH	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	ACK	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	FIN	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	RST	HTTP GET /	Allow
192.168.1.100	TCP	80	192.168.1.1	80	URG	HTTP GET /	Allow



EXFILTRATION RISK AUDIT

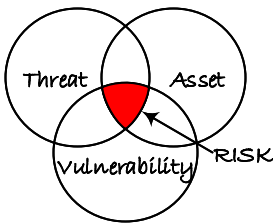
Traditional Threat Assessments test if you are blocking known exploits. They don't tell you what internal systems are freely sending data out of your company. Only an Exfiltration Risk Assessment can pinpoint what data is leaking out of your company.

If your company has performed an IT Systems Vulnerability Assessment, you have only done half the job. Firewalls, IDS/IPS like systems all are intercepting what is coming into your network. Firewalls are one way security devices with an inbound perspective. Their design lets internal source communications freely exit the company as trusted communications. But with the successful use of Phishing emails, bad guys have found a way to exfiltrate your company data undetected. Our Auditor software removes the cloak and identifies the outbound activity like turning on a light in a dark room.



The Cybersecurity Framework relies heavily on identifying and detecting risk before protection, response and recovery can take place. Most security risk assessment tools are focused on inbound. It's time to see the other half of the security picture and what you've been missing.

Every Exfiltration Risk Audit we've provided for customers has identified Exfiltrating data and risks for Exfiltration resulting in immediate remediation action. All of them had a security solution in place.






Cybercriminals do a pretty good job of staying undetected for as much as 200+ days before they actually perform their exploit, probing and learning more about your company and identifying where your most important data is stored. Your job is to detect their presence and quickly eradicate them from your servers and other hosts attempting to infiltrate your servers. You need a company with the tools to help you do just that. Risk can be prevented with the right tools.

- ✓ Advanced filters and forensic analysis tools to investigate risk or incidents for remediation or audit reporting
- ✓ Integrated threat intelligence feed provides the most up-to-date insights to help identify known risks
- ✓ Hundreds of out-of-the-box correlation rules are provided for on-premises network exfiltration risk detection
- ✓ Simplify compliance reporting with integrated audit-ready Maps and export report data
- ✓ Identify GDPR, CCPA data that must be protected and more

Exfiltration Assessment and Verification

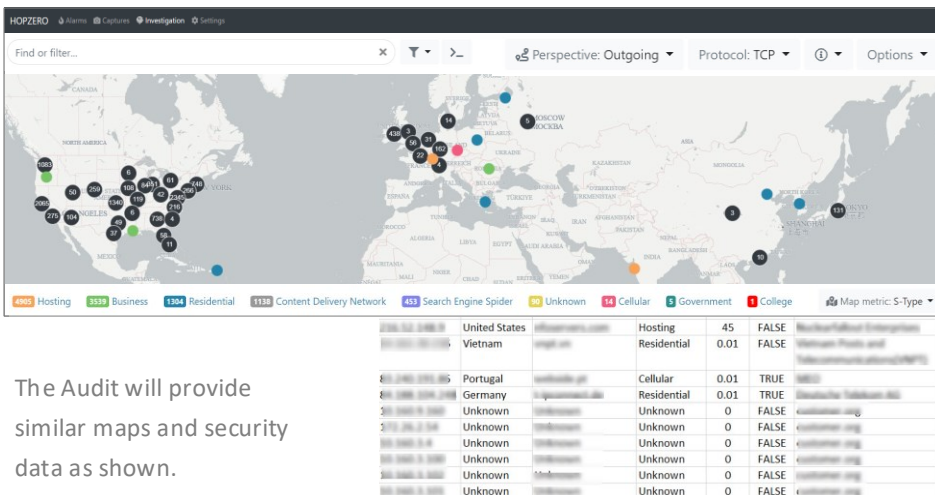
Exfiltration Audit Services

Audit Type	Duration	PCAP Snapshots	IP Devices	Recorder	Maps	Attack Surface Model
 Snapshot Audit	4 hrs	1	<3K	-	5	10
 Remote Audit	3-5 Days	5	<10K	1	25	100
 Onsite Audit	1-3 Weeks	10	<20K	2	50	200

Exfiltration Risk Audits Give You:

- Reports for discovered Exfiltration
- Verification of implemented controls
- Identification of control weaknesses
- Actionable recommendations for improvement
- Regulatory information for auditors

Every company has IT security controls in place but need a way to verify that those controls are effective and preventing data from being stolen by intruders. The Exfiltration Risk Audit reviews your security posture and provides physical proof of how well the implemented controls are working. The verification will identify any weaknesses in your exfiltration prevention controls and our experts will recommend steps to stop any data leaks. You will receive actionable recommendations on how to implement or fix controls so that data is contained to your organization. This service provides verification to satisfy regulatory auditors year after year. You are assured to receive a comprehensive review of your data exfiltration security posture.



The Audit will provide similar maps and security data as shown.

The Exfiltration Risk Audit is performed using our HOPZERO Auditor and Recorder products. Customers can purchase these same products working in their networks.

Learn more about Exfiltration Prevention and Data Containment at <https://hopzero.com/ExfiltrationRiskAudit>

Cybic - Australian Distributor

Suite 2, 65-71 Whiting Street,
Artarmon NSW 2064
Angus Button
Phone 0414-266-999
angus@cybic.net.au

About HOPZERO

HOPZERO is an Exfiltration Prevention solutions developer. Audits and proactive security solutions allow companies to protect their private data. HOPZERO products are managed with a unified SaaS management platform providing enterprise wide visibility and safe data containment policy enforcement. HOPZERO security systems eliminates complexity and training gaps normally associated with enterprise systems.

HOPZERO DataTravel™ Security