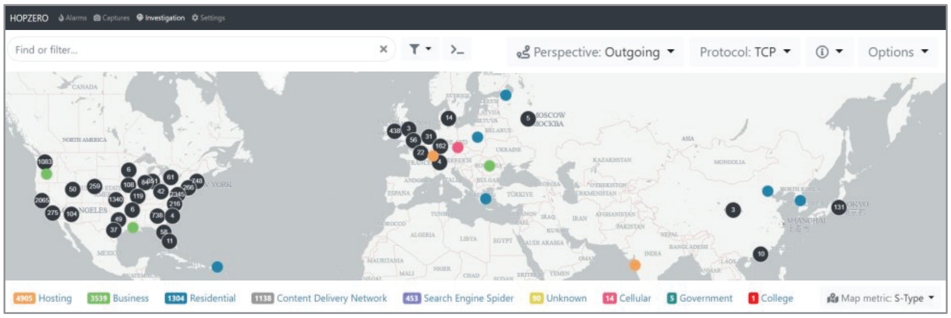
HOPZERO PORTAL

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

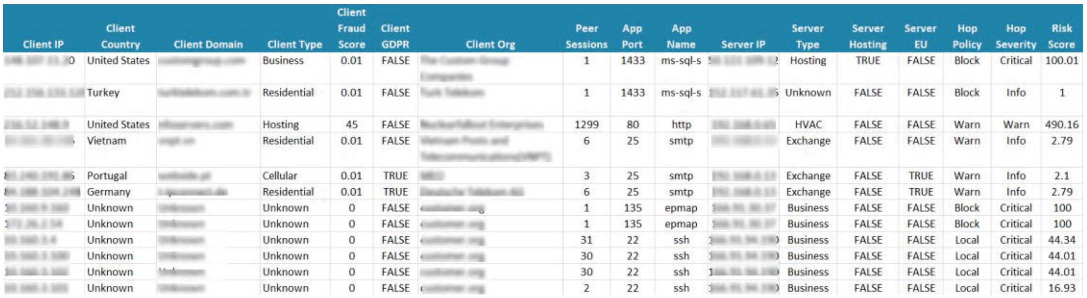
The Visualizer Portal is an online tool that lets you upload data session packet headers to our Portal and in minutes receive access to a graphical representation of where your data is traveling. This information is used to set Data-Travel™ limits to securely limit where your data is allowed to go. Sessions are continuously uploaded by installing a HOPZERO Collector or manually uploaded through the Portal capture page. The Visualizer Portal offers easy point and click filters that provide rapid security and forensic network information using advanced filters that can be customized for reuse. A single click produces a Block Session report with a map of where application connections are leaking out firewalls. Click a map dot and receive detailed security information for that session in seconds, saving a security analyst hours of 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.

52 imaps · 34 hpvirtgrp · 26 hpvroom · 17 smtp · 9 pop3s · 5 bnetgame · 3 pcsync-https · 3 tripe · 2 imap · 2 ftp · 2 hillrserv · 2 EtherNet/IP-1 · 1 can-ferret · 1 blizwow · 1 sips · 1 xmpp-client · 1 rxapi · 1 TCP (62887)



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
[redacted]	United States	[redacted]	Business	0.01	FALSE	[redacted]	1	1433	ms-sql-s	[redacted]	Hosting	TRUE	FALSE	Block	Critical	100.01
[redacted]	Turkey	[redacted]	Residential	0.01	FALSE	[redacted]	1	1433	ms-sql-s	[redacted]	Unknown	FALSE	FALSE	Block	Info	1
[redacted]	United States	[redacted]	Hosting	45	FALSE	[redacted]	1299	80	http	[redacted]	HVAC	FALSE	FALSE	Warn	Warn	490.16
[redacted]	Vietnam	[redacted]	Residential	0.01	FALSE	[redacted]	6	25	smtp	[redacted]	Exchange	FALSE	FALSE	Warn	Info	2.79
[redacted]	Portugal	[redacted]	Cellular	0.01	TRUE	[redacted]	3	25	smtp	[redacted]	Exchange	FALSE	TRUE	Warn	Info	2.1
[redacted]	Germany	[redacted]	Residential	0.01	TRUE	[redacted]	6	25	smtp	[redacted]	Exchange	FALSE	TRUE	Warn	Info	2.79
[redacted]	Unknown	[redacted]	Unknown	0	FALSE	[redacted]	1	135	epmap	[redacted]	Business	FALSE	FALSE	Block	Critical	100
[redacted]	Unknown	[redacted]	Unknown	0	FALSE	[redacted]	1	135	epmap	[redacted]	Business	FALSE	FALSE	Block	Critical	100
[redacted]	Unknown	[redacted]	Unknown	0	FALSE	[redacted]	31	22	ssh	[redacted]	Business	FALSE	FALSE	Local	Critical	44.34
[redacted]	Unknown	[redacted]	Unknown	0	FALSE	[redacted]	30	22	ssh	[redacted]	Business	FALSE	FALSE	Local	Critical	44.01
[redacted]	Unknown	[redacted]	Unknown	0	FALSE	[redacted]	30	22	ssh	[redacted]	Business	FALSE	FALSE	Local	Critical	44.01
[redacted]	Unknown	[redacted]	Unknown	0	FALSE	[redacted]	2	22	ssh	[redacted]	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/portal**

HOPZERO

11400 Concordia University Dr.
Austin, TX 78726
833-467-9376
inquire@hopzero.com

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

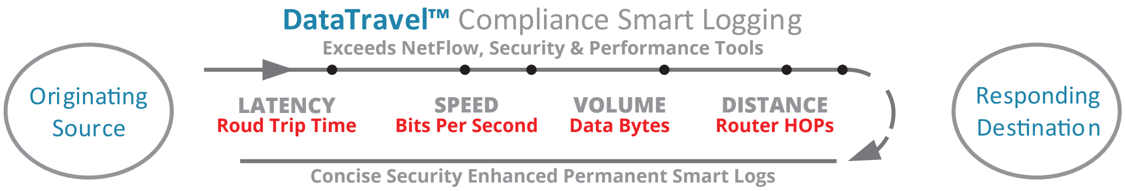
NETWORK COLLECTOR

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

The Network Collector is an on premise or cloud virtual security appliance with licensing that includes the Visibility Portal product. HOPZERO's collector 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 Collector renders graphical presentation of the current attack surface delivering "a picture is worth a thousand logs".

Smart Logs Improve Compliance.

Logging every communication session provides compliance with NIST, GDPR, HIPAA, PCI, ISO 27001, 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 kiddy hacker. Speed, distance, latency and volume combi ned with threat intelligence lookups, build a powerful risk score, zeroing in on material risks. DataTravel™ Compliance Logging exports to Excel, Or other SIEM or logging systems. Network Collector integrates raw device event logs to deliver user session context, enhanced smart security & performance session metrics. Actionable alarms notify of any 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.

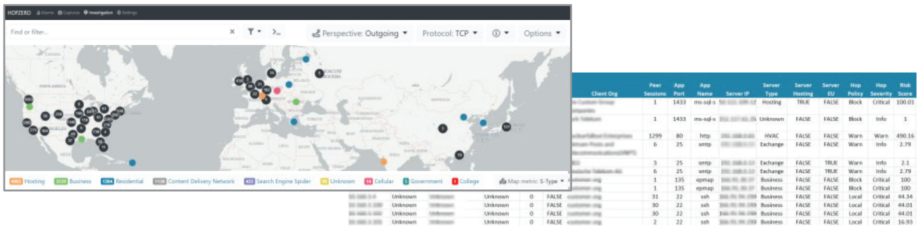


DataTravel™ Compliance Smart Logging

Exceeds NetFlow, Security & Performance Tools

Concise Security Enhanced Permanent Smart Logs

Only IP addresses and session meta-data is collected or stored by our products. Payload data is not collected. Network Collector with Visualizer Portal rapidly validates actual and potential exfiltration proving an organization's effective security or reveals data leaks. All information collected is encrypted in transit and at rest.



Client Org	Peer Sessions	App Port	App Name	Server IP	Server Type	Server Hosting	Server EU	Hop Policy	Hop Severity	Risk Score
[redacted]	1	1433	ms-sql-s	[redacted]	Hosting	TRUE	FALSE	Block	Critical	100.01
[redacted]	1	1433	ms-sql-s	[redacted]	Unknown	FALSE	FALSE	Block	Info	1
[redacted]	1299	80	http	[redacted]	HVAC	FALSE	FALSE	Warn	Warn	490.16
[redacted]	6	25	smtp	[redacted]	Exchange	FALSE	FALSE	Warn	Info	2.79
[redacted]	3	25	smtp	[redacted]	Exchange	FALSE	TRUE	Warn	Info	2.1
[redacted]	6	25	smtp	[redacted]	Exchange	FALSE	TRUE	Warn	Info	2.79
[redacted]	1	135	epmap	[redacted]	Business	FALSE	FALSE	Block	Critical	100
[redacted]	1	135	epmap	[redacted]	Business	FALSE	FALSE	Block	Critical	100
[redacted]	31	22	ssh	[redacted]	Business	FALSE	FALSE	Local	Critical	44.34
[redacted]	30	22	ssh	[redacted]	Business	FALSE	FALSE	Local	Critical	44.01
[redacted]	30	22	ssh	[redacted]	Business	FALSE	FALSE	Local	Critical	44.01
[redacted]	2	22	ssh	[redacted]	Business	FALSE	FALSE	Local	Critical	16.93

Network Collector requires Visualizer Portal 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/Collector**

HOPZERO
11400 Concordia University Dr.
Austin, TX 78726
833-467-9376
inquire@hopzero.com

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™ AGENT

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

The Sphere of Trust™ (SoT) Agent is a Server based enforcement agent that includes its own Network Collector that listens to its own traffic. The built in Enforcer uses information provided by both the internal Network Collector to recommend DataTravel™ limits on server communications that keeps data within a Sphere of Trust™. No data is allowed to travel beyond its security policy.

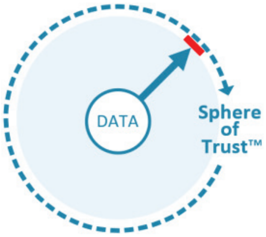
Actionable alarms are generated to notify of any attempt to access vital data from outside the Sphere of Trust™. Rapid validation of actual or potential exfiltration proves an organization's effective security or reveals data leaks requiring mitigation. The Agent is the proactive way to identify if data is being exfiltrated out of your organization and enforce limits to keep it from leaving the Sphere of Trust™. The Agent 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™**

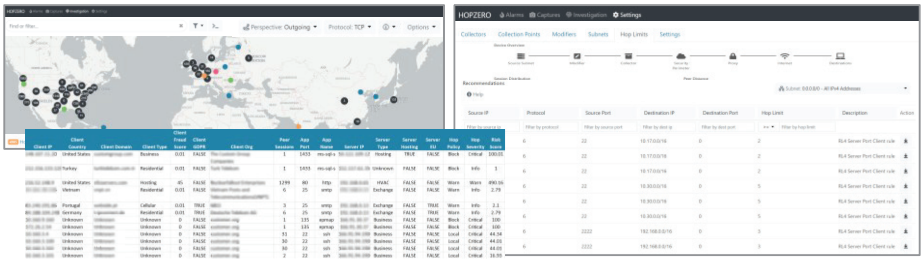
- Data Center Devices
- Safe Communications
- Vital Server Protection



Outside the **Sphere of Trust™**

- User Insider Threats
- Phish & Ransomware
- Internet Risks

The Agent learns the Attack Surface of each device, creating a SoT policy 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 compromised 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.



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
[redacted]	United States	[redacted]	Business	0.01	FALSE	[redacted]	1	1433	ms-sql-s	[redacted]	Hosting	TRUE	FALSE	Block	Critical	100.01
[redacted]	Turkey	[redacted]	Residential	0.01	FALSE	[redacted]	1	1433	ms-sql-s	[redacted]	Unknown	FALSE	FALSE	Block	Info	1
[redacted]	United States	[redacted]	Hosting	45	FALSE	[redacted]	1299	80	http	[redacted]	HVAC	FALSE	FALSE	Warn	Warn	490.16
[redacted]	Vietnam	[redacted]	Residential	0.01	FALSE	[redacted]	6	25	smtp	[redacted]	Exchange	FALSE	FALSE	Warn	Info	2.79
[redacted]	Portugal	[redacted]	Cellular	0.01	TRUE	[redacted]	3	25	smtp	[redacted]	Exchange	FALSE	TRUE	Warn	Info	2.1
[redacted]	Germany	[redacted]	Residential	0.01	TRUE	[redacted]	6	25	smtp	[redacted]	Exchange	FALSE	TRUE	Warn	Info	2.79
[redacted]	Unknown	[redacted]	Unknown	0	FALSE	[redacted]	1	135	epmap	[redacted]	Business	FALSE	FALSE	Block	Critical	100
[redacted]	Unknown	[redacted]	Unknown	0	FALSE	[redacted]	1	135	epmap	[redacted]	Business	FALSE	FALSE	Block	Critical	100
[redacted]	Unknown	[redacted]	Unknown	0	FALSE	[redacted]	31	22	ssh	[redacted]	Business	FALSE	FALSE	Local	Critical	44.34
[redacted]	Unknown	[redacted]	Unknown	0	FALSE	[redacted]	30	22	ssh	[redacted]	Business	FALSE	FALSE	Local	Critical	44.01
[redacted]	Unknown	[redacted]	Unknown	0	FALSE	[redacted]	30	22	ssh	[redacted]	Business	FALSE	FALSE	Local	Critical	44.01
[redacted]	Unknown	[redacted]	Unknown	0	FALSE	[redacted]	2	22	ssh	[redacted]	Business	FALSE	FALSE	Local	Critical	16.93

Source IP	Protocol	Source Port	Destination IP	Destination Port	Hop Limit	Description	Action
Filter by source ip	Filter by protocol	Filter by source port	Filter by dest ip	Filter by dest port	>= Filter by hop limit		
	6	22	10.17.0.0/16	0	2	RL4 Server Port Client rule	
	6	22	10.17.0.0/16	0	2	RL4 Server Port Client rule	
	6	22	10.17.0.0/16	0	2	RL4 Server Port Client rule	
	6	22	10.30.0.0/16	0	5	RL4 Server Port Client rule	
	6	22	10.30.0.0/16	0	5	RL4 Server Port Client rule	
	6	22	10.30.0.0/16	0	5	RL4 Server Port Client rule	
	6	2222	192.168.0.0/16	0	3	RL4 Server Port Client rule	
	6	2222	192.168.0.0/16	0	3	RL4 Server Port Client rule	

Sphere of Trust™ Agent works with the HOPZERO Portal to understand and control Data Travel on individual servers.

Proactively blocking data exfiltration and alarm on attempts.

Learn more about Exfiltration Prevention and Data Containment at **https://hopzero.com/Agent**

HOPZERO

11400 Concordia University Dr.
Austin, TX 78726
833-467-9376
inquire@hopzero.com

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.

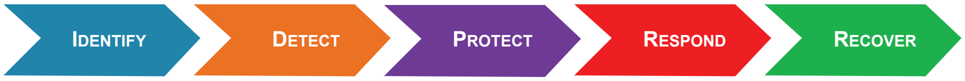
HOPZERO DataTravel™ Security

EXFILTRATION RISK AUDIT

Traditional Threat Assessments test how well your security systems block 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 data that 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 HOPZERO Data Exfiltration Visibility System removes the cloak and identifies the outbound activity like turning on a light in a dark room.

CYBERSECURITY FRAMEWORK

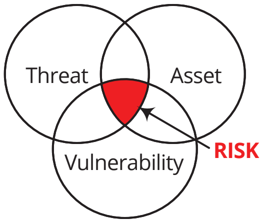


IDENTIFY → DETECT → PROTECT → RESPOND → RECOVER

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 the right security tools to help you do just that. Risk can be prevented with HOPZERO security 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.

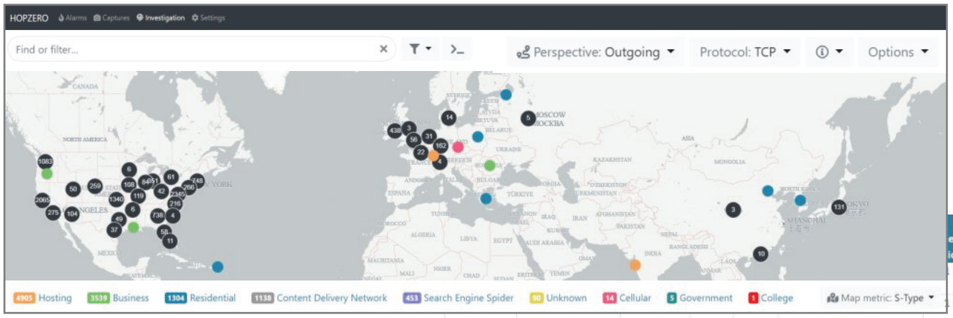
Exfiltration Assessment and Verification

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

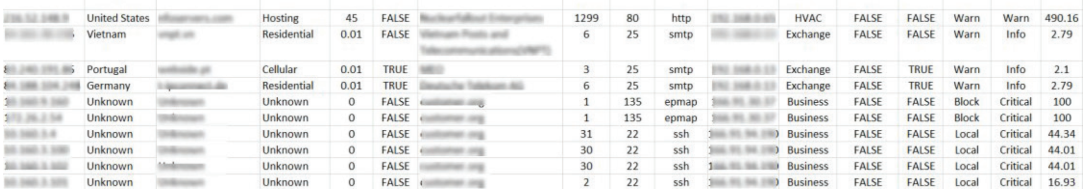
- Reports for discovered Exfiltration
- Verification of implemented controls
- Identification of control weaknesses
- Actionable recommendations for improvement
- Regulatory information for auditors

Every company has IT security controls in place but need a way to verify that those controls are effective and preventing dat a 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 receive a comprehensive review of your data exfiltration security posture.



The Exfiltration Risk Audit is performed using our HOPZERO Portal, Agent and Collector products. Customers can purchase these same products working in their networks.

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



							er ions	App Port	App Name	Server IP	Server Type	Server Hosting	Server EU	Hop Policy	Hop Severity	Risk Score
							1	1433	ms-sql-s	[redacted]	Hosting	TRUE	FALSE	Block	Critical	100.01
							1	1433	ms-sql-s	[redacted]	Unknown	FALSE	FALSE	Block	Info	1
[redacted]	United States	[redacted]	Hosting	45	FALSE	[redacted]	1299	80	http	[redacted]	HVAC	FALSE	FALSE	Warn	Warn	490.16
[redacted]	Vietnam	[redacted]	Residential	0.01	FALSE	[redacted]	6	25	smtp	[redacted]	Exchange	FALSE	FALSE	Warn	Info	2.79
[redacted]	Portugal	[redacted]	Cellular	0.01	TRUE	[redacted]	3	25	smtp	[redacted]	Exchange	FALSE	TRUE	Warn	Info	2.1
[redacted]	Germany	[redacted]	Residential	0.01	TRUE	[redacted]	6	25	smtp	[redacted]	Exchange	FALSE	TRUE	Warn	Info	2.79
[redacted]	Unknown	[redacted]	Unknown	0	FALSE	[redacted]	1	135	epmap	[redacted]	Business	FALSE	FALSE	Block	Critical	100
[redacted]	Unknown	[redacted]	Unknown	0	FALSE	[redacted]	1	135	epmap	[redacted]	Business	FALSE	FALSE	Block	Critical	100
[redacted]	Unknown	[redacted]	Unknown	0	FALSE	[redacted]	31	22	ssh	[redacted]	Business	FALSE	FALSE	Local	Critical	44.34
[redacted]	Unknown	[redacted]	Unknown	0	FALSE	[redacted]	30	22	ssh	[redacted]	Business	FALSE	FALSE	Local	Critical	44.01
[redacted]	Unknown	[redacted]	Unknown	0	FALSE	[redacted]	30	22	ssh	[redacted]	Business	FALSE	FALSE	Local	Critical	44.01
[redacted]	Unknown	[redacted]	Unknown	0	FALSE	[redacted]	2	22	ssh	[redacted]	Business	FALSE	FALSE	Local	Critical	16.93

HOPZERO

11400 Concordia University Dr.
Austin, TX 78726
833-467-9376
inquire@hopzero.com

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