



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

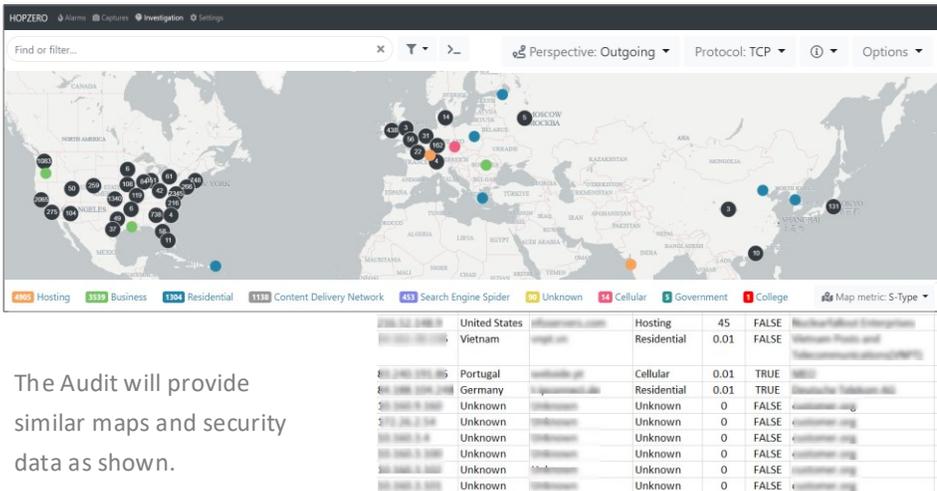
Exfiltration Assessment and Verification

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.



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

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

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

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

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.