SolarWinds Breach

SolarWinds Case Study with Packet Analysis Exhibits

Bill.Alderson@Cogent.Management

SharkFest'23 US
Wireshark Developer and User Conference • San Diego, CA • June 10-15

Packetman007

Course PDF https://Cogent.Management/SharkFestSolarWinds

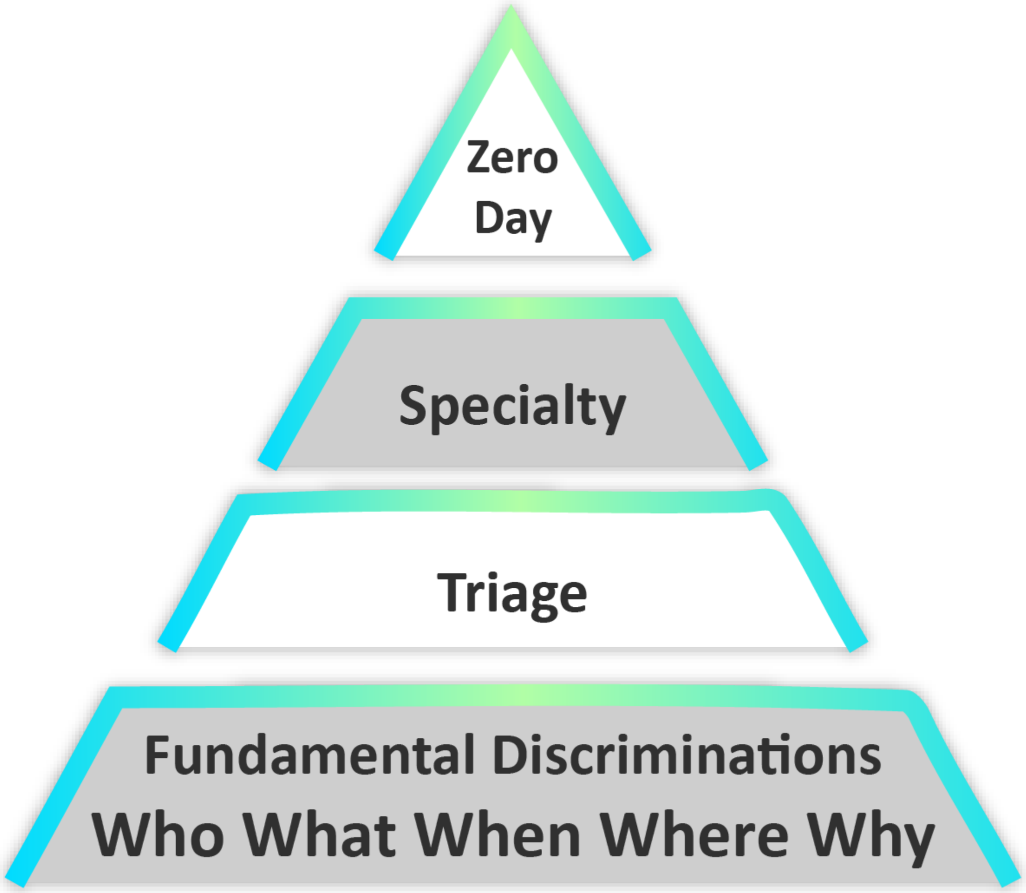
SECURITY INSTITUTE

SolarWinds – Security Breach Analysis

Eleven evading steps to compromise

8-part series

Security Analysis Hierarchy

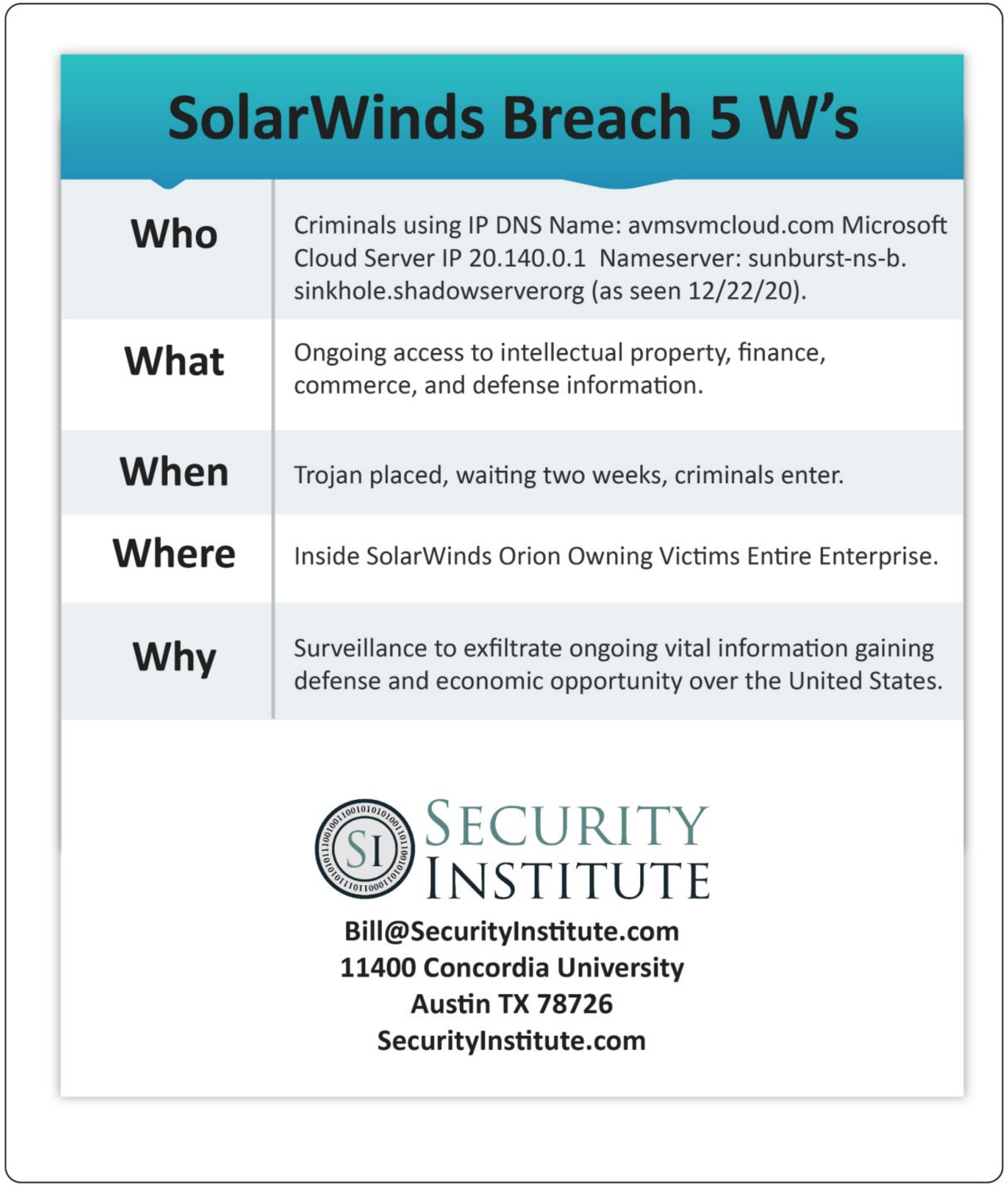


Zero Day

Specialty

Triage

Fundamental Discriminations
Who What When Where Why



SolarWinds Breach 5 W's

Who	Criminals using IP DNS Name: avmsvmcloud.com Microsoft Cloud Server IP 20.140.0.1 Nameserver: sunburst-ns-b. sinkhole.shadowserverorg (as seen 12/22/20).
What	Ongoing access to intellectual property, finance, commerce, and defense information.
When	Trojan placed, waiting two weeks, criminals enter.
Where	Inside SolarWinds Orion Owning Victims Entire Enterprise.
Why	Surveillance to exfiltrate ongoing vital information gaining defense and economic opportunity over the United States.

SI SECURITY INSTITUTE

Bill@SecurityInstitute.com
11400 Concordia University
Austin TX 78726
SecurityInstitute.com

Anatomy of a Massive Data Breach

Part 1

SolarWinds Software

SolarWinds is monitoring software that does not itself hold high value data

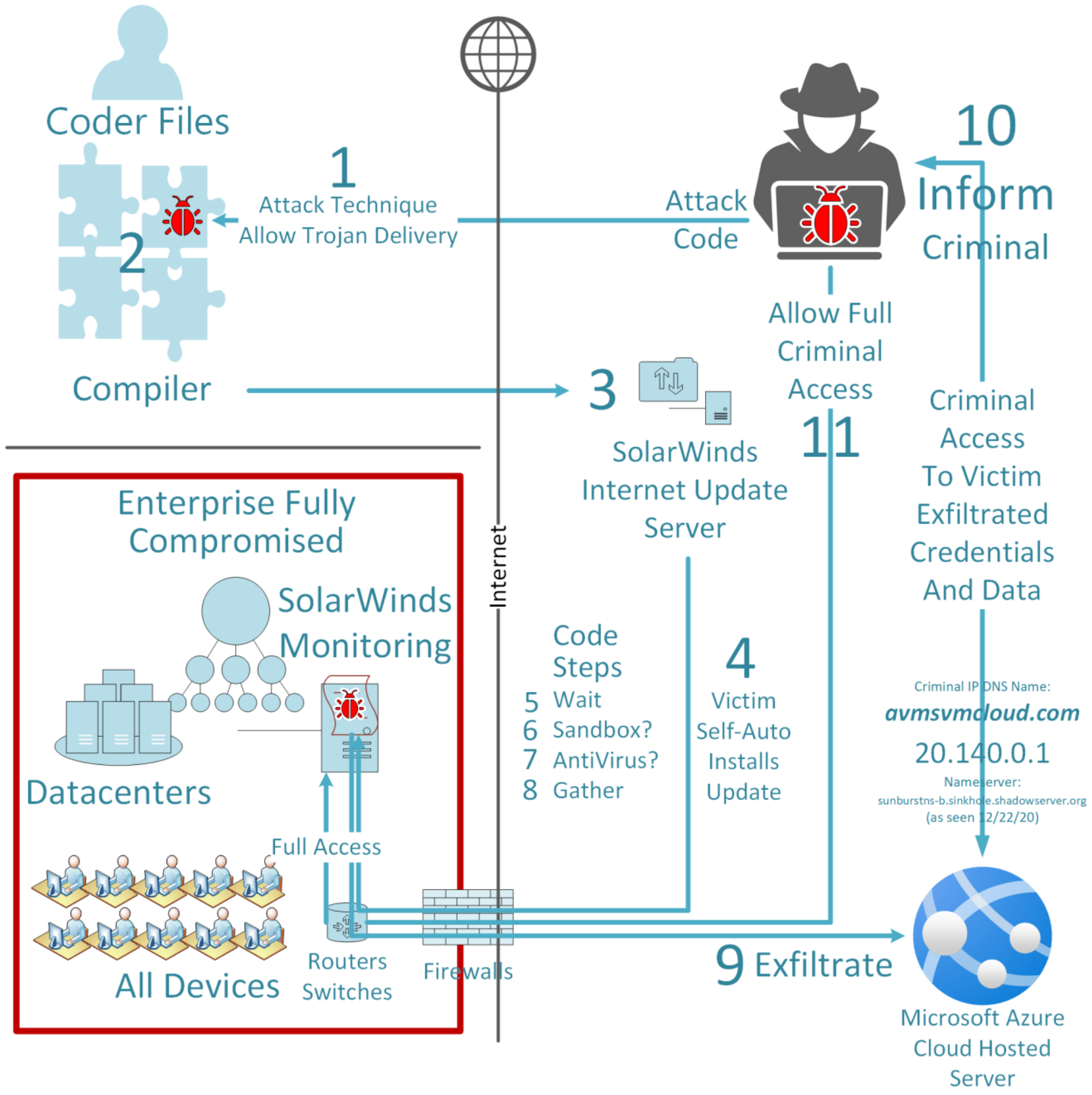
Requires all access to customer security credentials to firewalls, SQL servers, workstations and routers for deep internal monitoring

Due to all access pass, it is an excellent back door to exploit secured information if breached

Eleven Steps to Breach – part 1

- Criminals insert Rogue code disguised as a general software update
- Get the code directly into the general victim's server
- Latency in release to avoid detection
- Avoid detection hiding the breach

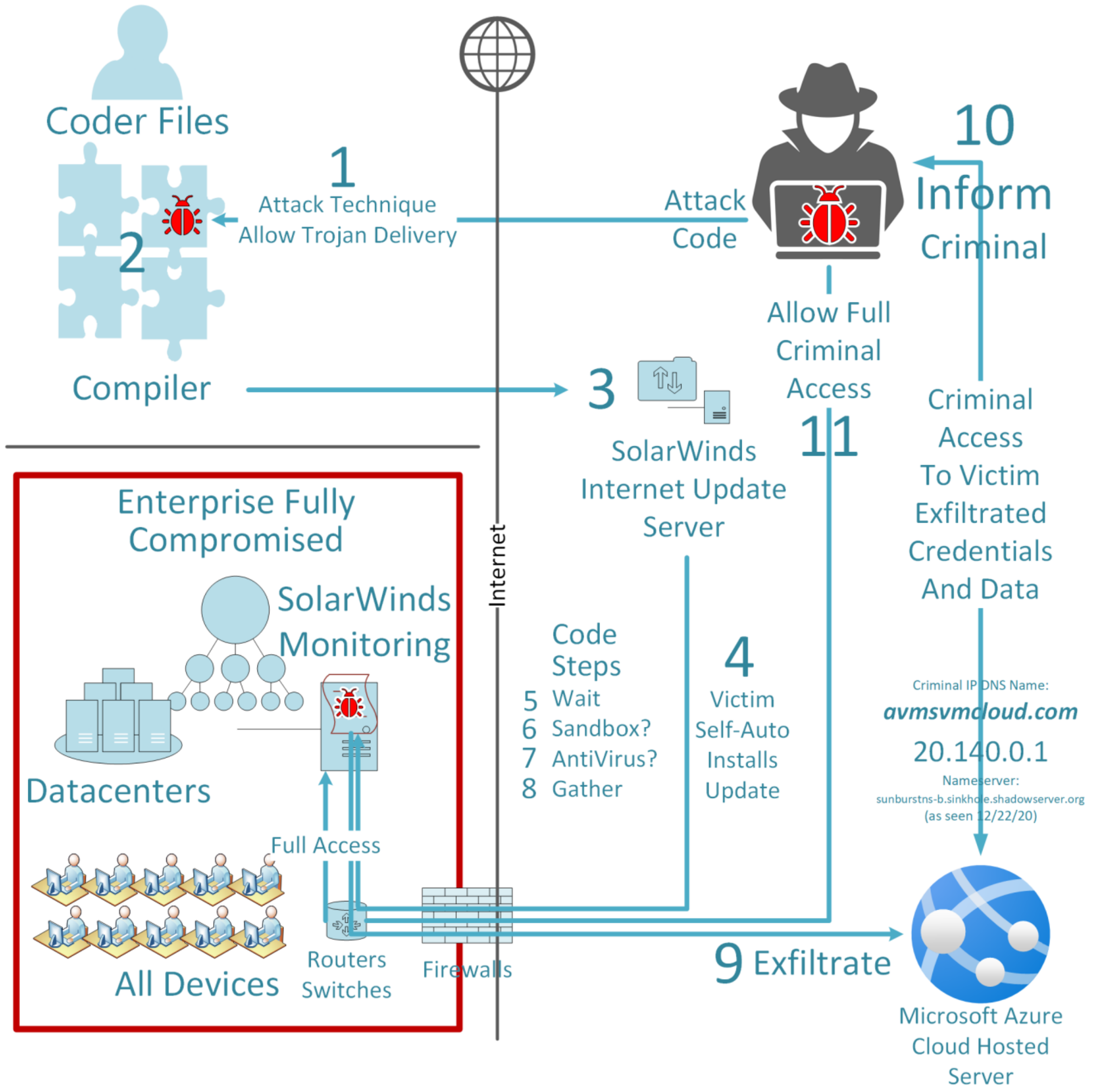
SolarWinds 11 Breach Steps



Eleven Steps to Breach – part 2

- Once in data is gathered
- Data Exfiltration
- Criminals have access
- Additional exploits and trojans placed

SolarWinds 11 Breach Steps



Coder Files

1 Attack Technique Allow Trojan Delivery

Attack Code

10 Inform Criminal

2

Compiler

3

Allow Full Criminal Access

11

SolarWinds Internet Update Server

Criminal Access To Victim Exfiltrated Credentials And Data

Enterprise Fully Compromised

SolarWinds Monitoring

Internet

Datacenters

Code Steps
5 Wait
6 Sandbox?
7 AntiVirus?
8 Gather

4 Victim Self-Auto Installs Update

Criminal IP DNS Name:
avmsvmcloud.com
20.140.0.1
Nameserver:
sunburstns-b.sinkhole.shadowserver.org
(as seen 12/22/20)

Full Access

All Devices

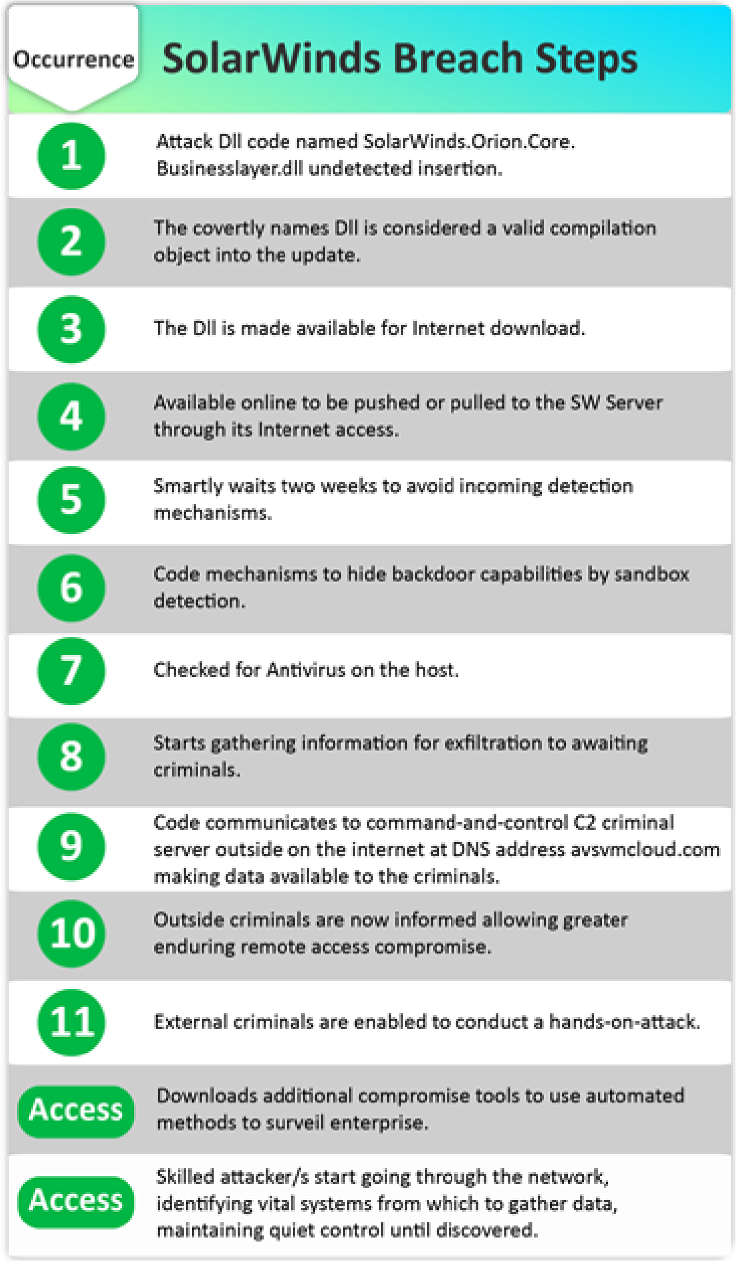
Routers Switches

Firewalls

9 Exfiltrate

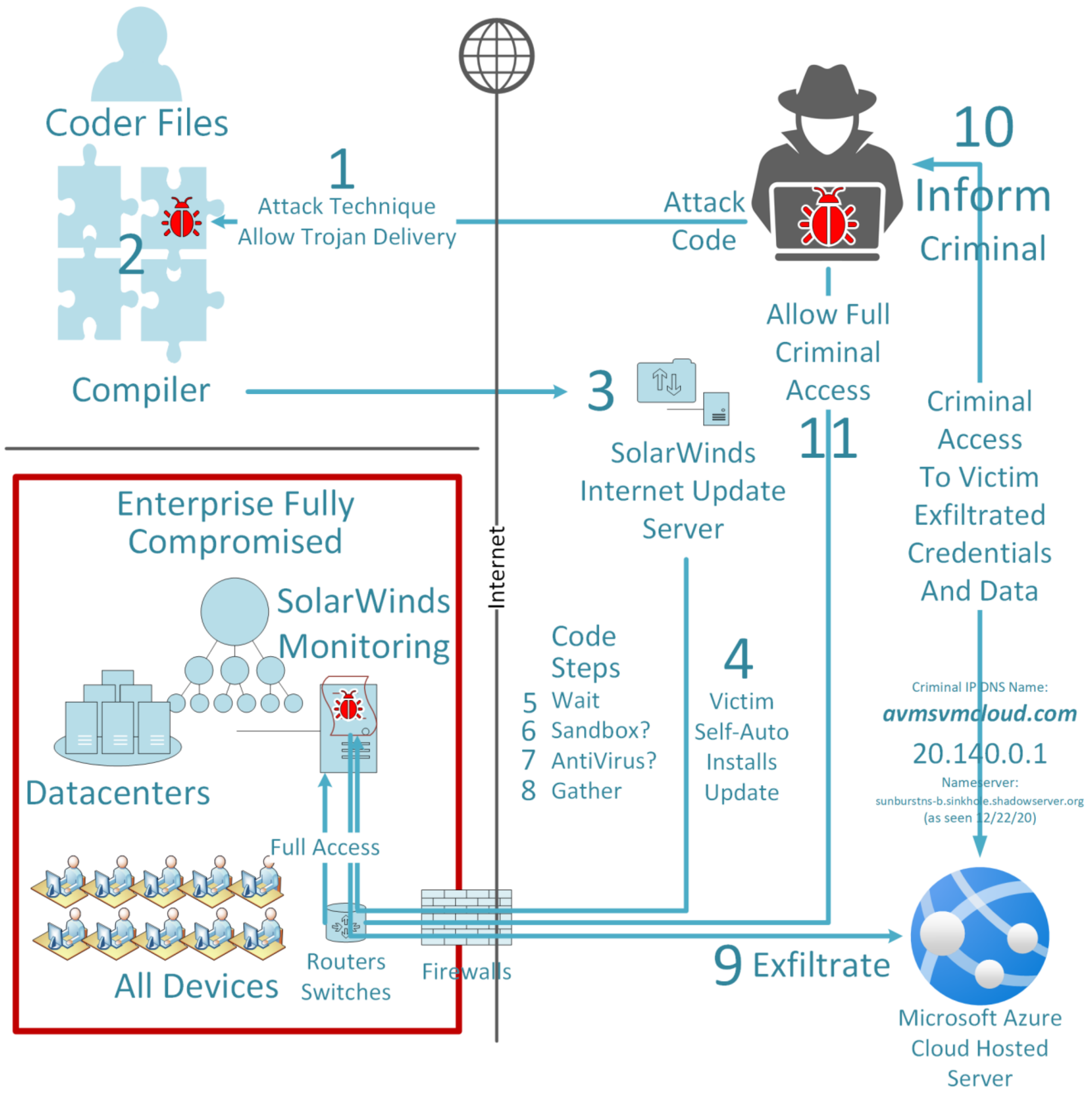
Microsoft Azure Cloud Hosted Server

Anatomy of a Massive Breach



Occurrence	SolarWinds Breach Steps
1	Attack Dll code named SolarWinds.Orion.Core. Businesslayer.dll undetected insertion.
2	The covertly names Dll is considered a valid compilation object into the update.
3	The Dll is made available for Internet download.
4	Available online to be pushed or pulled to the SW Server through its Internet access.
5	Smartly waits two weeks to avoid incoming detection mechanisms.
6	Code mechanisms to hide backdoor capabilities by sandbox detection.
7	Checked for Antivirus on the host.
8	Starts gathering information for exfiltration to awaiting criminals.
9	Code communicates to command-and-control C2 criminal server outside on the internet at DNS address avsvmcloud.com making data available to the criminals.
10	Outside criminals are now informed allowing greater enduring remote access compromise.
11	External criminals are enabled to conduct a hands-on-attack.
Access	Downloads additional compromise tools to use automated methods to surveil enterprise.
Access	Skilled attacker/s start going through the network, identifying vital systems from which to gather data, maintaining quiet control until discovered.

SolarWinds 11 Breach Steps



Danger of Direct Internet Updates

Part 2

Danger of Direct Internet Updates

Currently companies

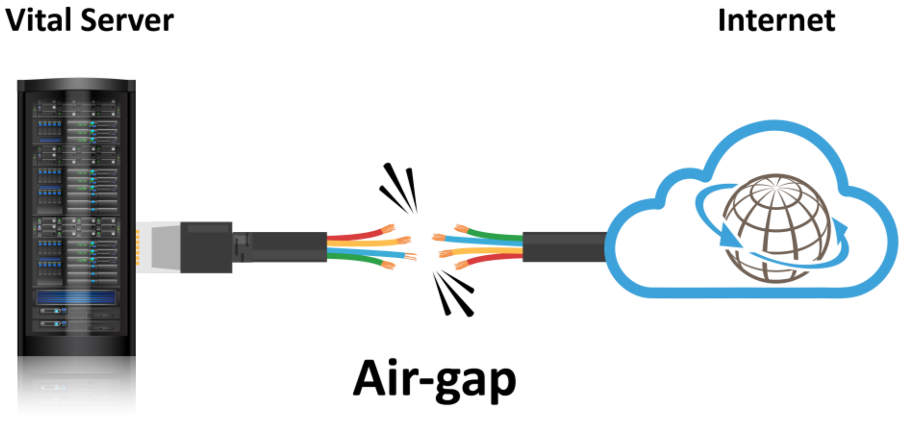
- Depend on “certification by brand security”
- Consider firewalls as high security
- Air gapping not a practiced security method

Brand’s keep Internet access wide open to allow automatic direct updates making work easy, but insecure

Direct Internet access was a vital part for the rogue code that breached SolarWinds software

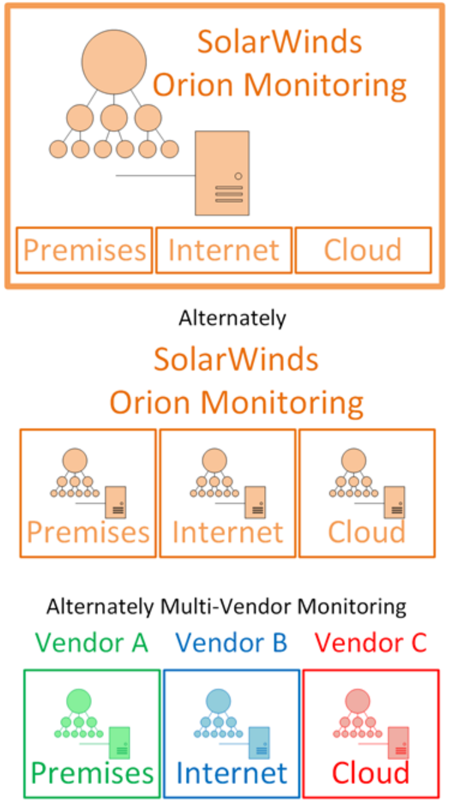
“Automatic Internet updates are akin to having your coffee maker automatically add cream and sugar”

Danger of Direct Internet Updates



Danger of Monitoring In One "all access" Platform

- Premises
- Internet
- Cloud



Reasons Internet Access May Have Allowed SolarWinds Attack

1. Victims would not have been able to directly download the update, automatically or otherwise. If an internal Update Server was used, increased scrutiny may have prevented placement on an internal hardened Update Server.

2. Criminals may have used a backchannel from SolarWinds Internet Update to reach back into the Coder's compiler files allowing Trojan code to be placed. Simply reversing direction, the Coder used to place a file on the Internet for download might have been the path for reverse insertion.

3. Trojan code may have failed its DNS lookup Sandbox test to Api.solarwinds.com. A Vital Server should not have access to External Internet DNS, it should resolve to an internal DNS server maintained to include mission critical records and exclude known risky Internet-wide DNS records which may have stopped access to the amsvmcloud.com criminal DNS entry. Notice the DNS Nameserver's name.

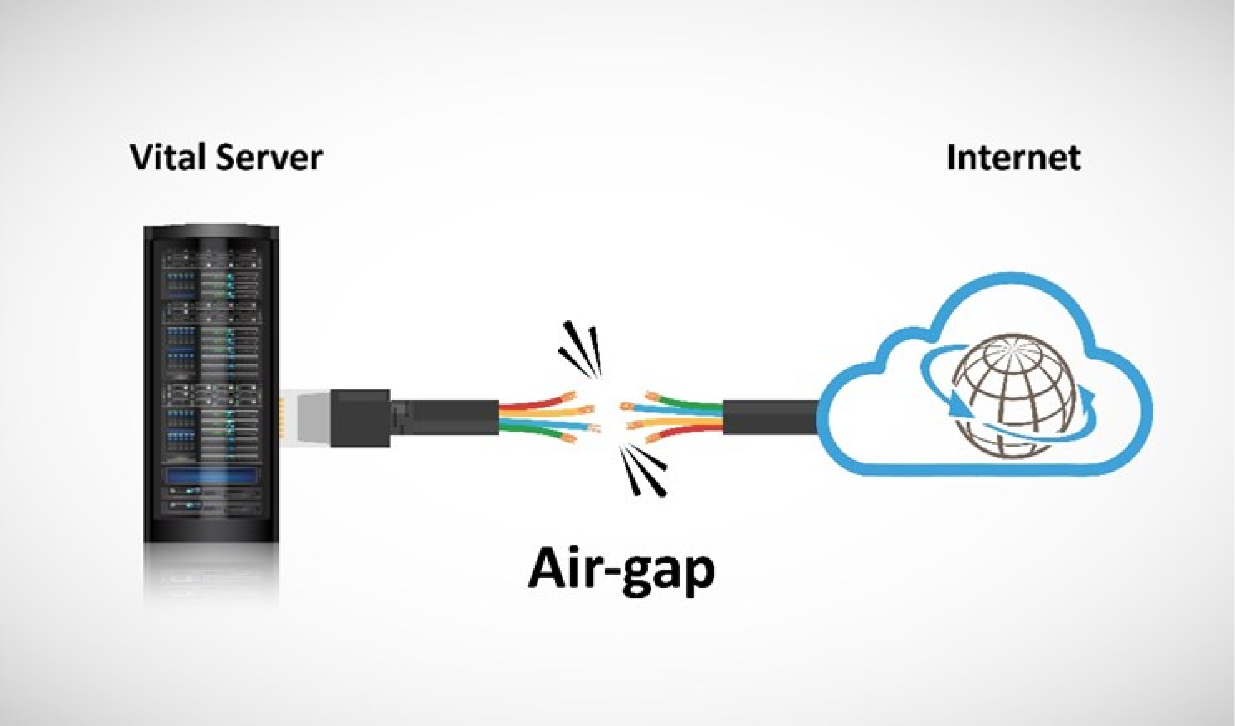
4. If the Sandbox test included a communications access check to reach api.solarwinds.com before launching attack, it would have failed.

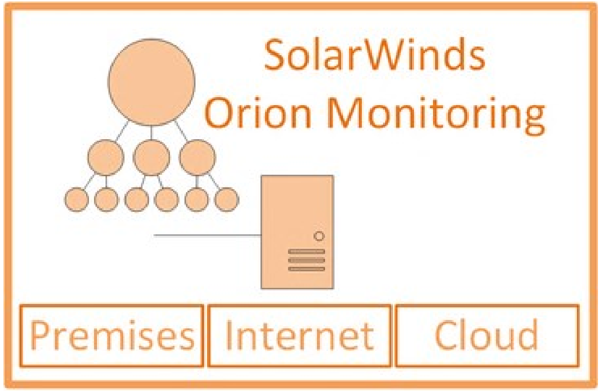
5. Exfiltration to the Internet Hosted Microsoft Azure Server avmsvmcloud.com would have failed preventing the Attacker from getting or using information gathered from the inside altogether.

Reducing Risk of Internet Updates and Centralized Monitoring

Enterprise solutions for Air-gapping

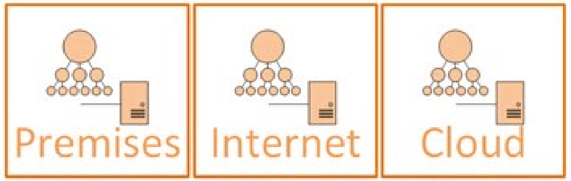
- Windows Security Update Server (WSUS)
- System Control Update Centre (SCUC)
- Internal network patch manager product by SolarWinds



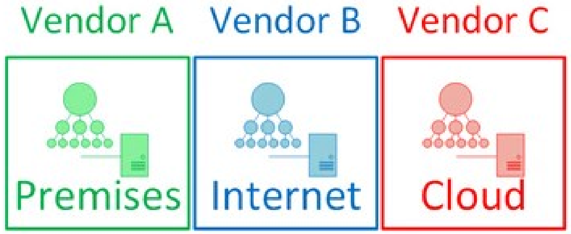


Alternately

SolarWinds
Orion Monitoring



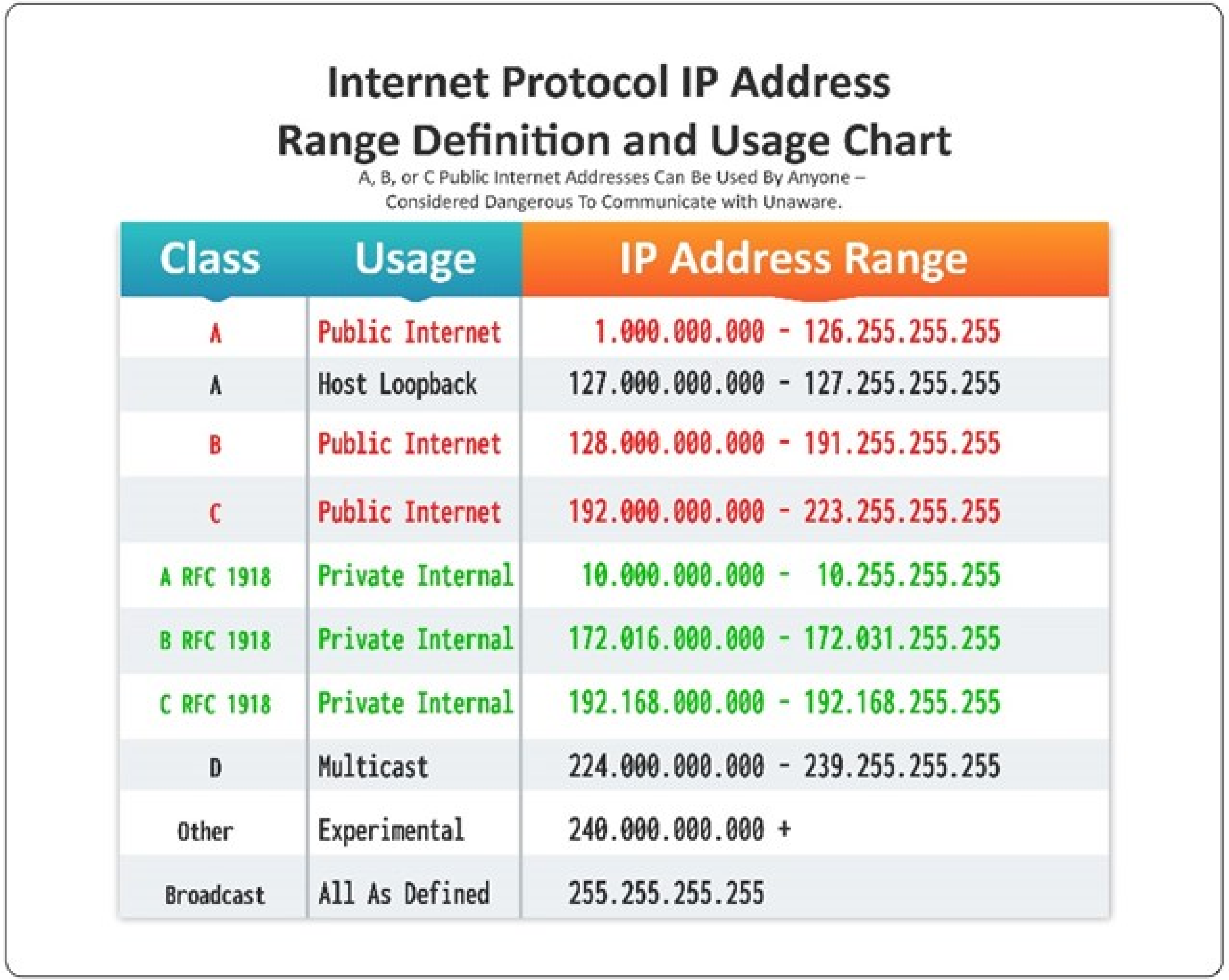
Alternately Multi-Vendor Monitoring



Four Communications Perspectives of a Vital Server

Part 3

Multiple Directional Perspectives



Internet Protocol IP Address Range Definition and Usage Chart

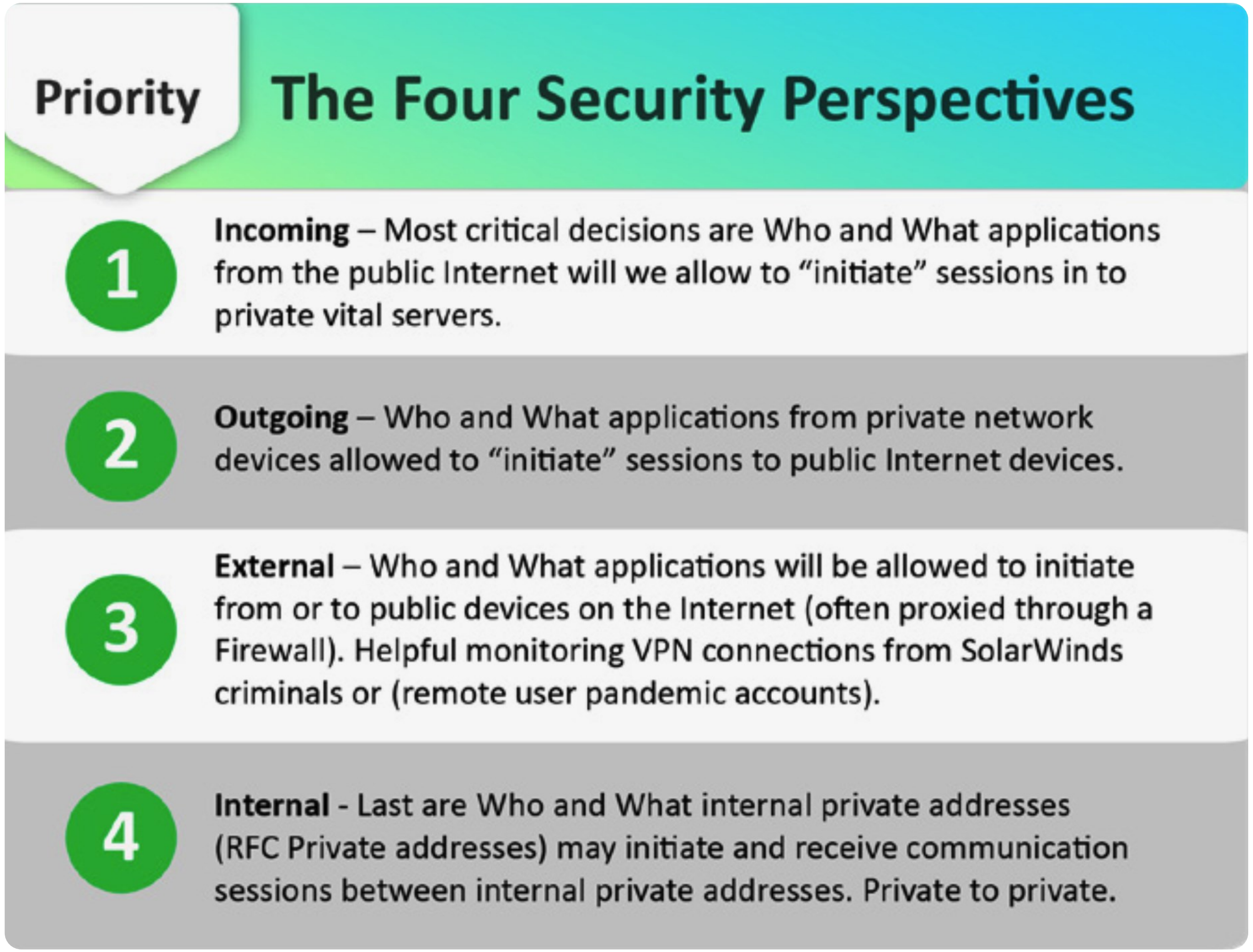
A, B, or C Public Internet Addresses Can Be Used By Anyone –
Considered Dangerous To Communicate with Unaware.

Class	Usage	IP Address Range
A	Public Internet	1.000.000.000 - 126.255.255.255
A	Host Loopback	127.000.000.000 - 127.255.255.255
B	Public Internet	128.000.000.000 - 191.255.255.255
C	Public Internet	192.000.000.000 - 223.255.255.255
A RFC 1918	Private Internal	10.000.000.000 - 10.255.255.255
B RFC 1918	Private Internal	172.016.000.000 - 172.031.255.255
C RFC 1918	Private Internal	192.168.000.000 - 192.168.255.255
D	Multicast	224.000.000.000 - 239.255.255.255
Other	Experimental	240.000.000.000 +
Broadcast	All As Defined	255.255.255.255

There are 4 perspectives that require evaluation to identify security threats

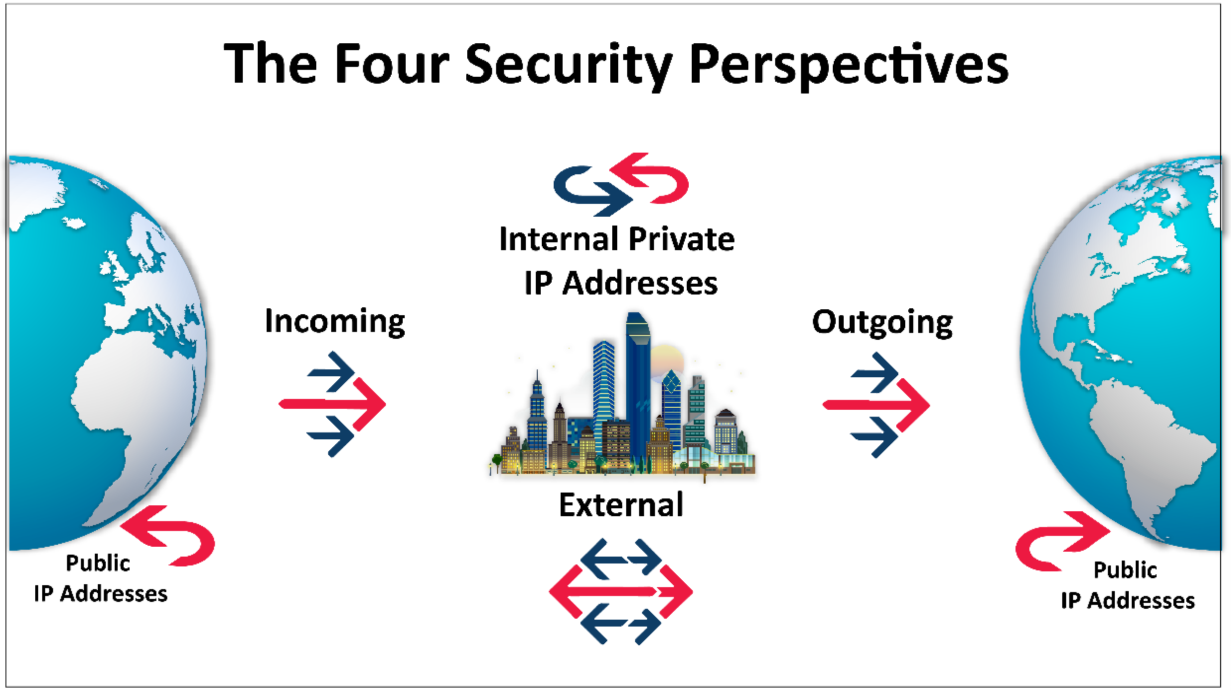
Four Communications Perspectives of a Vital Server

Building in security control protocols into to each aspect can decrease the likelihood of a breach

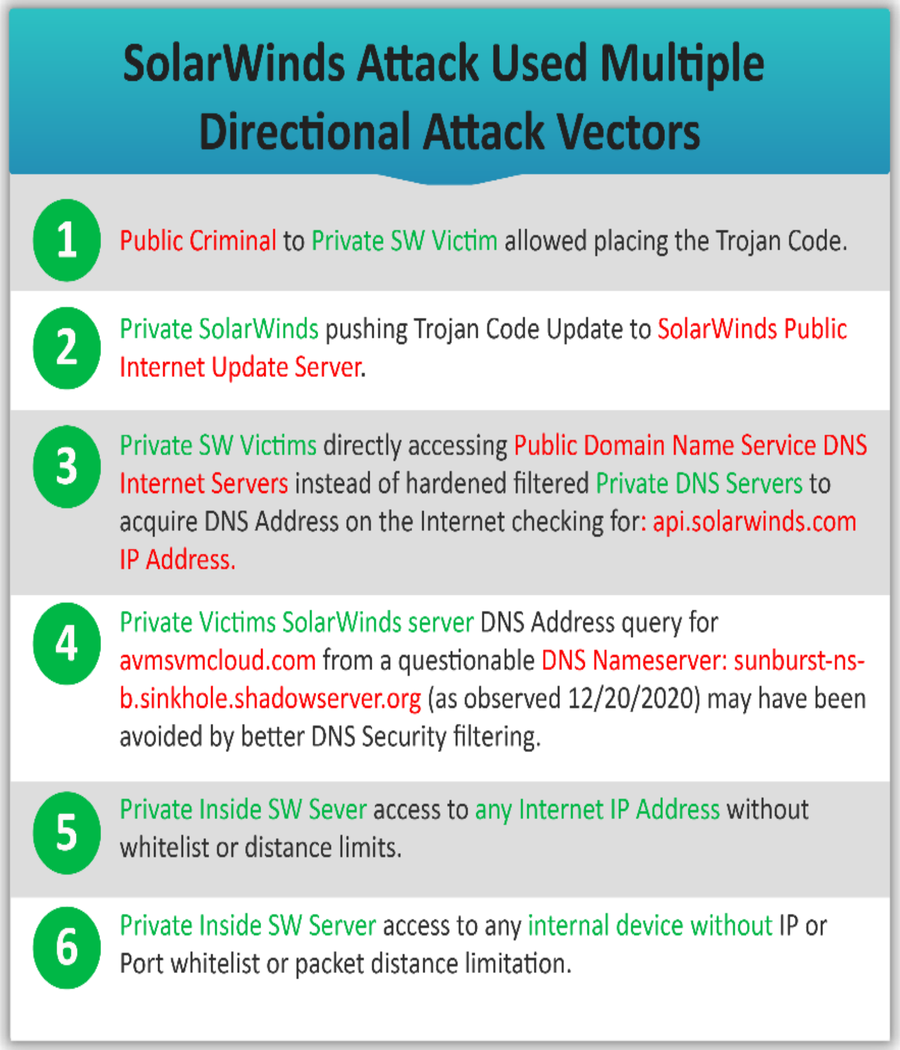


Priority	The Four Security Perspectives
1	**Incoming** – Most critical decisions are Who and What applications from the public Internet will we allow to "initiate" sessions in to private vital servers.
2	**Outgoing** – Who and What applications from private network devices allowed to "initiate" sessions to public Internet devices.
3	**External** – Who and What applications will be allowed to initiate from or to public devices on the Internet (often proxied through a Firewall). Helpful monitoring VPN connections from SolarWinds criminals or (remote user pandemic accounts).
4	**Internal** - Last are Who and What internal private addresses (RFC Private addresses) may initiate and receive communication sessions between internal private addresses. Private to private.

Multiple Directional Attacks used in the SolarWinds Breach



Limitations should be introduced to disrupt criminal vectors at each stage that SolarWinds attack software infiltrated



SolarWinds Attack Used Multiple Directional Attack Vectors

1 Public Criminal to Private SW Victim allowed placing the Trojan Code.

2 Private SolarWinds pushing Trojan Code Update to SolarWinds Public Internet Update Server.

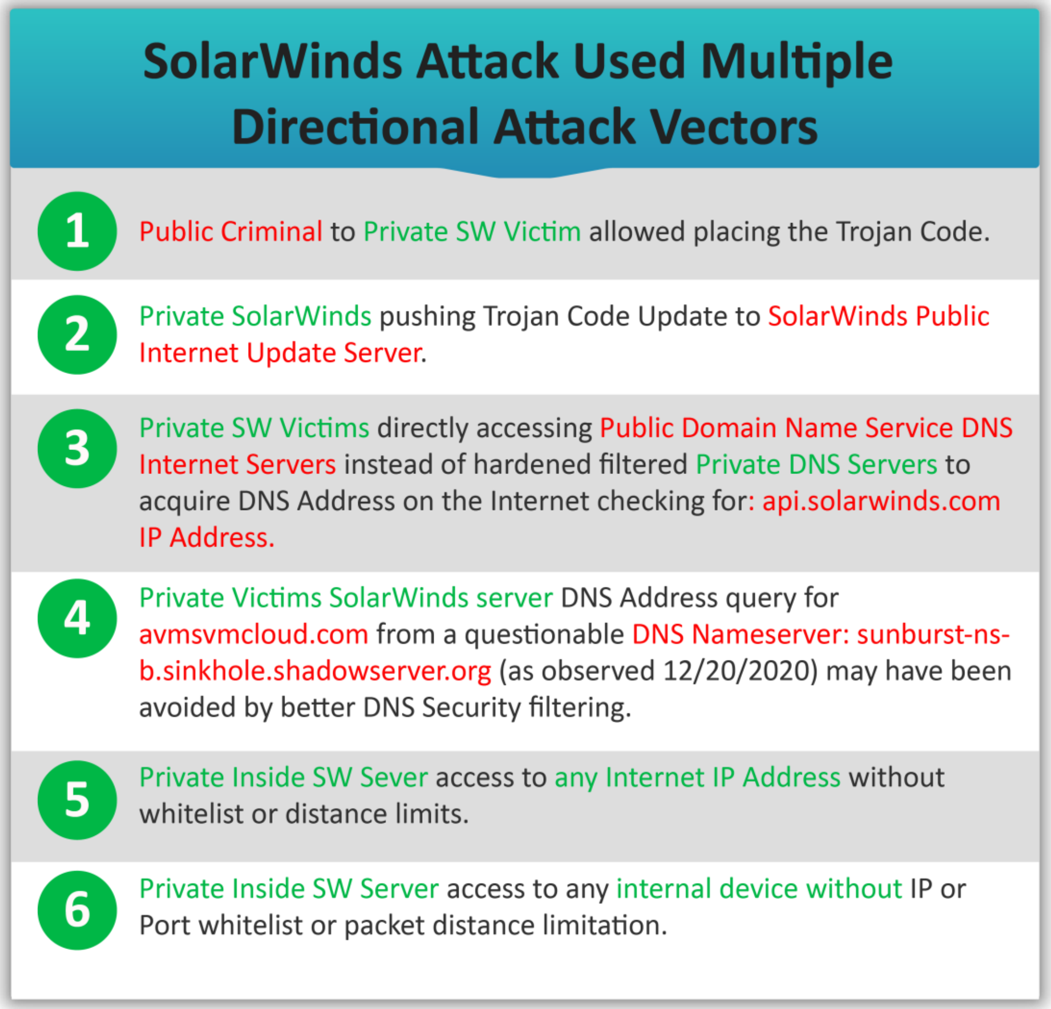
3 Private SW Victims directly accessing Public Domain Name Service DNS Internet Servers instead of hardened filtered Private DNS Servers to acquire DNS Address on the Internet checking for: api.solarwinds.com IP Address.

4 Private Victims SolarWinds server DNS Address query for avmsvmcloud.com from a questionable DNS Nameserver: sunburst-ns-b.sinkhole.shadowserver.org (as observed 12/20/2020) may have been avoided by better DNS Security filtering.

5 Private Inside SW Sever access to any Internet IP Address without whitelist or distance limits.

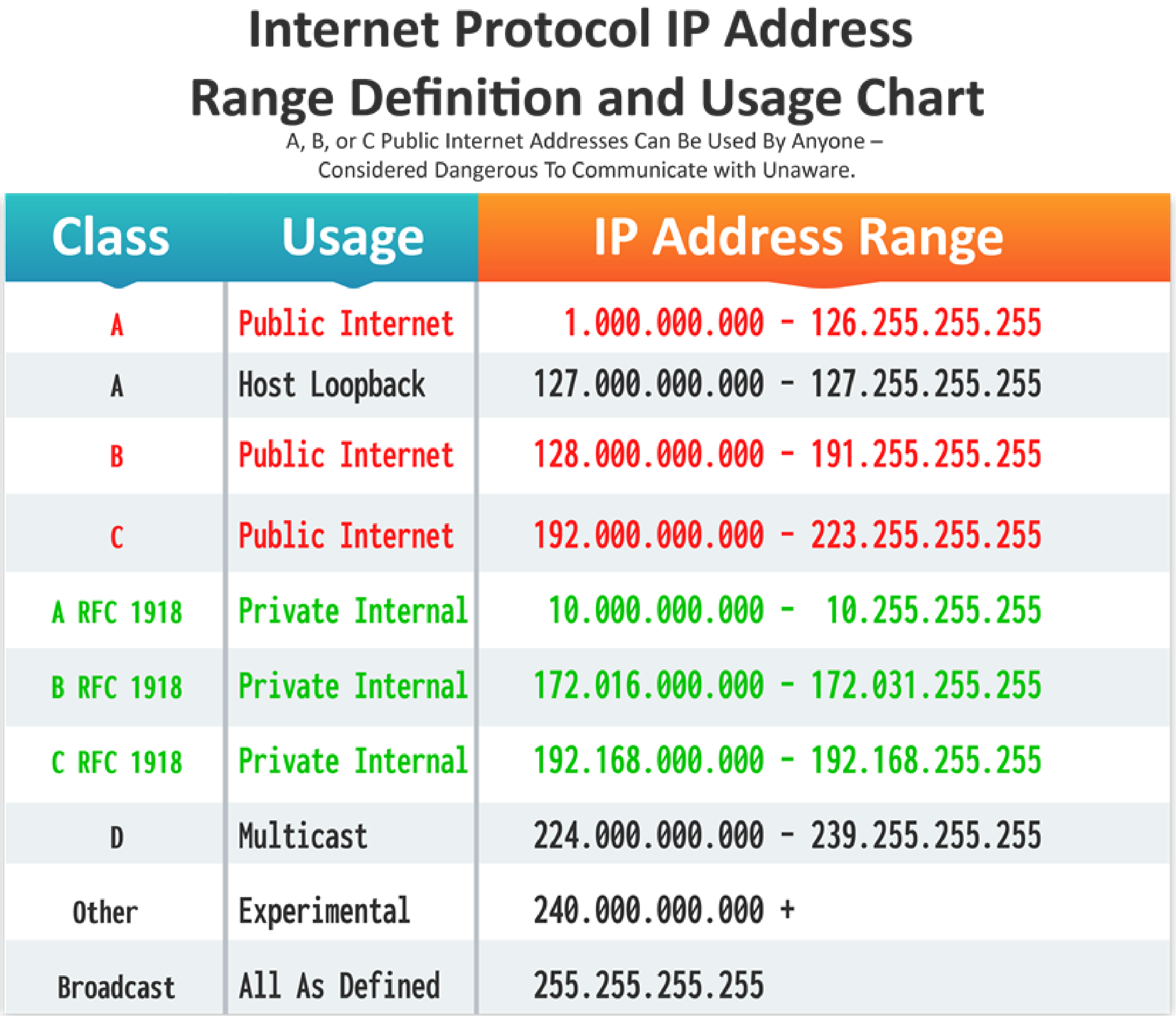
6 Private Inside SW Server access to any internal device without IP or Port whitelist or packet distance limitation.

Four Communications Perspectives of a Vital Server



SolarWinds Attack Used Multiple Directional Attack Vectors

1. Public Criminal to Private SW Victim allowed placing the Trojan Code.
2. Private SolarWinds pushing Trojan Code Update to SolarWinds Public Internet Update Server.
3. Private SW Victims directly accessing Public Domain Name Service DNS Internet Servers instead of hardened filtered Private DNS Servers to acquire DNS Address on the Internet checking for: api.solarwinds.com IP Address.
4. Private Victims SolarWinds server DNS Address query for avmsvmcloud.com from a questionable DNS Nameserver: sunburst-ns-b.sinkhole.shadowserver.org (as observed 12/20/2020) may have been avoided by better DNS Security filtering.
5. Private Inside SW Sever access to any Internet IP Address without whitelist or distance limits.
6. Private Inside SW Server access to any internal device without IP or Port whitelist or packet distance limitation.



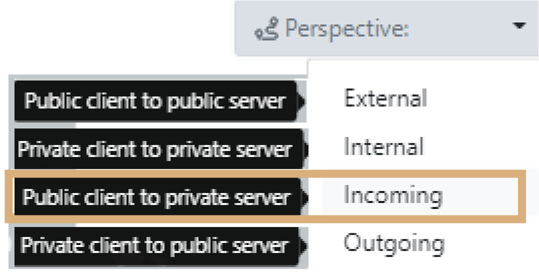
Internet Protocol IP Address Range Definition and Usage Chart

A, B, or C Public Internet Addresses Can Be Used By Anyone –
Considered Dangerous To Communicate with Unaware.

Class	Usage	IP Address Range
A	Public Internet	1.000.000.000 - 126.255.255.255
A	Host Loopback	127.000.000.000 - 127.255.255.255
B	Public Internet	128.000.000.000 - 191.255.255.255
C	Public Internet	192.000.000.000 - 223.255.255.255
A RFC 1918	Private Internal	10.000.000.000 - 10.255.255.255
B RFC 1918	Private Internal	172.016.000.000 - 172.031.255.255
C RFC 1918	Private Internal	192.168.000.000 - 192.168.255.255
D	Multicast	224.000.000.000 - 239.255.255.255
Other	Experimental	240.000.000.000 +
Broadcast	All As Defined	255.255.255.255

Incoming Traffic

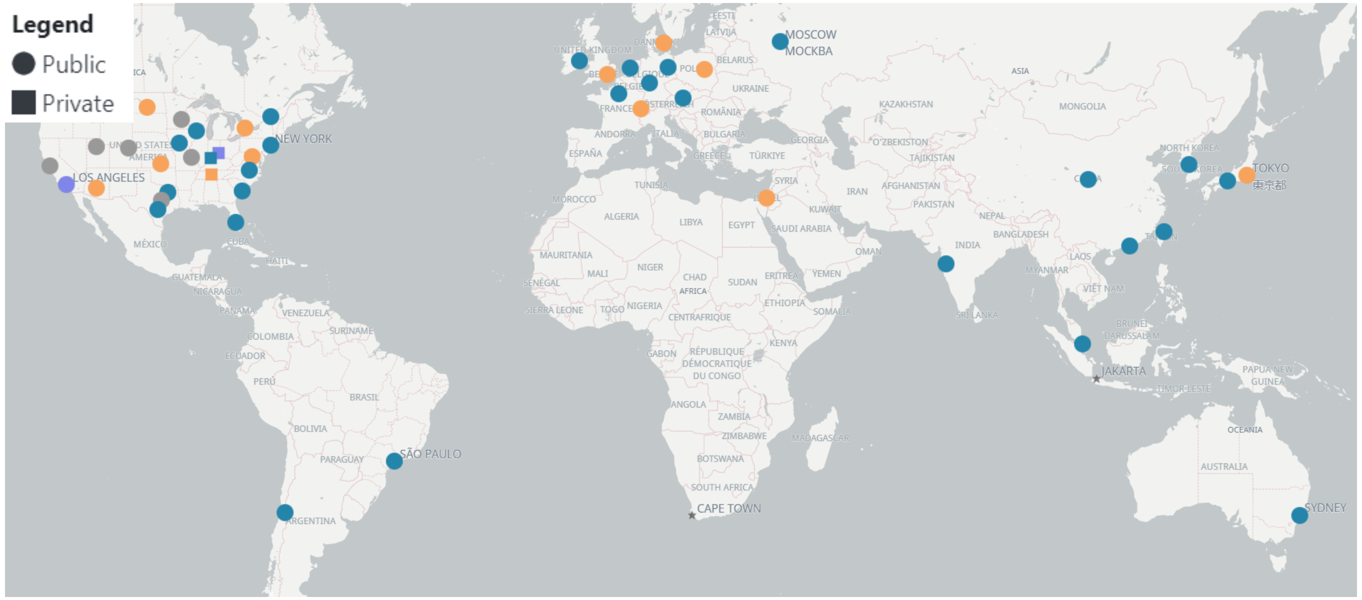
Incoming, the most dangerous direction. What can get through your firewall to your vital servers? If volume exploited it can create a denial of service of your Internet, Firewall, Network and Vital Servers.



Perspective:

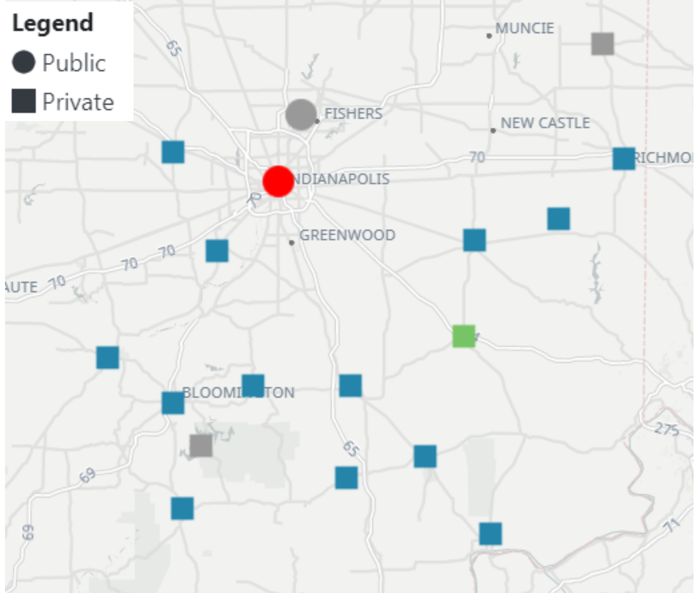
Public client to public server	External
Private client to private server	Internal
Public client to private server	Incoming
Private client to public server	Outgoing

Internet Devices



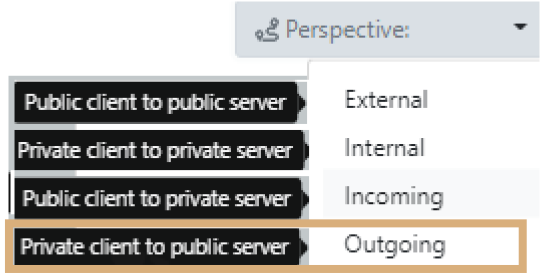
Incoming

Internal Devices



Outgoing Traffic

Outgoing, sessions initiated from trusted inside - can return like a boomerang, with Phish, Ransomware and other viral media. Today's traffic is encrypted – you can't see it until it's too late.

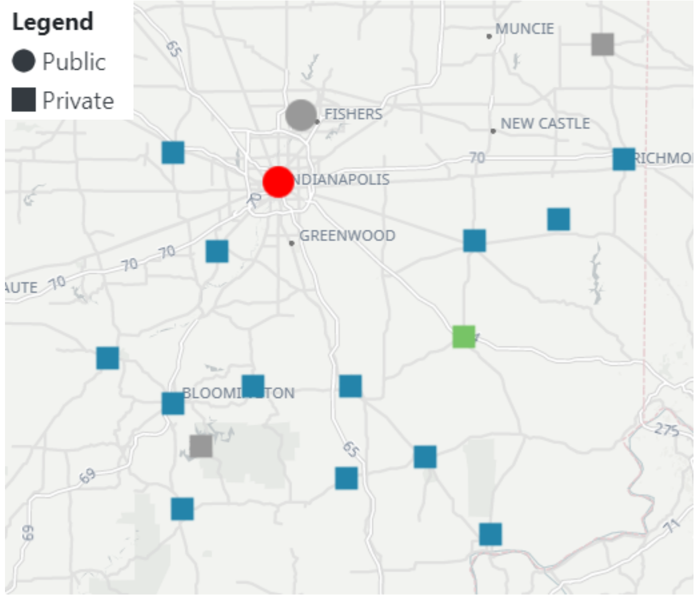


Perspective:

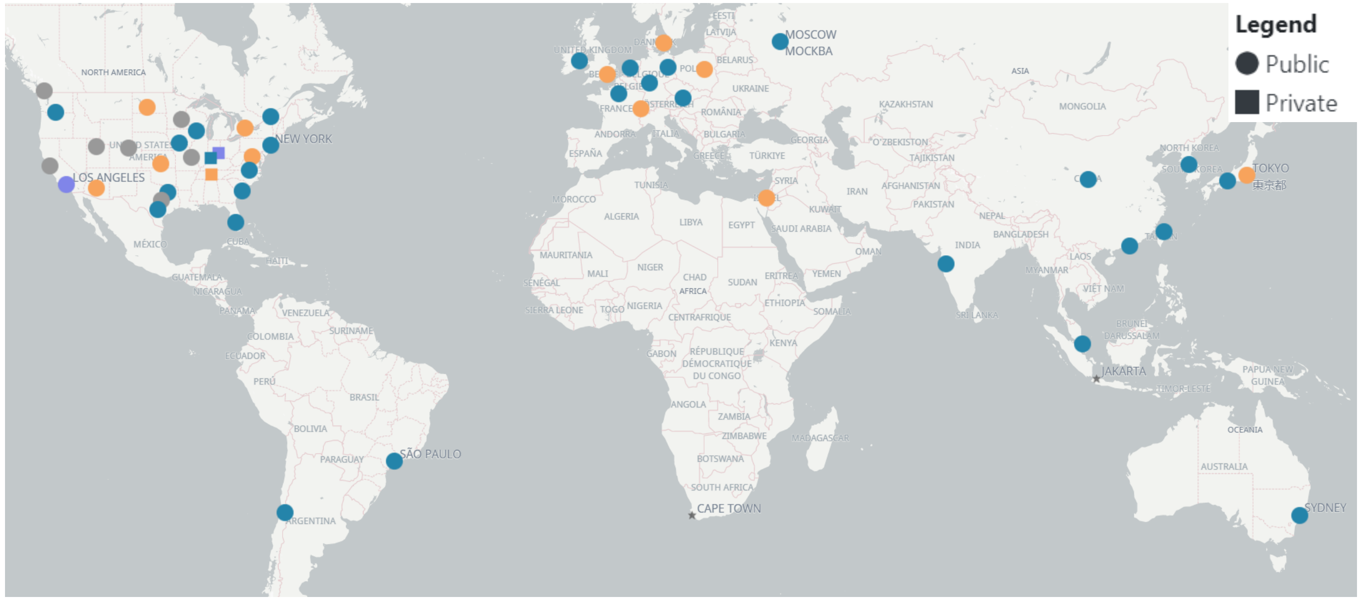
Public client to public server	External
Private client to private server	Internal
Public client to private server	Incoming
Private client to public server	Outgoing

Internal Devices

External Internet Devices

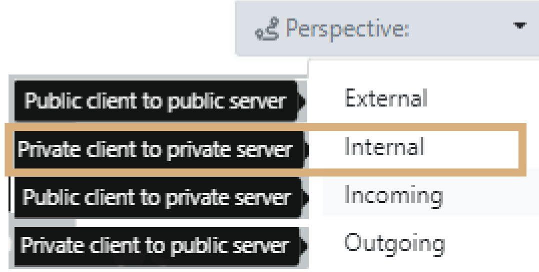


Outgoing



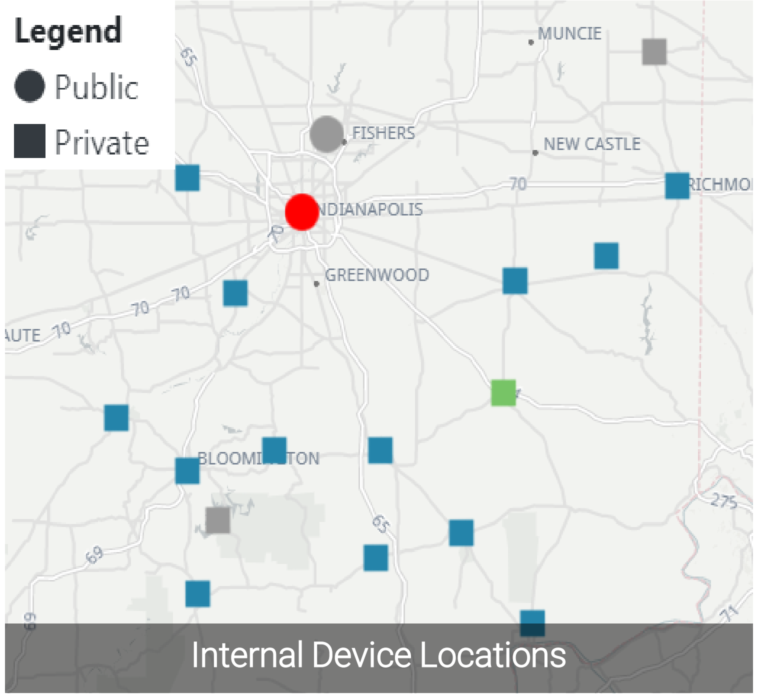
Internal Private Traffic

Once Ransomware, Phish is inside – it replicates on your internal network. Seeing a user machine or a server suddenly communicate with many others, or massive traffic provides the clues to shut it down.



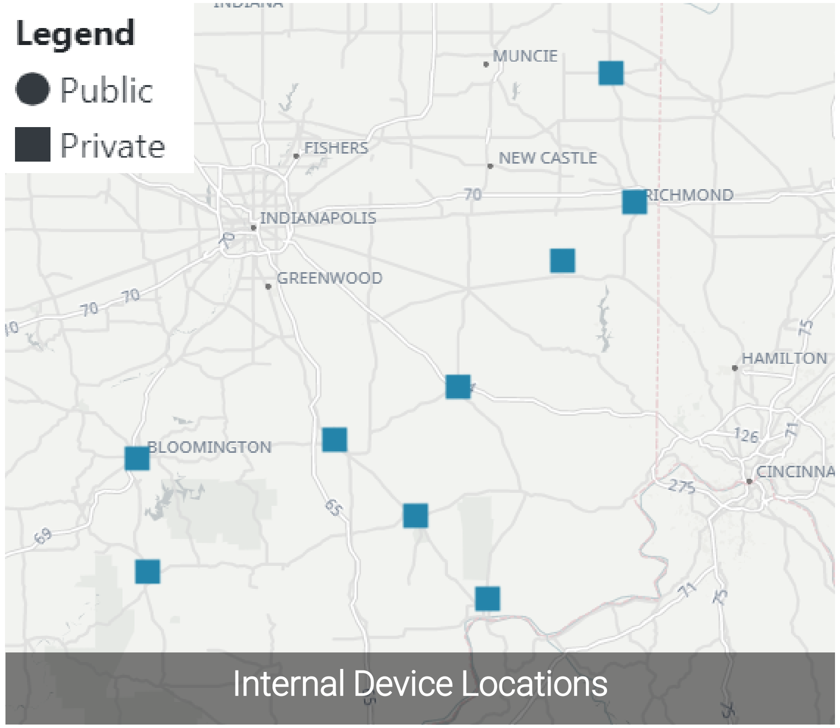
Perspective:

Public client to public server	External
Private client to private server	Internal
Public client to private server	Incoming
Private client to public server	Outgoing



Internal Device Locations

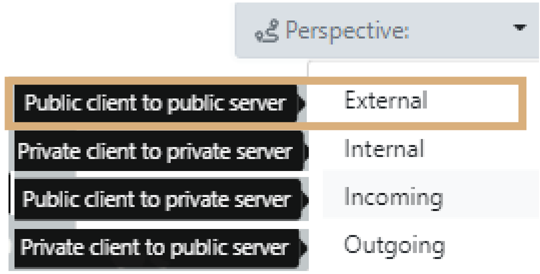
Internal



Internal Device Locations

Public Facing to Internet

External traffic to your VPN's from foreign or suspect locations means compromised user credentials are loose – don't depend on finding them on the Dark Web before they are used! Watch VPN sources.



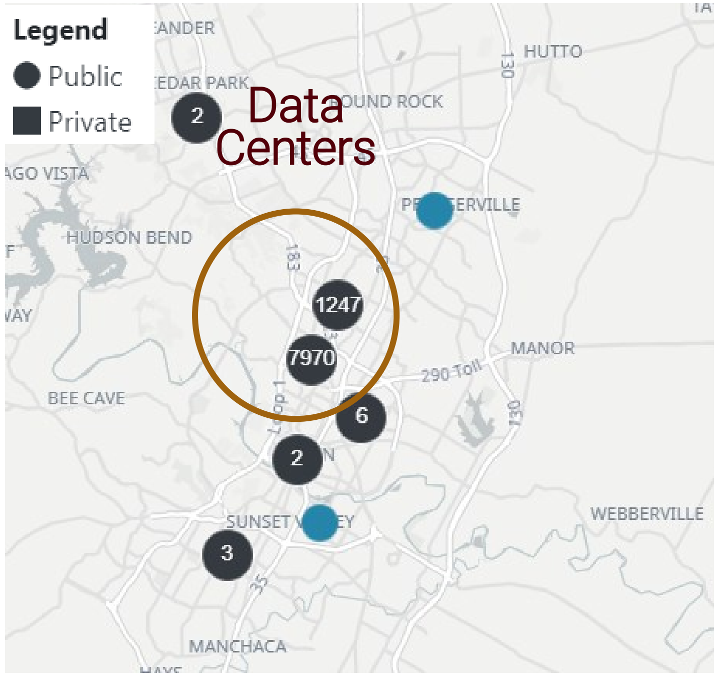
Perspective:

Public client to public server External

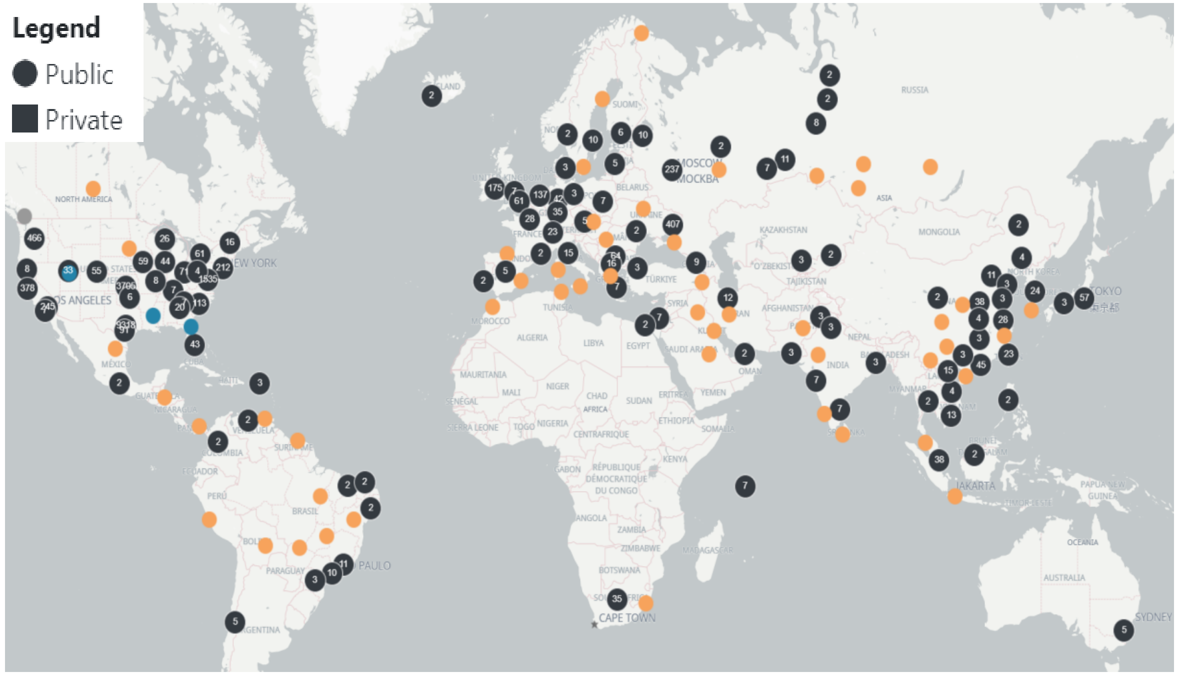
Private client to private server Internal

Public client to private server Incoming

Private client to public server Outgoing



External



Vital Server Communication Vetting 5W’s

Part 4

Vetting Server Communication

Manage Security access to or from a vital server

Develop a baseline

Availability of an interactive map and filterable matrix to filter on IP, Port, ASN#

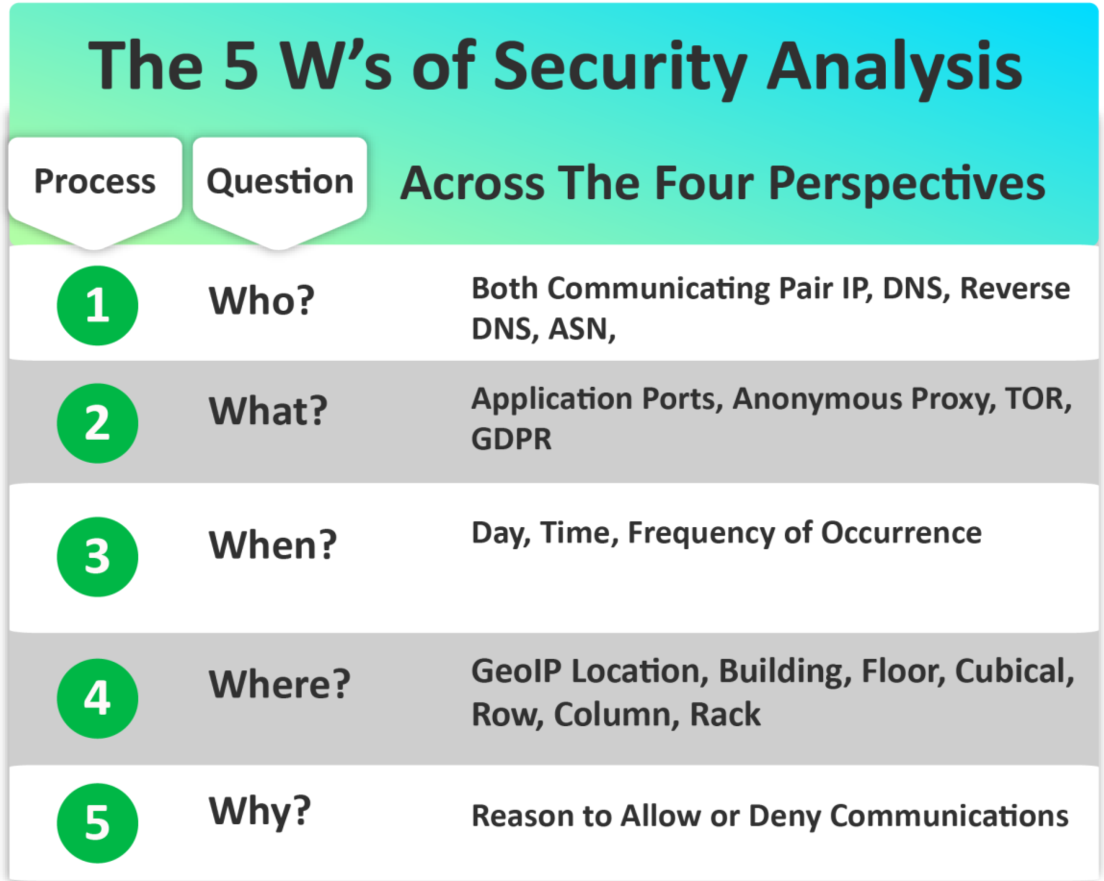
Require data owner and platform admin collaboration to Vet anonymous communication

Know DNS, Port and IP address DataTravel

True Zero-Trust

Access to business-as-usual information increases likelihood of a breach

Vital Server Communication Vetting 5 W's



The 5 W's of Security Analysis

Process	Question	Across The Four Perspectives
1	Who?	Both Communicating Pair IP, DNS, Reverse DNS, ASN,
2	What?	Application Ports, Anonymous Proxy, TOR, GDPR
3	When?	Day, Time, Frequency of Occurrence
4	Where?	GeoIP Location, Building, Floor, Cubical, Row, Column, Rack
5	Why?	Reason to Allow or Deny Communications

Actual SolarWinds Breach Exfiltration Host 5 W's Security Research Provided from Tool at Right.

Who:

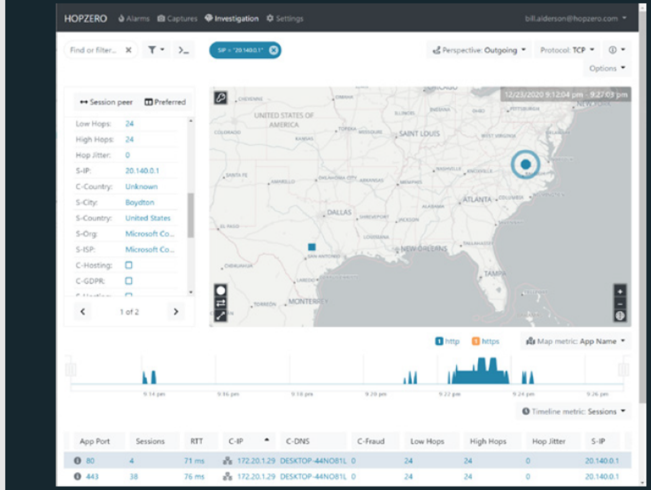
Criminals using IP DNS Name: avmsvmcloud.com
Microsoft Cloud Hosted Server IP Address 20.140.0.1
Autonomous System Number ASN: 8070,
ASN Name: Microsoft-Corp-Msn-ASN
Criminal Nameserver: sunburst-ns-b.sinkhole.shadowserver.org

What:

Data Exfiltration on HTTPS TCP Port 443
Client Server Bytes C-Bytes 43429 S-Bytes 32076 (example session)
TCP Sessions: 38 Slow speed 1927 – 2609 bps
Risk Scores: Disabled for this test
Criminal ongoing access to intellectual property, finance, commerce, and defense information

When:

Trojan placed, waited two weeks, gather credential data
Exfiltration Date: Dec 23, 2020 at 9:12:04PM CST (example)



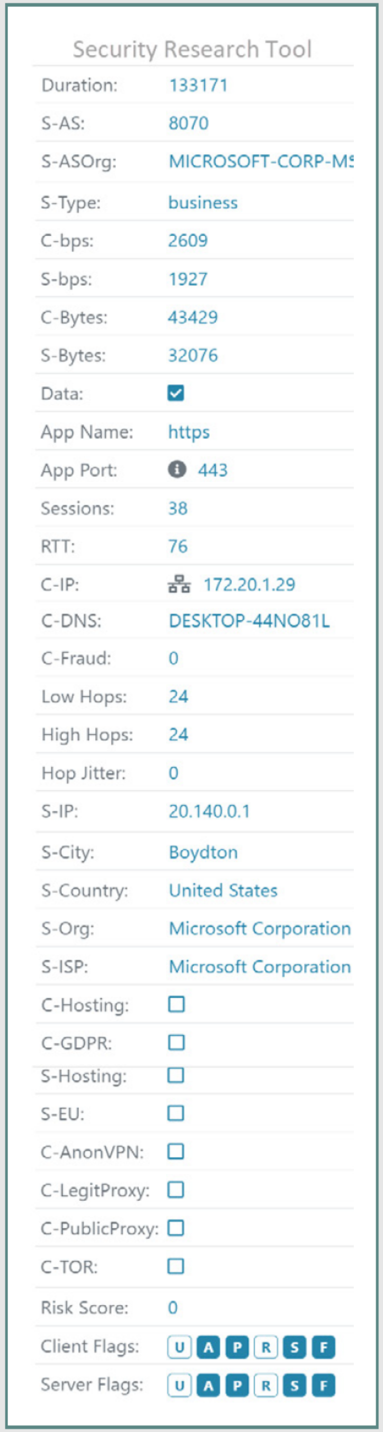
App Port	Sessions	RTT	C-IP	C-DNS	C-Fraud	Low Hops	High Hops	Hop Jitter	S-IP
80	4	71 ms	172.20.1.29	DESKTOP-44NO81L	0	24	24	0	20.140.0.1
443	38	76 ms	172.20.1.29	DESKTOP-44NO81L	0	24	24	0	20.140.0.1

Where:

Server Responder Microsoft Azure Datacenter Boydton VA
Client Request Inside SolarWinds-Victims Entire Enterprise
(Example: Austin Texas, Steiner Ranch, St. Address Redacted)
Distance: 24 Network Router Hops away, no Hop Jitter
Round Trip Time RTT: 76ms

Why:

Surveillance to exfiltrate ongoing vital information gaining defense and economic opportunity over the United States

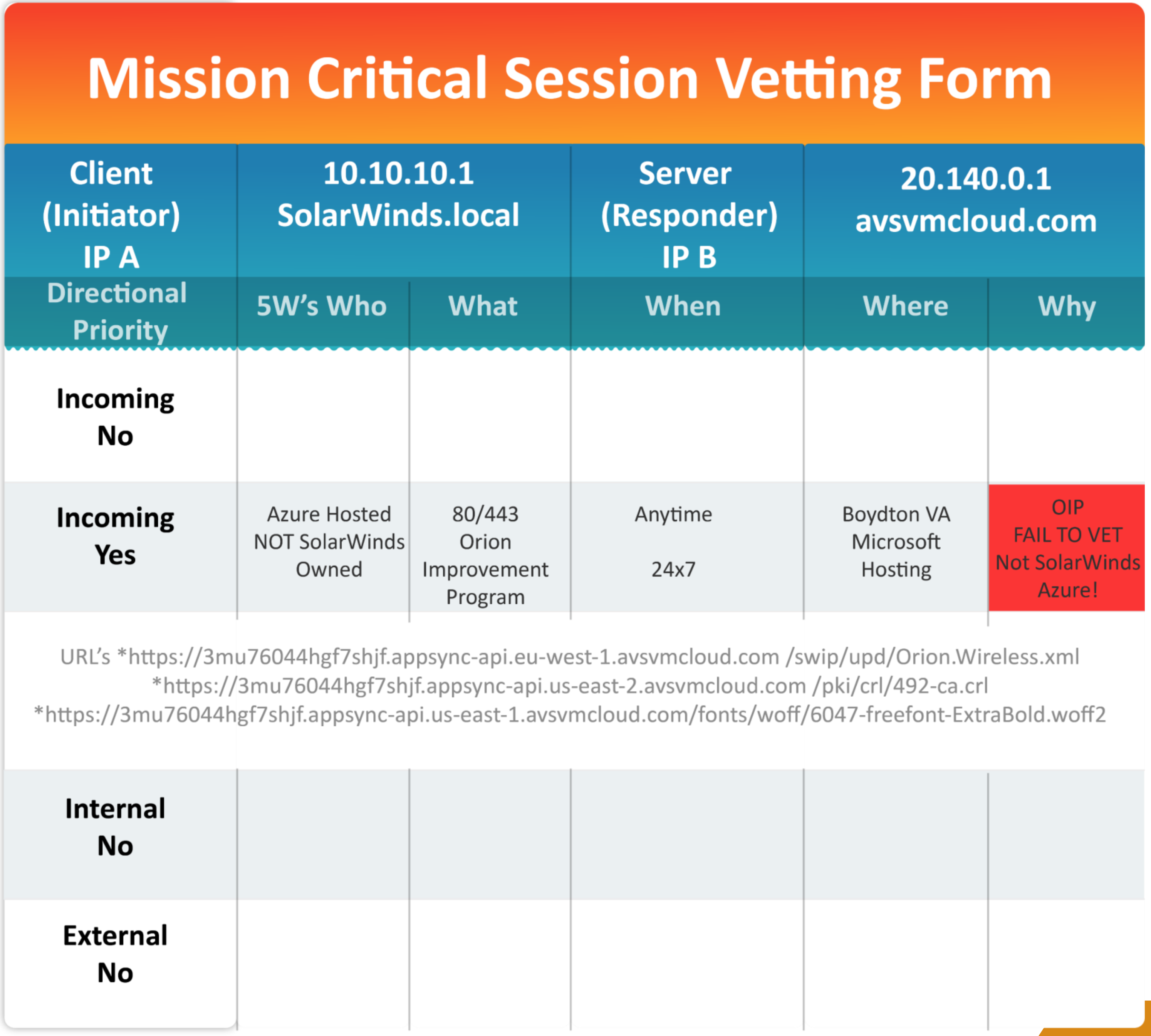


Security Research Tool

Duration:	133171
S-AS:	8070
S-ASOrg:	MICROSOFT-CORP-MS
S-Type:	business
C-bps:	2609
S-bps:	1927
C-Bytes:	43429
S-Bytes:	32076
Data:	☑
App Name:	https
App Port:	443
Sessions:	38
RTT:	76
C-IP:	172.20.1.29
C-DNS:	DESKTOP-44NO81L
C-Fraud:	0
Low Hops:	24
High Hops:	24
Hop Jitter:	0
S-IP:	20.140.0.1
S-City:	Boydton
S-Country:	United States
S-Org:	Microsoft Corporation
S-ISP:	Microsoft Corporation
C-Hosting:	□
C-GDPR:	□
S-Hosting:	□
S-EU:	□
C-AnonVPN:	□
C-LegitProxy:	□
C-PublicProxy:	□
C-TOR:	□
Risk Score:	0
Client Flags:	U A P R S F
Server Flags:	U A P R S F

Vital Server Communication Vetting 5 W's

Application	Port Number
HTTP	80
HTTPS	443
Oracle SQL	1225
Microsoft SQL	1433



Mission Critical Session Vetting Form

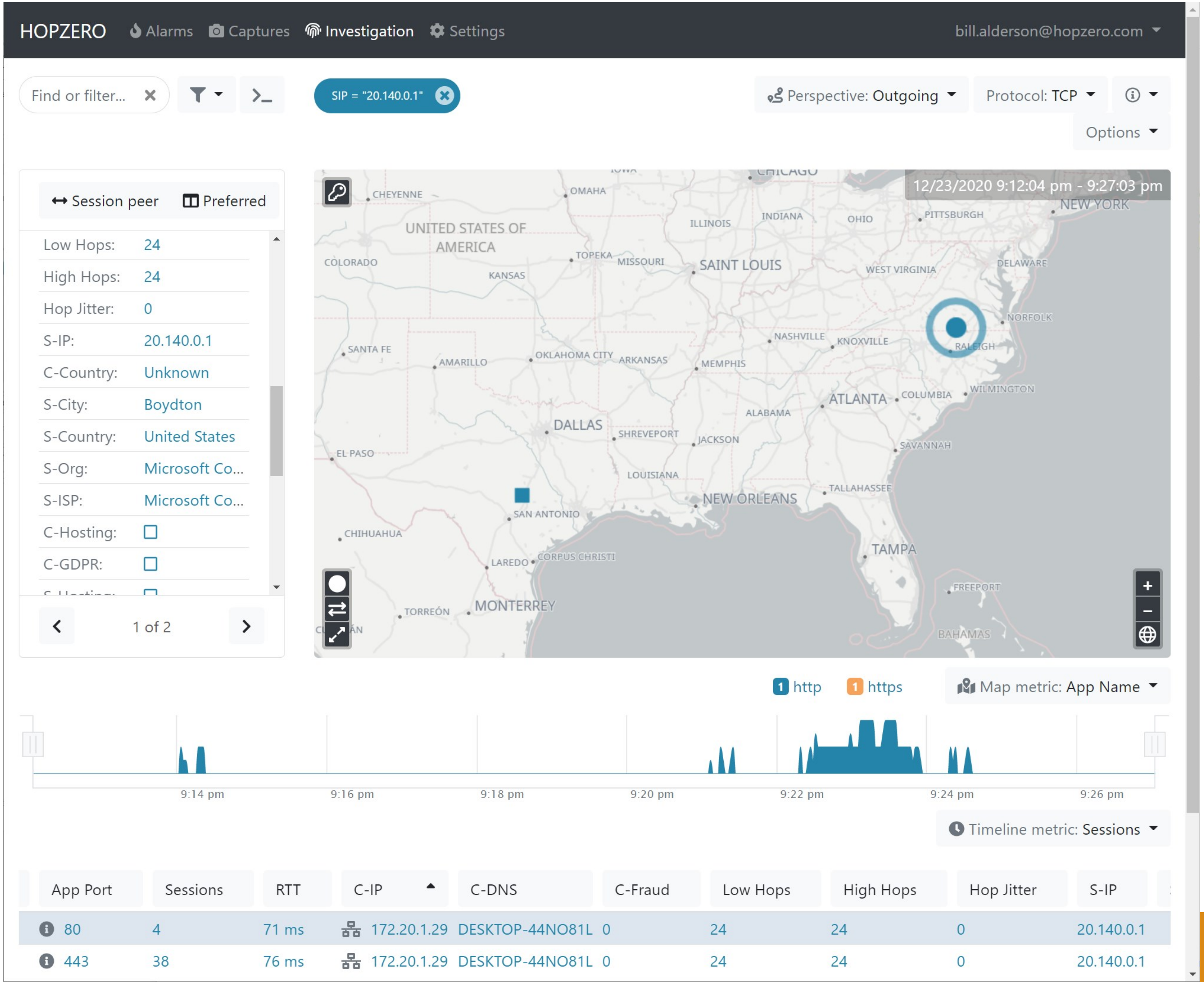
Client (Initiator) IP A	10.10.10.1 SolarWinds.local		Server (Responder) IP B	20.140.0.1 avsvmcloud.com	
Directional Priority	5W's Who	What	When	Where	Why
Incoming No					
Incoming Yes	Azure Hosted NOT SolarWinds Owned	80/443 Orion Improvement Program	Anytime 24x7	Boydton VA Microsoft Hosting	OIP FAIL TO VET Not SolarWinds Azure!
URL's *https://3mu76044hgf7shjf.appsync-api.eu-west-1.avsvmcloud.com /swip/upd/Orion.Wireless.xml *https://3mu76044hgf7shjf.appsync-api.us-east-2.avsvmcloud.com /pki/crl/492-ca.crl *https://3mu76044hgf7shjf.appsync-api.us-east-1.avsvmcloud.com/fonts/woff/6047-freefont-ExtraBold.woff2					
Internal No					
External No					

Vetting and Exterminating Entrenched Criminals

Powerful Sensory Analysis of Where Data Is Traveling

Detailed Matrix of Communications Security Details

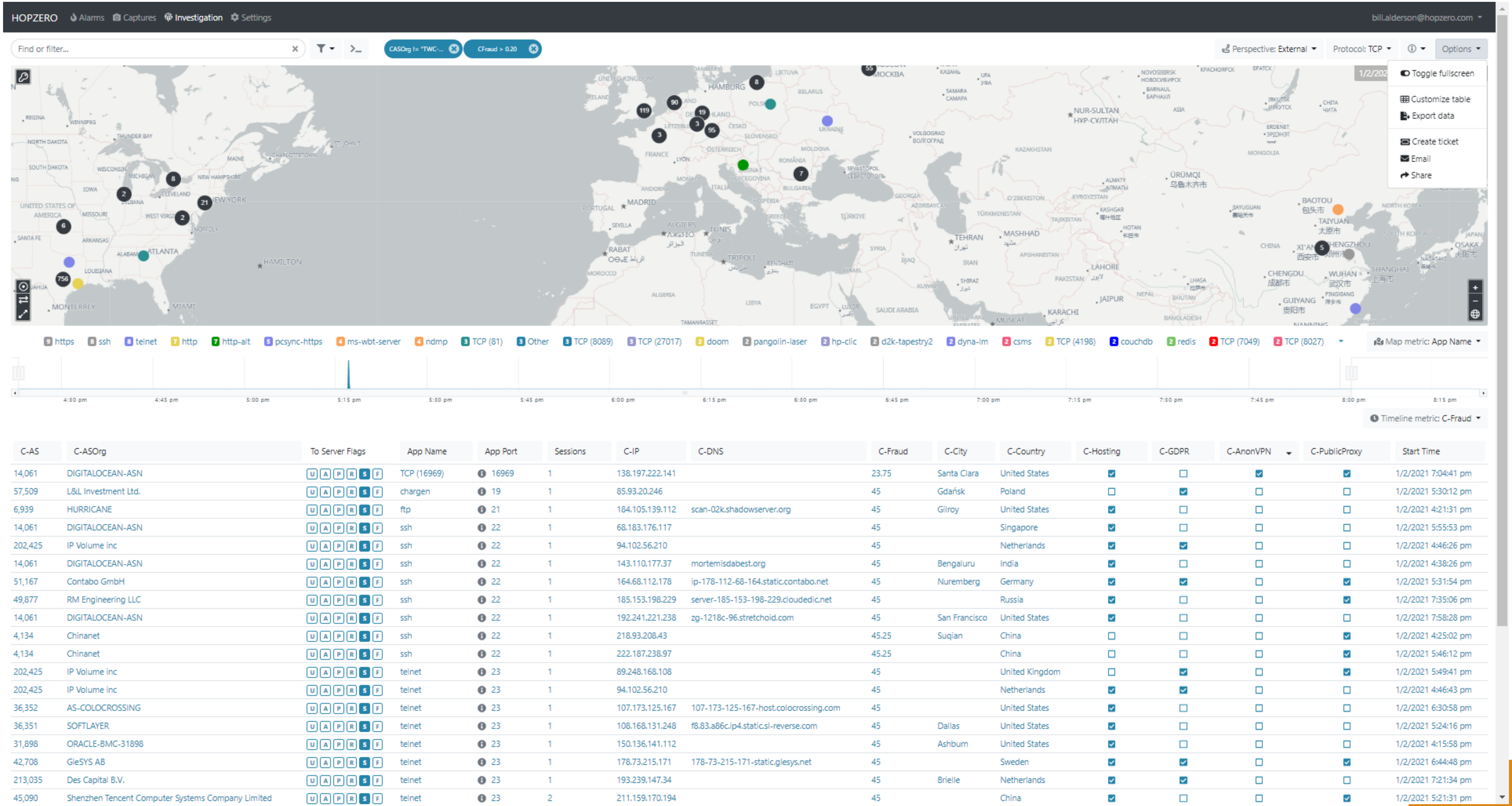
Both Internet GeoIP and Internal RFC 1918 Address Visualization Mapping of Private and Public IP’s



Low Hops:	24
High Hops:	24
Hop Jitter:	0
S-IP:	20.140.0.1
C-Country:	Unknown
S-City:	Boydton
S-Country:	United States
S-Org:	Microsoft Co...
S-ISP:	Microsoft Co...
C-Hosting:	□
C-GDPR:	□
S-Hosting:	□

App Port	Sessions	RTT	C-IP	C-DNS	C-Fraud	Low Hops	High Hops	Hop Jitter	S-IP
80	4	71 ms	172.20.1.29	DESKTOP-44NO81L	0	24	24	0	20.140.0.1
443	38	76 ms	172.20.1.29	DESKTOP-44NO81L	0	24	24	0	20.140.0.1

Vetting and Exterminating Entrenched Criminals



CASOrg != "TWC-...

CFraud > 0.20

C-AS	C-ASOrg	To Server Flags	App Name	App Port	Sessions	C-IP	C-DNS	C-Fraud	C-City	C-Country	C-Hosting	C-GDPR	C-AnonVPN	C-PublicProxy	Start Time
14,061	DIGITALOCEAN-ASN	U A P R S F	TCP (16969)	16969	1	138.197.222.141		23.75	Santa Clara	United States	☑	☐	☑	☑	1/2/2021 7:04:41 pm
57,509	L&L Investment Ltd.	U A P R S F	chargen	19	1	85.93.20.246		45	Gdańsk	Poland	☐	☑	☐	☐	1/2/2021 5:30:12 pm
6,939	HURRICANE	U A P R S F	ftp	21	1	184.105.139.112	scan-02k.shadowserver.org	45	Gilroy	United States	☑	☐	☐	☐	1/2/2021 4:21:31 pm
14,061	DIGITALOCEAN-ASN	U A P R S F	ssh	22	1	68.183.176.117		45		Singapore	☑	☐	☐	☐	1/2/2021 5:55:53 pm
202,425	IP Volume inc	U A P R S F	ssh	22	1	94.102.56.210		45		Netherlands	☑	☑	☐	☐	1/2/2021 4:46:26 pm
14,061	DIGITALOCEAN-ASN	U A P R S F	ssh	22	1	143.110.177.37	mortemisdabest.org	45	Bengaluru	India	☑	☐	☐	☐	1/2/2021 4:38:26 pm
51,167	Contabo GmbH	U A P R S F	ssh	22	1	164.68.112.178	ip-178-112-68-164.static.contabo.net	45	Nuremberg	Germany	☑	☑	☐	☑	1/2/2021 5:31:54 pm
49,877	RM Engineering LLC	U A P R S F	ssh	22	1	185.153.198.229	server-185-153-198-229.cloudedic.net	45		Russia	☑	☐	☐	☑	1/2/2021 7:35:06 pm
14,061	DIGITALOCEAN-ASN	U A P R S F	ssh	22	1	192.241.221.238	zg-1218c-96.stretchoid.com	45	San Francisco	United States	☑	☐	☐	☐	1/2/2021 7:58:28 pm
4,134	Chinanet	U A P R S F	ssh	22	1	218.93.208.43		45.25	Suqian	China	☐	☐	☐	☑	1/2/2021 4:25:02 pm
4,134	Chinanet	U A P R S F	ssh	22	1	222.187.238.97		45.25		China	☐	☐	☐	☑	1/2/2021 5:46:12 pm
202,425	IP Volume inc	U A P R S F	telnet	23	1	89.248.168.108		45		United Kingdom	☐	☑	☐	☑	1/2/2021 5:49:41 pm
202,425	IP Volume inc	U A P R S F	telnet	23	1	94.102.56.210		45		Netherlands	☑	☑	☐	☐	1/2/2021 4:46:43 pm
36,352	AS-COLOCROSSING	U A P R S F	telnet	23	1	107.173.125.167	107-173-125-167-host.colocrossing.com	45		United States	☑	☐	☐	☐	1/2/2021 6:30:58 pm
36,351	SOFTLAYER	U A P R S F	telnet	23	1	108.168.131.248	f8.83.a86c.ip4.static.sl-reverse.com	45	Dallas	United States	☑	☐	☐	☐	1/2/2021 5:24:16 pm
31,898	ORACLE-BMC-31898	U A P R S F	telnet	23	1	150.136.141.112		45	Ashburn	United States	☑	☐	☐	☐	1/2/2021 4:15:58 pm
42,708	GleSYS AB	U A P R S F	telnet	23	1	178.73.215.171	178-73-215-171-static.glesys.net	45		Sweden	☑	☑	☐	☑	1/2/2021 6:44:48 pm
213,035	Des Capital B.V.	U A P R S F	telnet	23	1	193.239.147.34		45	Brielle	Netherlands	☑	☑	☐	☐	1/2/2021 7:21:34 pm
45,090	Shenzhen Tencent Computer Systems Company Limited	U A P R S F	telnet	23	2	211.159.170.194		45		China	☑	☐	☐	☑	1/2/2021 5:21:31 pm

Software Improvement Program – An Inside Job?

Some Inside Job Considerations

1 Impossible to Know Intimate Information

File names of compiling file components.
File directory names.
Network location of files.
Server name where files located.
Security credentials to access and add files.
Internal SolarWinds compiling steps and resultant file package destinations.
Where files are moved along the steps to SolarWinds Update Server on Internet.
SolarWinds Internal Processes Updates Utilize.

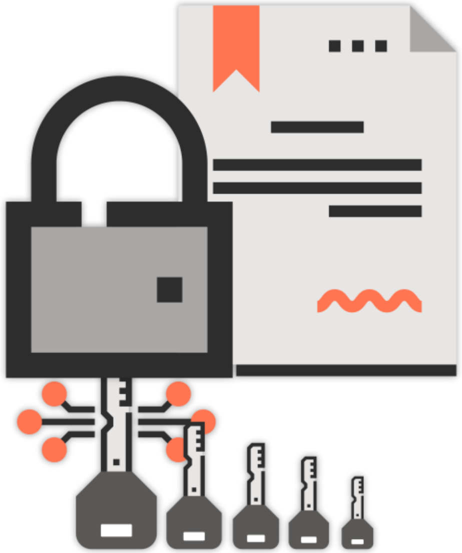
2 Commonly Available Information

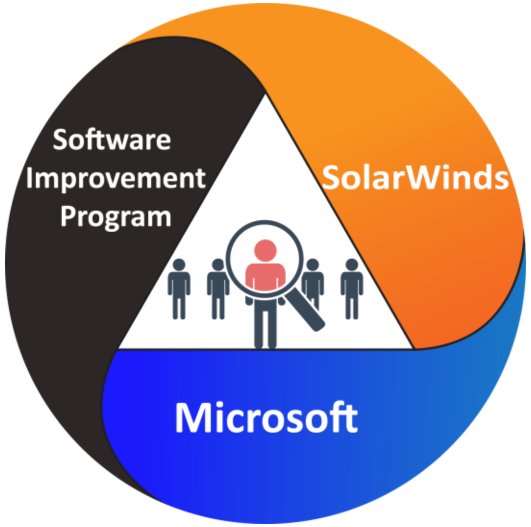
Standard Microsoft or Dev Kit compiling file default locations
Software Improvement Program Dev Products and Service Companies
Standard File directory names
Previous SolarWinds Update directory and filenames

3 Intimate Information Found or Guessed

Previous undiscovered SolarWinds breaches.
Previous unreported SolarWinds breaches.
Included in SolarWinds RFQ for OIP/SIP Developers.
Microsoft Developer Training Documentation and Examples Names

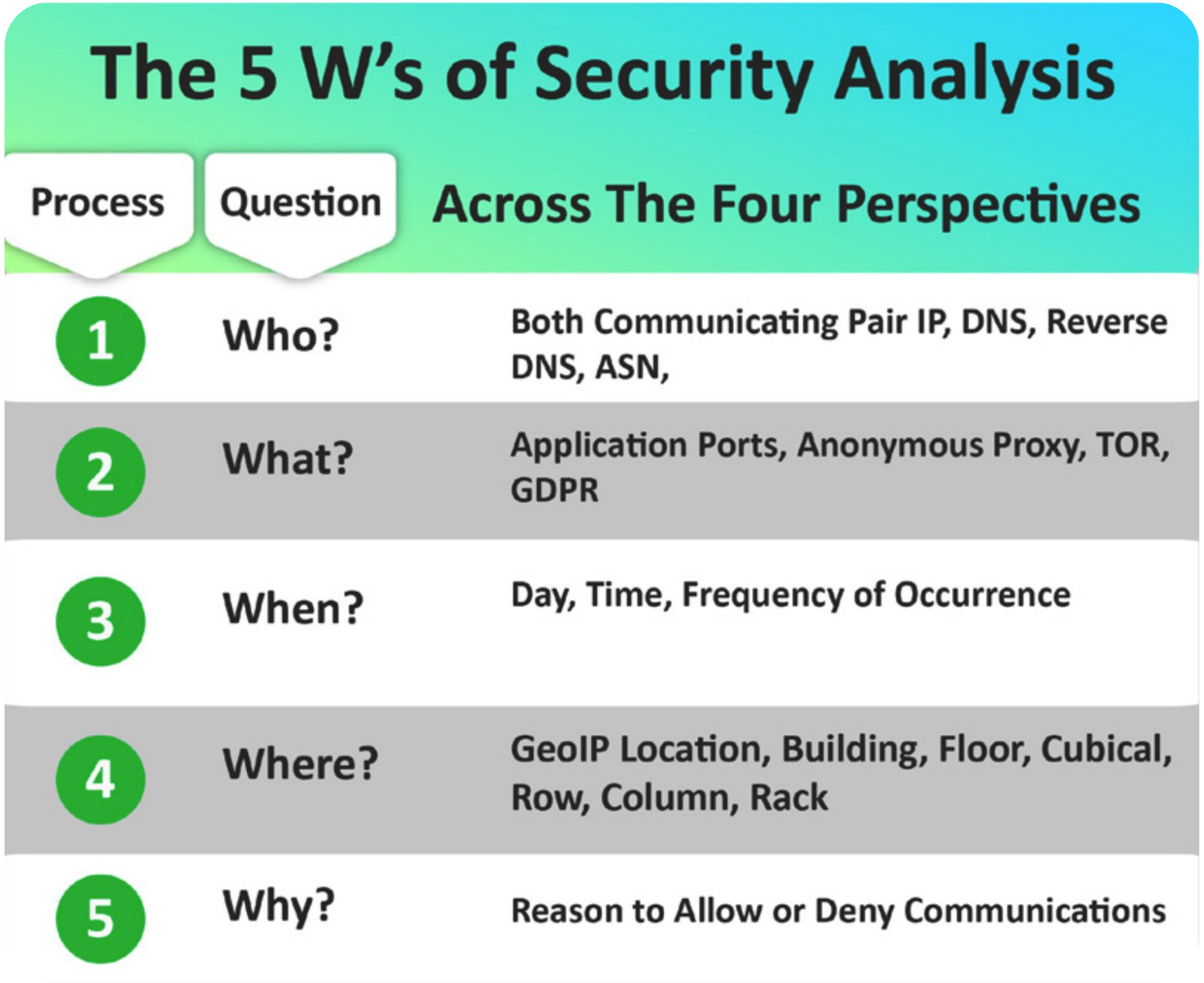
Criminals Create Authentic Certificates Reusing Keys & Tokens





5W’s for Vetting of Vital Server Communications

Setting up vetting of the vital server communication based on the 5 W’s process will ensure clear understanding of required access



The 5 W’s of Security Analysis

Process	Question	Across The Four Perspectives
1	Who?	Both Communicating Pair IP, DNS, Reverse DNS, ASN,
2	What?	Application Ports, Anonymous Proxy, TOR, GDPR
3	When?	Day, Time, Frequency of Occurrence
4	Where?	GeoIP Location, Building, Floor, Cubical, Row, Column, Rack
5	Why?	Reason to Allow or Deny Communications

Evaluation of Server communication

Who?	Communication between IP of SQL Server and Middleware server	IP SolarWinds Server and DNS amsvmcloud.com resolve 20.140.0.1 a Microsoft Hosted Server by DNS Nameserver sunburst-ns-b-sinkhole
Where?	In the Datacenter	In the Datacenter but not to anywhere
When?	24 hours as developer flow diagram specifies	Anytime
What?	Using Oracle Port 1525	Port HTTP 443 or HTTP 80
Why?	Database to Middleware/Web server	Bogus DNS Name, resolved by a Bogus DNS Nameserver to a Paid Microsoft Hosting Service IP address
Approval	Allowed	Denied

Software Improvement Program – An Inside Job?

Part 5

An Inside Job?

SolarWinds development may have used 3rd party Dev kit

SolarWinds benefitted through collection of customer information from Software Improvement programs (SIP)

Who would they reveal internal information to

- Programmers change jobs often and/or freelance outside
- Hiring of freelancers for process development

Controls for internal and outsourced employees are limited

Impossible to Access Information

Impossible to Know Intimate information

- File names of compiling file components
- File directory names
- Network location of files
- Server name where files located
- Security credentials to access and add files
- Internal SolarWinds compiling steps and resultant file package destinations
- Where files are moved along the steps to SolarWinds Update Server on Internet
- SolarWinds Internal Processes Updates Utilize

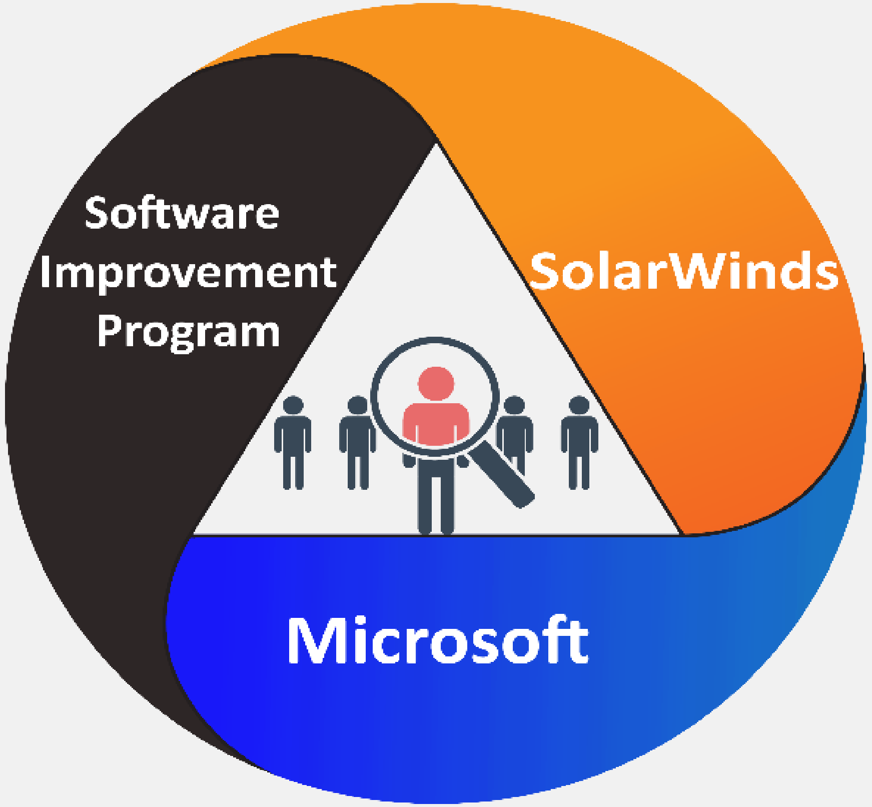
More available information

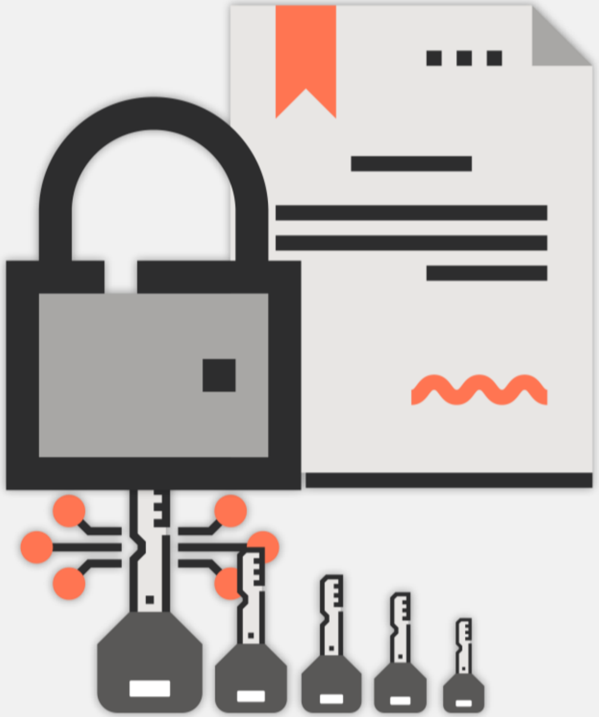
- Standard compiling file default locations
- Standard File directory names
- Previous SolarWinds Update directory and filenames

Ways Intimate information may have been guessed or found

- Previous undiscovered SolarWinds breaches
- Previous unreported SolarWinds breaches
- Employees, contractors, companies receiving development SolarWinds RFQ for OIP/SIP Developers
- Microsoft Developer Training Documentation and Examples names used.

Who might have helped criminals? How Inside Information was used





Inside information was used to create authentic certificates that later are reused by criminals for gaining access to other information the tokens allow

Vetting and Exterminating Entrenched Criminals

Part 6

Vetting Bulk Sessions - Exterminating Entrenched Criminals

Once the system has been infiltrated the following steps need to be followed to prevent further breach

1 Record and log actual network communication sessions “on the wire” as criminals expunge their log activity

2 Look for suspicious incomplete and partial TCP/IP communications session attempts

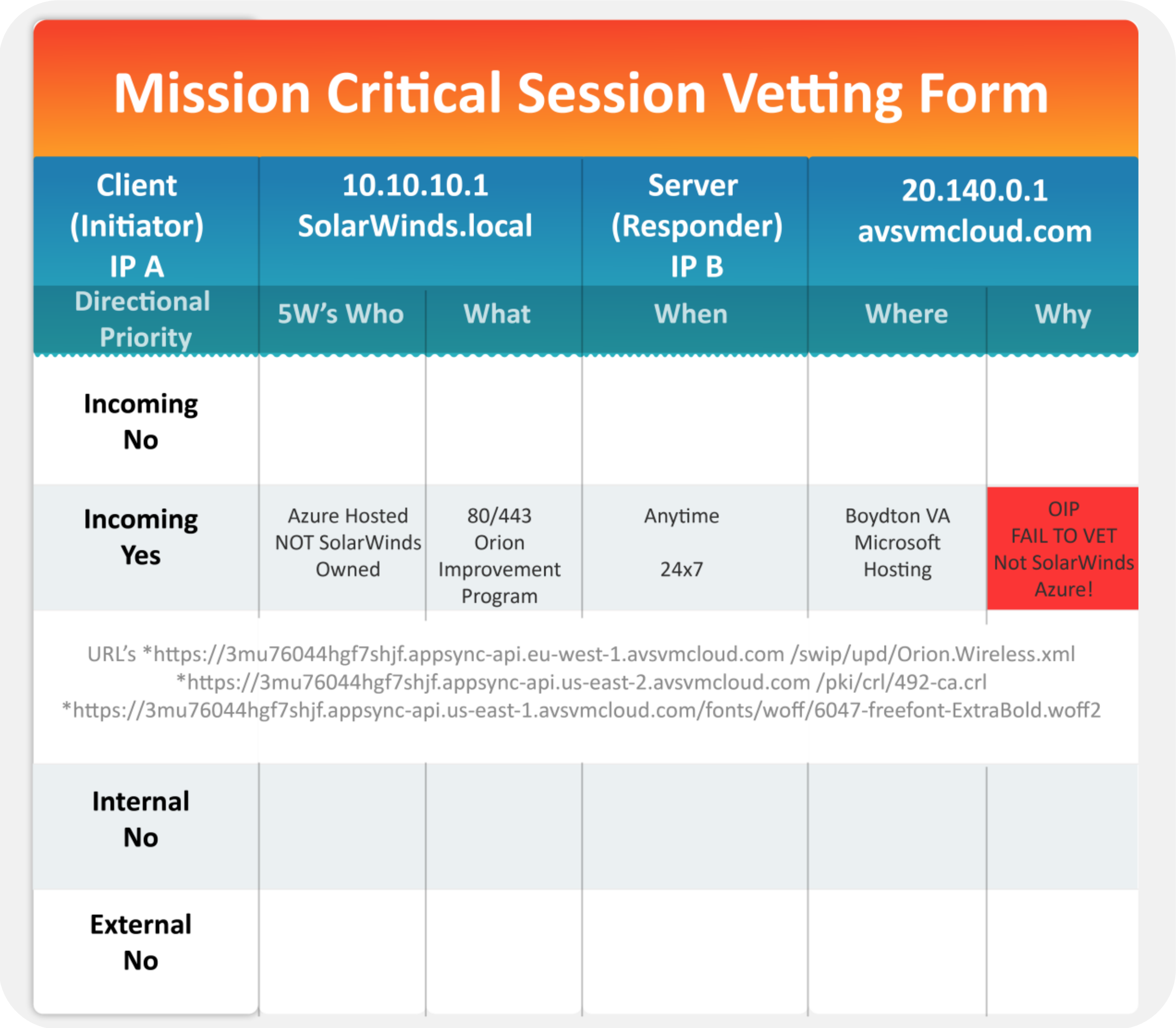
3 Regularly spot check persistent continued communication attempts occurring on the outside of the Firewall that now may be denied by changes after the breach

4 Use tools that identify the running program executable responsible for spawning each network session. MS-NetMon is a good tool for secondary investigation

5 From a server owned by your organization, most encrypted sessions can be decrypted by using your private encryption certificate in a specially configured analysis tool

6 Its not possible to decrypt sessions to external devices that use an external (or criminal) owned private certificate to encrypt the session. In this event 5W’s must be trusted for the destination server to Vet the session

Maximizing the Vetting Process

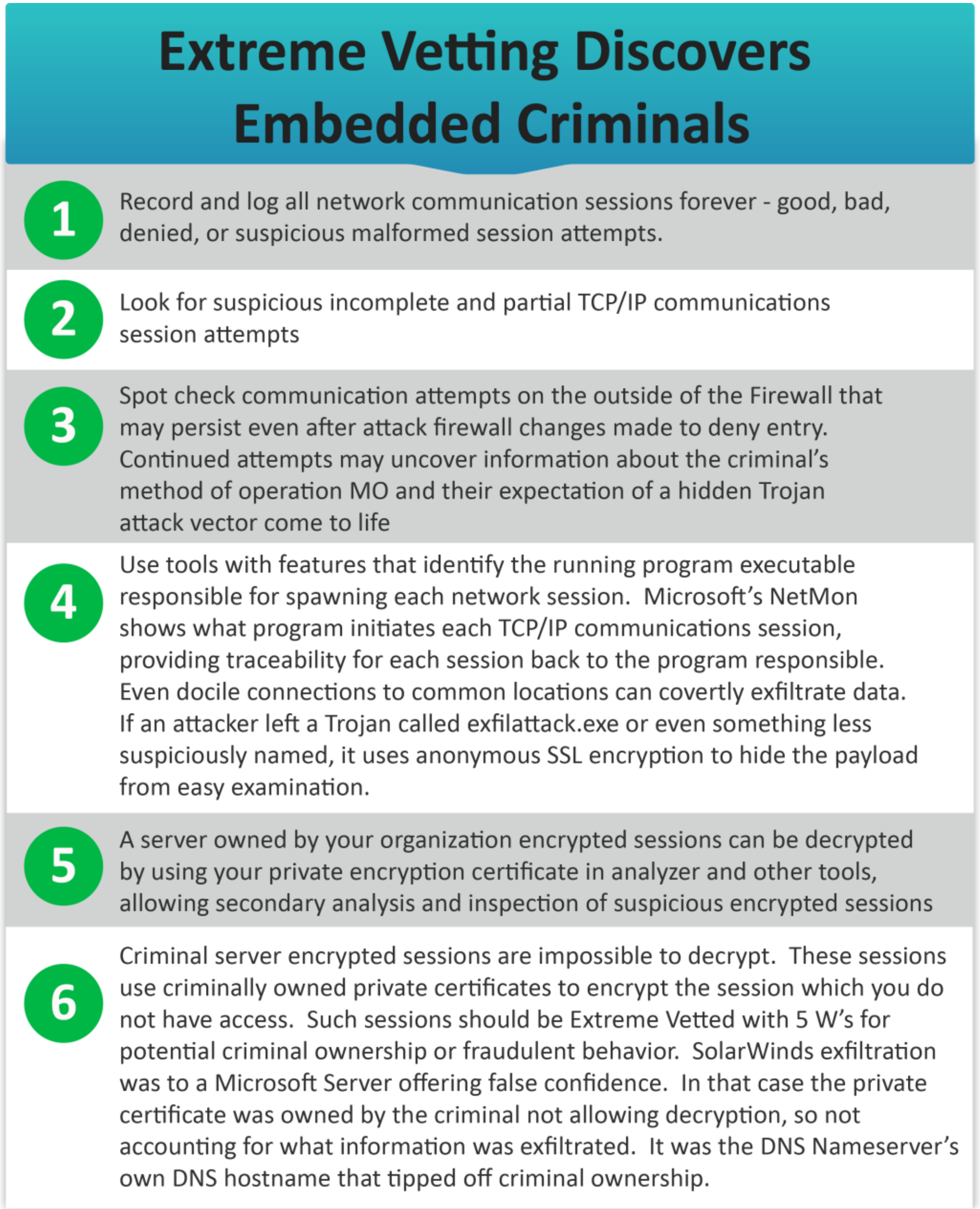


Mission Critical Session Vetting Form

Client (Initiator) IP A	10.10.10.1 SolarWinds.local		Server (Responder) IP B	20.140.0.1 avsvmcloud.com	
Directional Priority	5W's Who	What	When	Where	Why
Incoming No					
Incoming Yes	Azure Hosted NOT SolarWinds Owned	80/443 Orion Improvement Program	Anytime 24x7	Boydton VA Microsoft Hosting	OIP FAIL TO VET Not SolarWinds Azure!
URL's *https://3mu76044hgf7shjf.appsync-api.eu-west-1.avsvmcloud.com /swip/upd/Orion.Wireless.xml *https://3mu76044hgf7shjf.appsync-api.us-east-2.avsvmcloud.com /pki/crl/492-ca.crl *https://3mu76044hgf7shjf.appsync-api.us-east-1.avsvmcloud.com/fonts/woff/6047-freefont-ExtraBold.woff2					
Internal No					
External No					

Using a sortable, filterable list of session vetting provides fast Vetting of thousands of sessions to discover and exterminate criminals dwelling inside a network

Vetting and Exterminating Entrenched Criminals



Extreme Vetting Discovers Embedded Criminals

1. Record and log all network communication sessions forever - good, bad, denied, or suspicious malformed session attempts.

2. Look for suspicious incomplete and partial TCP/IP communications session attempts

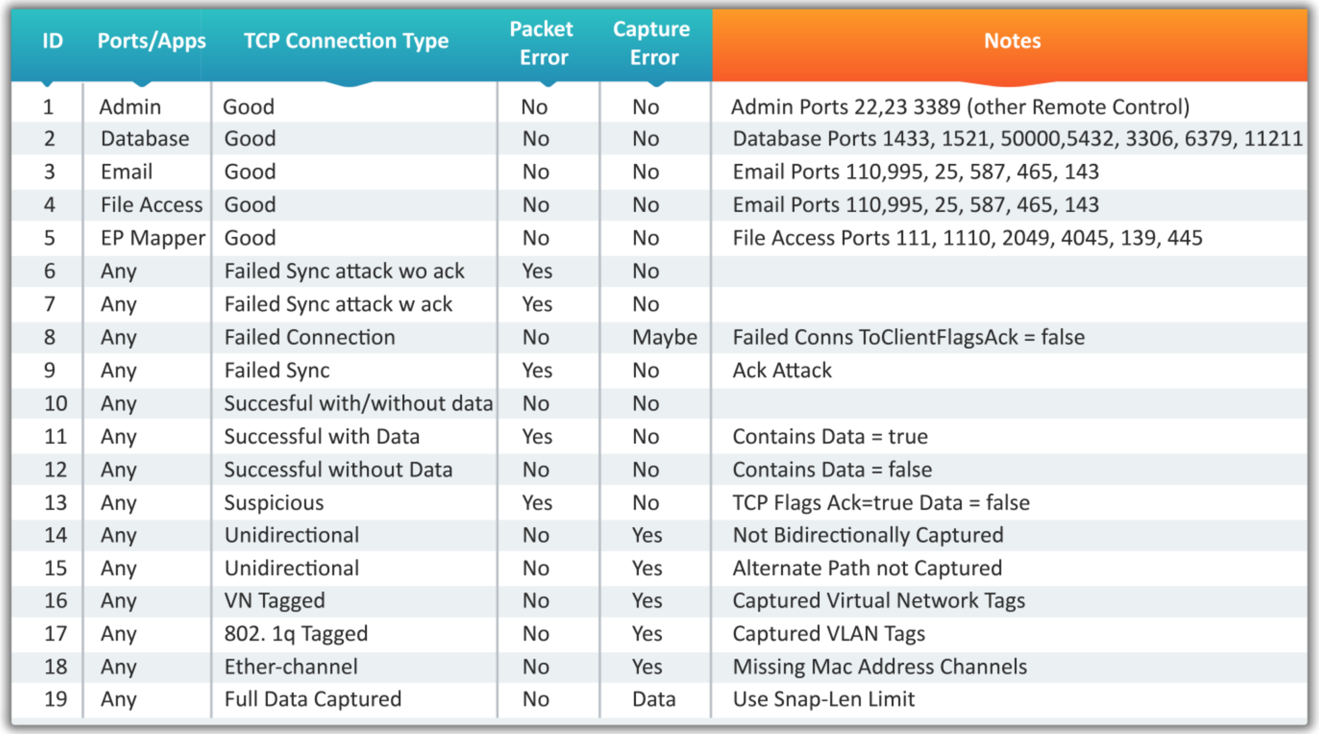
3. Spot check communication attempts on the outside of the Firewall that may persist even after attack firewall changes made to deny entry. Continued attempts may uncover information about the criminal's method of operation MO and their expectation of a hidden Trojan attack vector come to life

4. Use tools with features that identify the running program executable responsible for spawning each network session. Microsoft's NetMon shows what program initiates each TCP/IP communications session, providing traceability for each session back to the program responsible. Even docile connections to common locations can covertly exfiltrate data. If an attacker left a Trojan called exfilattack.exe or even something less suspiciously named, it uses anonymous SSL encryption to hide the payload from easy examination.

5. A server owned by your organization encrypted sessions can be decrypted by using your private encryption certificate in analyzer and other tools, allowing secondary analysis and inspection of suspicious encrypted sessions

6. Criminal server encrypted sessions are impossible to decrypt. These sessions use criminally owned private certificates to encrypt the session which you do not have access. Such sessions should be Extreme Vetted with 5 W's for potential criminal ownership or fraudulent behavior. SolarWinds exfiltration was to a Microsoft Server offering false confidence. In that case the private certificate was owned by the criminal not allowing decryption, so not accounting for what information was exfiltrated. It was the DNS Nameserver's own DNS hostname that tipped off criminal ownership.

TCP Connection Status Indicators



ID	Ports/Apps	TCP Connection Type	Packet Error	Capture Error	Notes
1	Admin	Good	No	No	Admin Ports 22,23 3389 (other Remote Control)
2	Database	Good	No	No	Database Ports 1433, 1521, 50000,5432, 3306, 6379, 11211
3	Email	Good	No	No	Email Ports 110,995, 25, 587, 465, 143
4	File Access	Good	No	No	Email Ports 110,995, 25, 587, 465, 143
5	EP Mapper	Good	No	No	File Access Ports 111, 1110, 2049, 4045, 139, 445
6	Any	Failed Sync attack wo ack	Yes	No	
7	Any	Failed Sync attack w ack	Yes	No	
8	Any	Failed Connection	No	Maybe	Failed Conns ToClientFlagsAck = false
9	Any	Failed Sync	Yes	No	Ack Attack
10	Any	Succesful with/without data	No	No	
11	Any	Successful with Data	Yes	No	Contains Data = true
12	Any	Successful without Data	No	No	Contains Data = false
13	Any	Suspicious	Yes	No	TCP Flags Ack=true Data = false
14	Any	Unidirectional	No	Yes	Not Bidirectionally Captured
15	Any	Unidirectional	No	Yes	Alternate Path not Captured
16	Any	VN Tagged	No	Yes	Captured Virtual Network Tags
17	Any	802. 1q Tagged	No	Yes	Captured VLAN Tags
18	Any	Ether-channel	No	Yes	Missing Mac Address Channels
19	Any	Full Data Captured	No	Data	Use Snap-Len Limit

Who is Responsible for the SolarWinds Breach

Part 7

Infiltration Through System Failures

SolarWinds

- Allowed hacker code inclusion in the software update
- Neglected to vet the files in the software update
- Uploaded files containing a trojan on the internet update server

Customer/ Victim

- Manually or automatically downloaded update file without proper vetting
- Allowed internet access to the code allowing exfiltration
- Does not have an AntiVirus to detect an attack
- Failed to vet external domain allowing exfiltration
- Allowed the criminal full control causing the development of an Advanced Persistent Threat

Rogue code/ Criminal

- 2-week dormancy to avoid detection, unable to exfiltrate without internet access
- Gathers information and credentials for exfiltration
- Connected to Microsoft Azure to inform criminal regarding a new victim

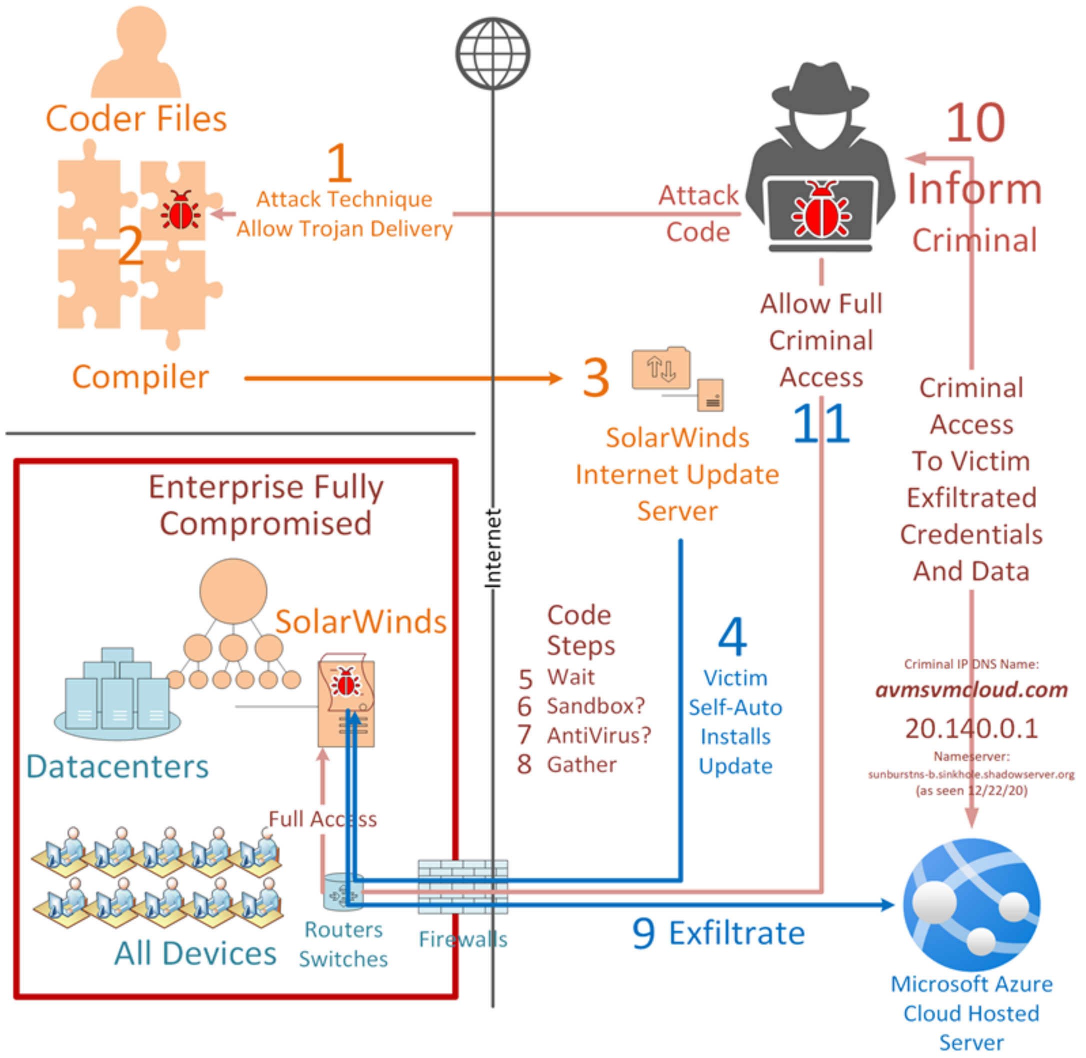
Responsible Party Details

Step	Responsible Party	What Happened	Reason	Impact
1	SolarWinds	Inserted Dll code named: SolarWinds. Orion.Core.Businesslayer.dll	Failed to Vet Incoming	Criminals insert Trojan
2	SolarWinds	Dll considered valid compilation object into the update	Failed to Control Critical Files	Compiled DLL signed
3	SolarWinds	Dll is made available for Internet download	Available for Auto update	Update by Customer
4	Customer-Victim	Update push or pull to the SolarWinds Server through Internet access	Vital Server direct on Internet	Updates not vetted on Vital server
5	Criminal	Criminal	Avoid detection mechanisms	Dll Continues
6	Customer-Victim	Code test Internet access for backdoor capabilities sandbox detection	Trojan impotent without Internet Access	Internet access green lights the DLL
7	Admin	Checked for antivirus on host	Avoids AV Detection	Avoids Detection
8	SolarWinds Customer-Victim	Gathers information for exfiltration to awaiting criminals	No Isolation by SolarWinds or customer	Premises Internet and Cloud all compromised
9	Customer-Victim	Internet DNS address avsvmcloud.com making data available to criminals	No limits Direct Internet Server to non-SolarWinds domain.	Exfiltration of Vital Data
10	Customer-Victim	Criminals informed - enduring remote access compromise	Allows Outgoing Access to Bad Server	Places Vital Data on Bad Server
11	Customer-Victim	External criminals are enabled to conduct hands-on attack	Vital Server Direct on Internet	Extends Criminal Access

SolarWinds Orion Breach Steps

Trojan code has built in protection to avoid detection

Infiltration is dependent upon SolarWinds and its customers failing to protect against an external attack by not following fundamental network security best practices



Outcome of the Breach

- Users of SolarWinds software are not aware of the landmines placed by the rogue code or subsequent criminal access
- Breached companies are ill equipped to find the fundamental issues – desiring only “automatic software”
- Bulk session analysis needs to identify any malicious sessions
- Criminals can delete log entries of their activities to evade
- Network tap and switch span provides a reliable method of recording session traffic

Preventing Data Breach Through Data Travel Limits

Part 8

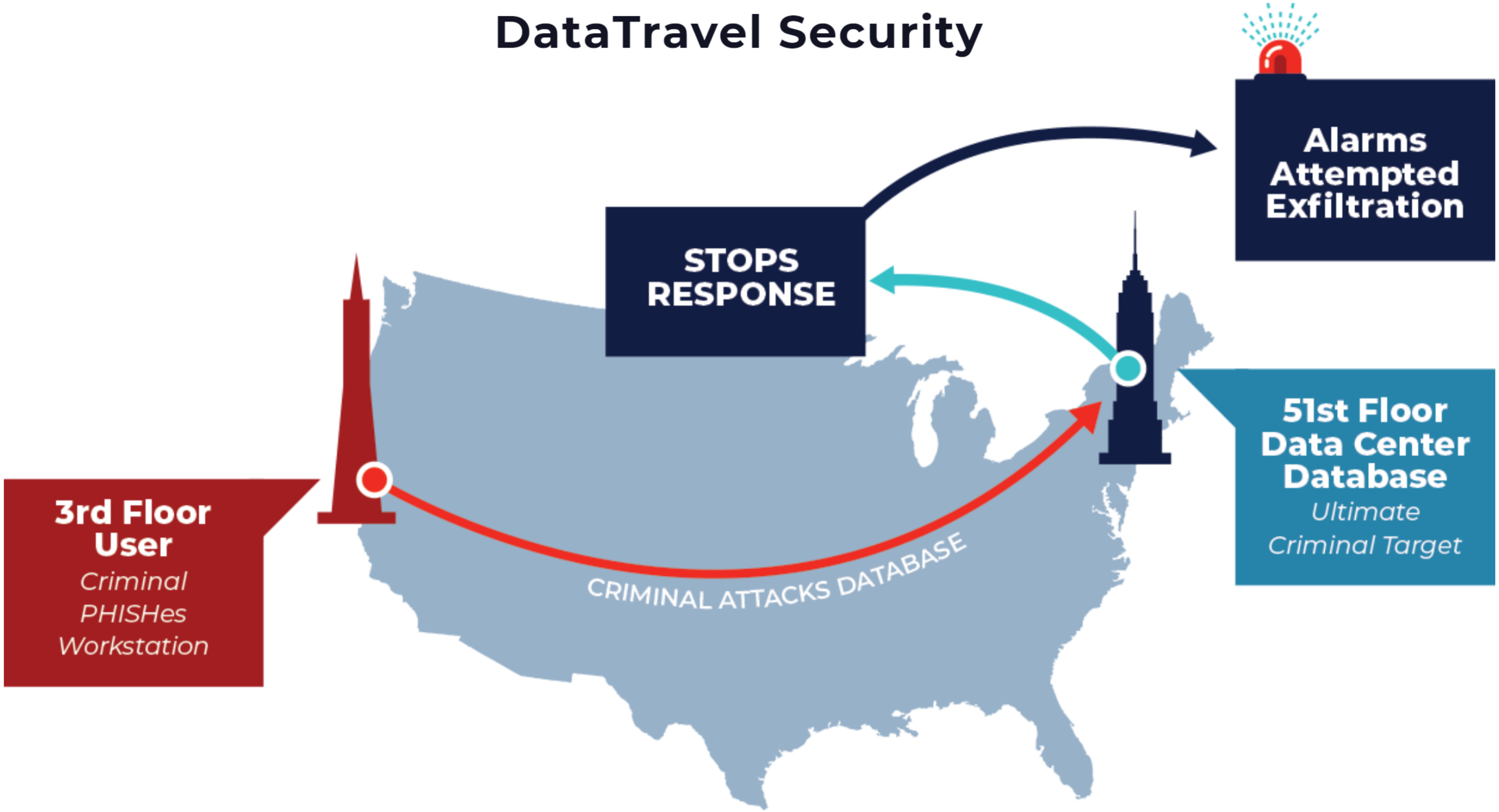
Data Travel Limits

After the analysis of SolarWinds breach and other software breaches it has been clear a new method of prevention was necessary

Introducing data travel limits can reduce the threat of malware and phish

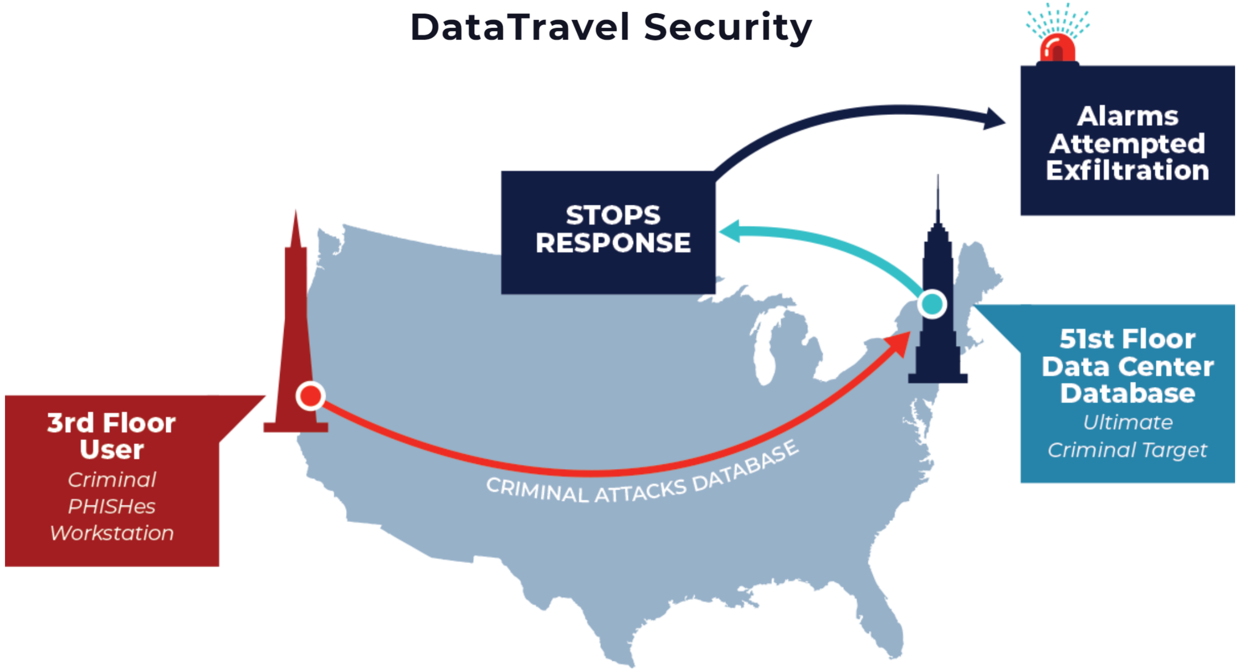
Data travel limits ensure that only adjacent local devices can receive information

DataTravel Catches Phish and Ransomware

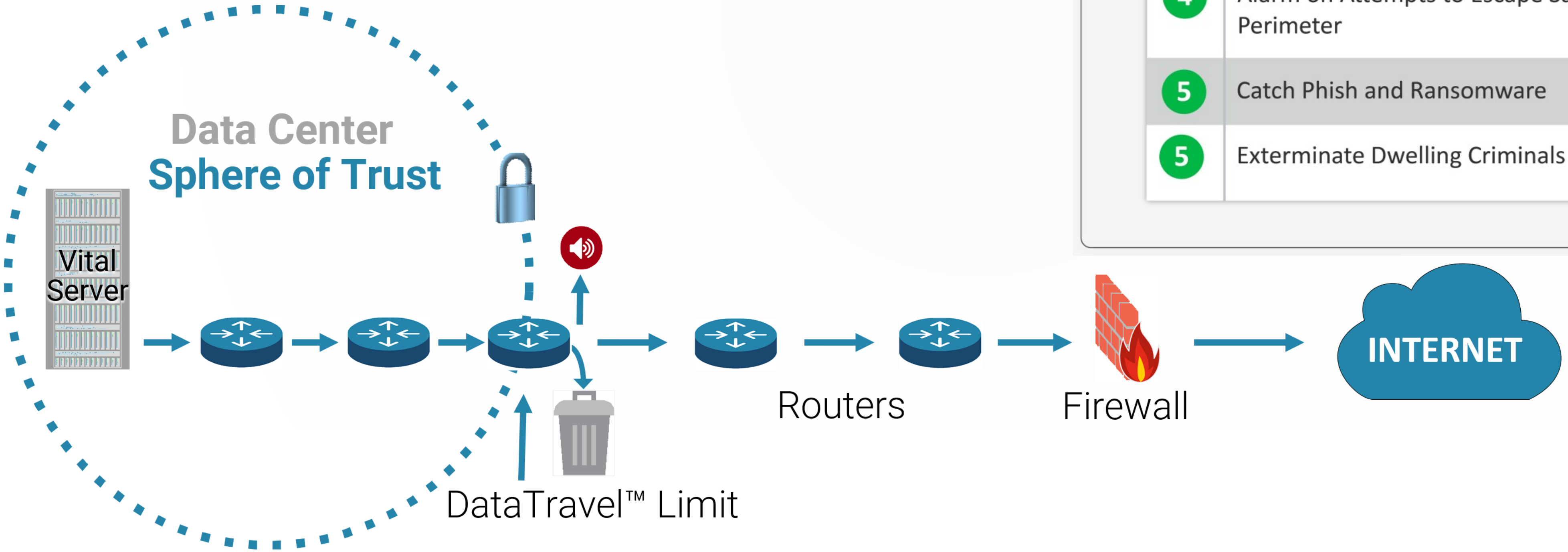

DataTravel Security
3rd Floor User
Criminal PHISHes Workstation
CRIMINAL ATTACKS DATABASE
51st Floor Data Center Database
Ultimate Criminal Target
STOPS RESPONSE
Alarms Attempted Exfiltration

Prevention of a Breach Through Data Travel Limits

1. Study the distance vital server is communicating
2. Calculate the safe data travel perimeter and set as a default HOP value
3. Use data travel record to log all communication sessions
4. Set up an alarm to identify any requests beyond the safe data travel perimeter
5. Use software such as Microsoft NetMon to trace the session to the originating IP and to establish the 5W's
6. Catch and exterminate phish and ransomware activity


DataTravel Security
Alarms Attempted Exfiltration
STOPS RESPONSE
3rd Floor User
Criminal PHISHes Workstation
CRIMINAL ATTACKS DATABASE
51st Floor Data Center Database
Ultimate Criminal Target

DataTravel Limits



Data Center

Sphere of Trust

Vital Server

Routers

Firewall

INTERNET

DataTravel™ Limit

SolarWinds Breach Responsibility Opinion

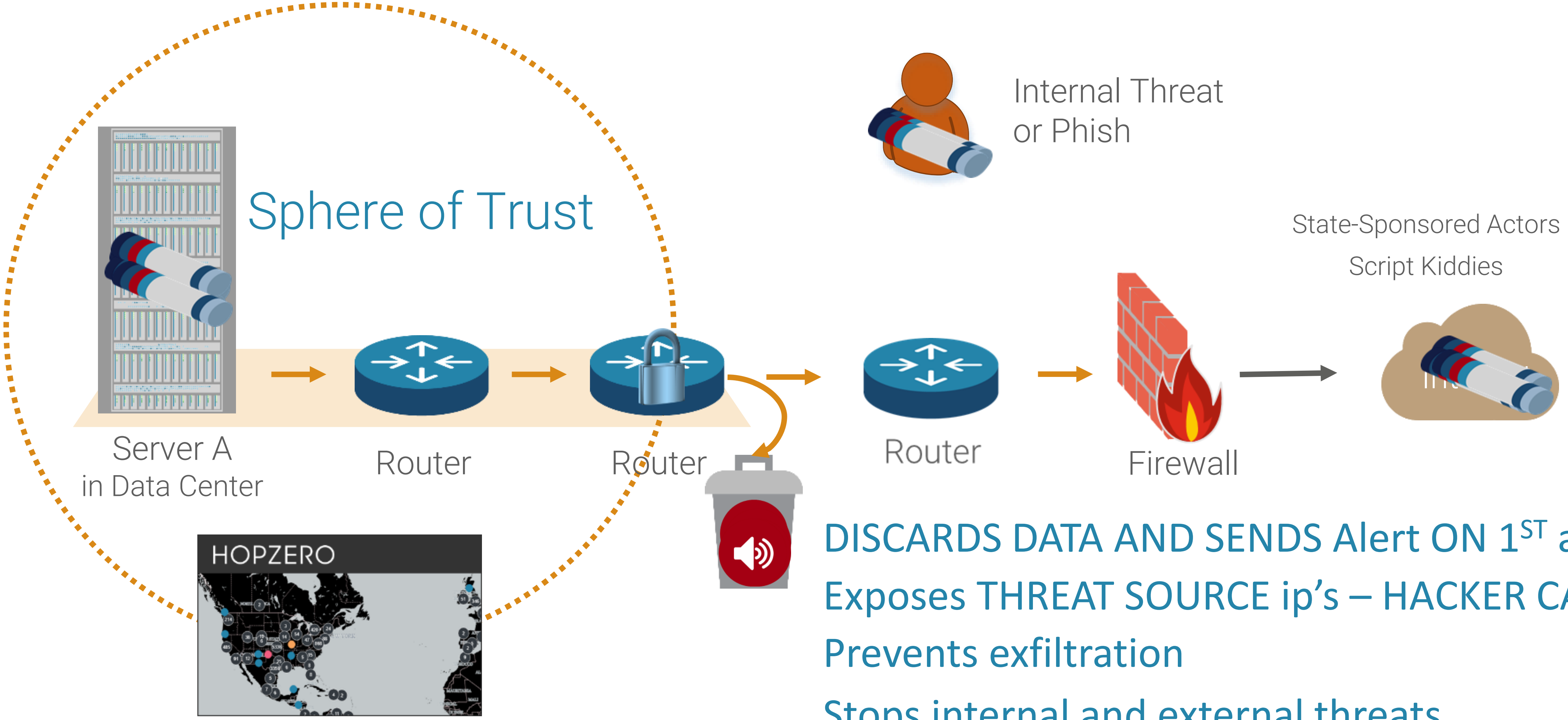
	DataTravel Limit Technology Steps
1	Learn Distance Metrics
2	Apply Distance Limit
3	Monitor Communication Sessions
4	Alarm on Attempts to Escape Safe Perimeter
5	Catch Phish and Ransomware
5	Exterminate Dwelling Criminals

Cogent … *clear, collaborative, insightful*
powerfully persuasive, balanced, weighty, inclusive

Topics Prof Assn's Conferences SME's Vendors
Content Videos LiveStream Collaboration
Root Cause Analysis Chat GPT Cybersecurity
QUIC Protocol SharkFest - WireShark Betty Dubois
ISSA / ISC2 Leadership Podcasts

Packetman007

Control: Protect data – catch phish, stop ransomware



DISCARDS DATA AND SENDS Alert ON 1ST attemp

Exposes THREAT SOURCE ip's – HACKER CAUGHT

Prevents exfiltration

Stops internal and external threats

Global Attack Surface

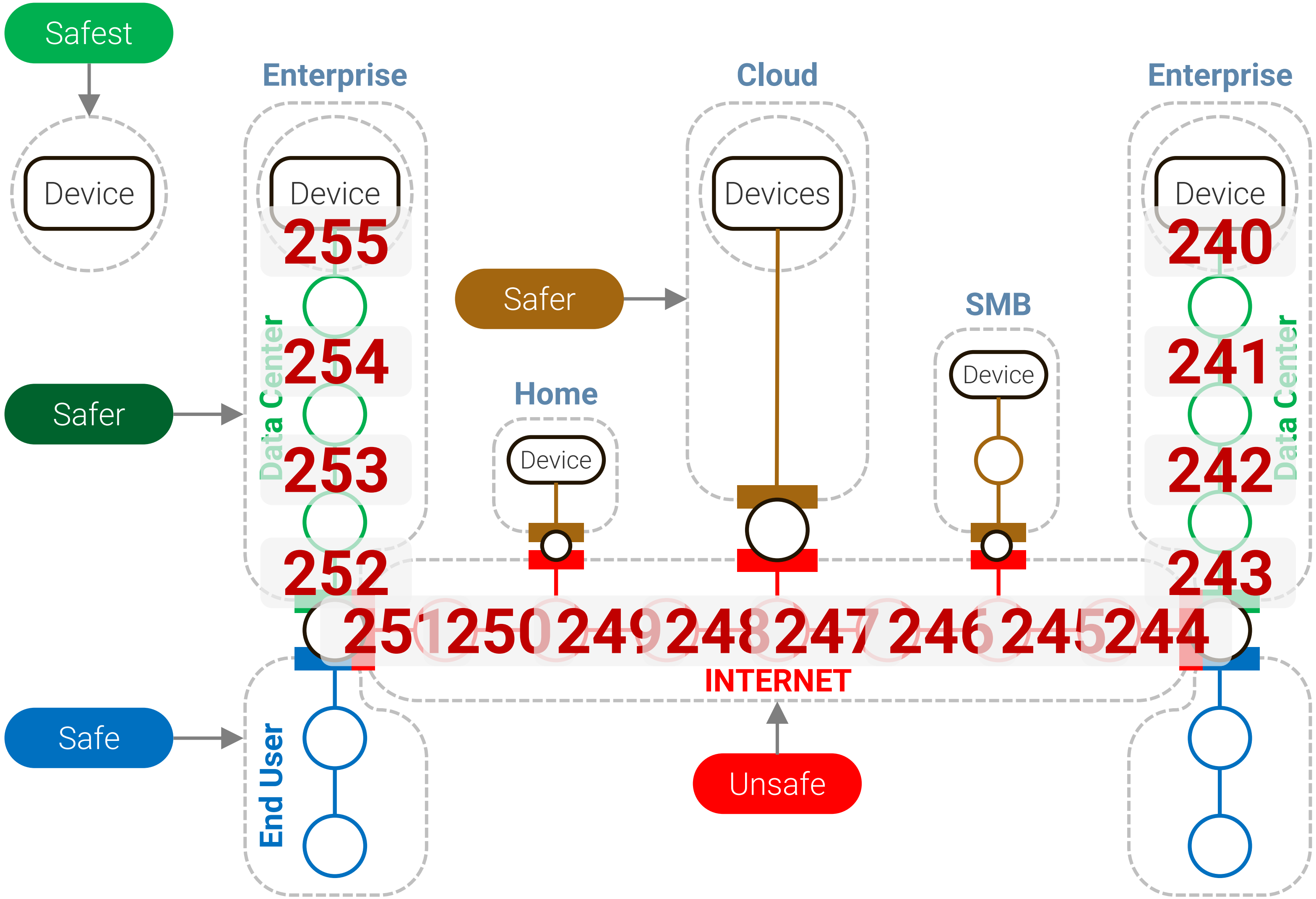
Default Hop Value Dangerously High!

HOPZERO learns Hops needed

Starting Hop   255
At Destination   -240
Hops Needed =15

Linux   64
Microsoft   128
Oracle / Cisco   255

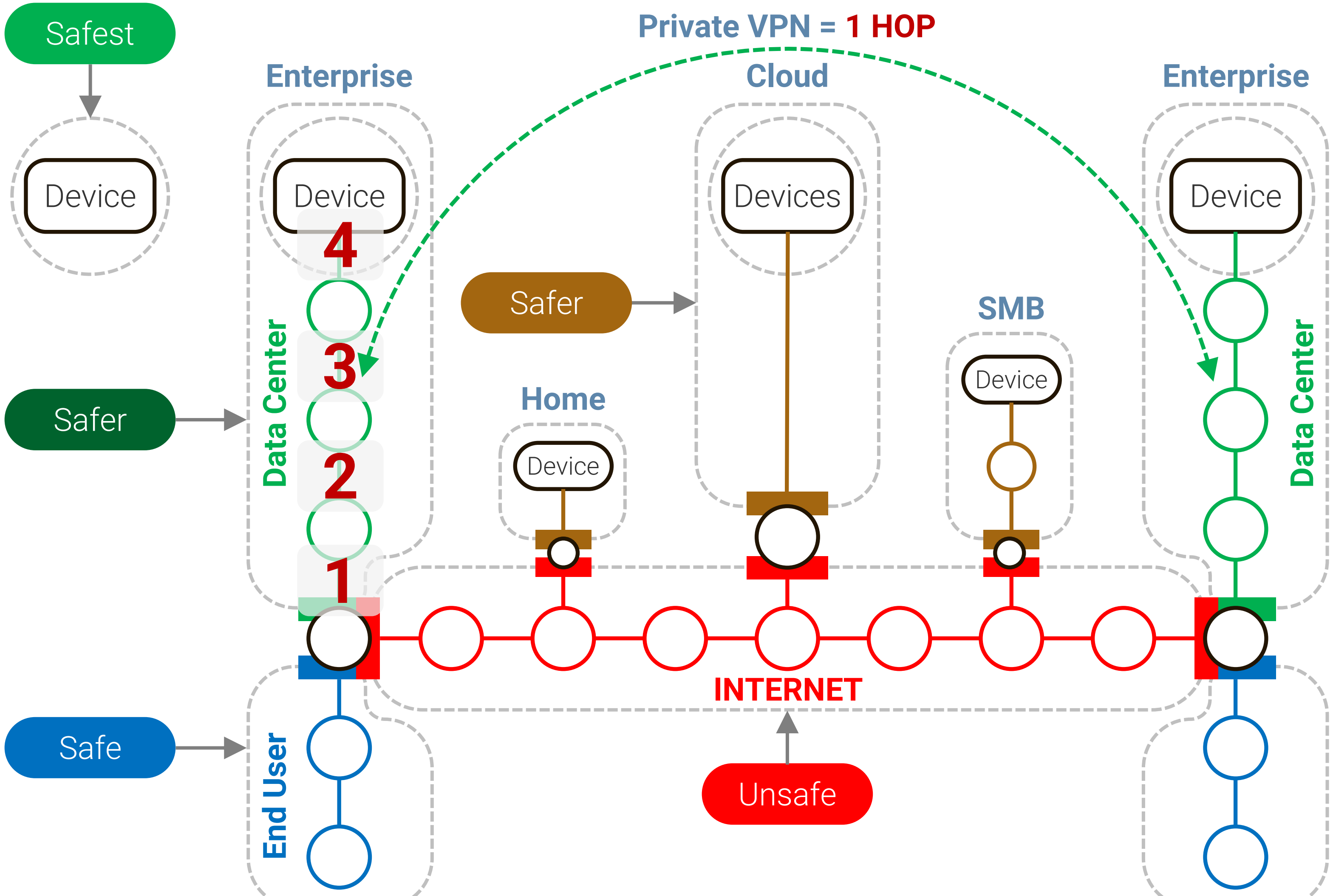
Anything above 40 Hops Allows Global Access



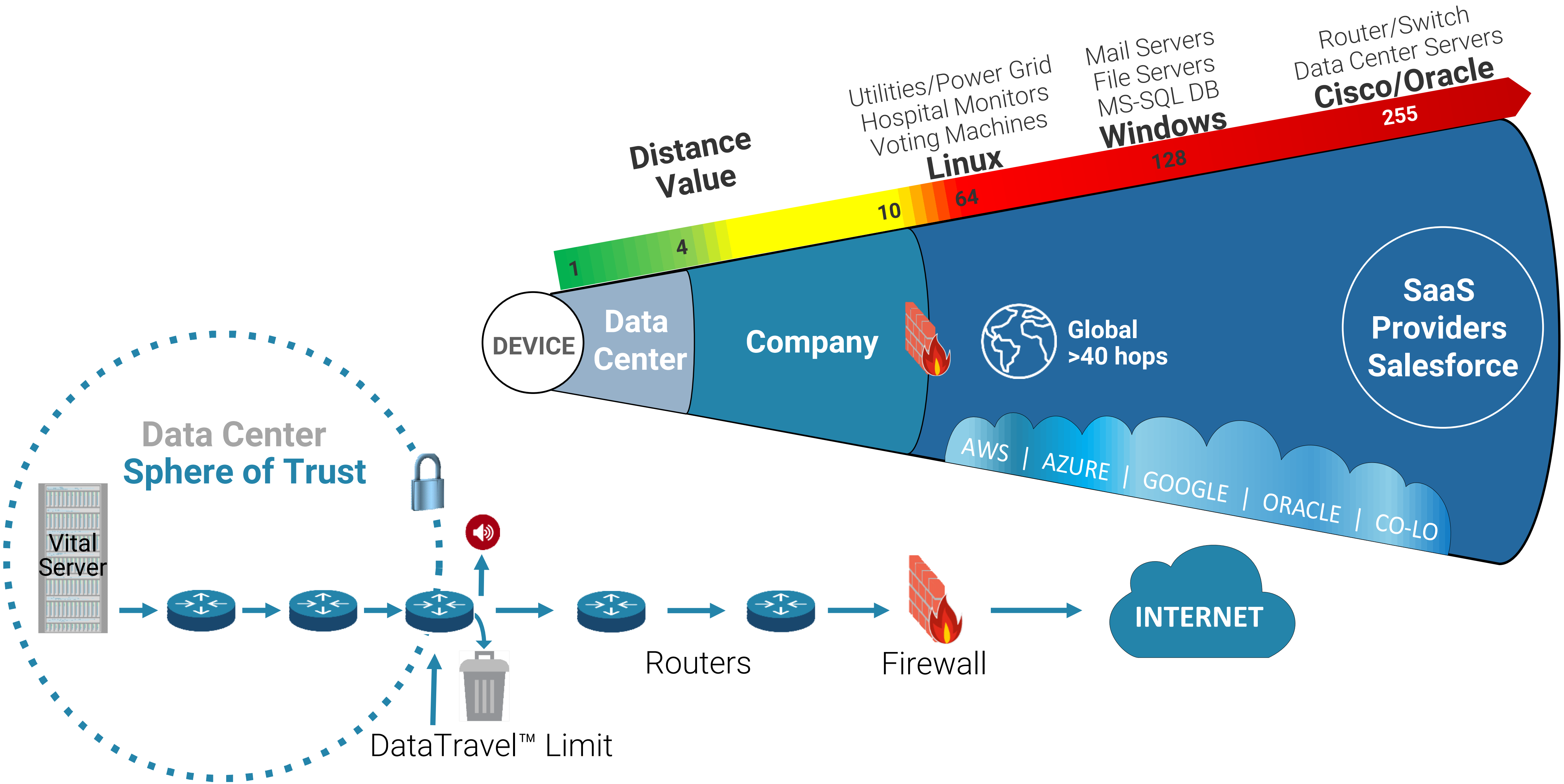
Attack Surface Exposure

Lower HOP Safer Attack Surface

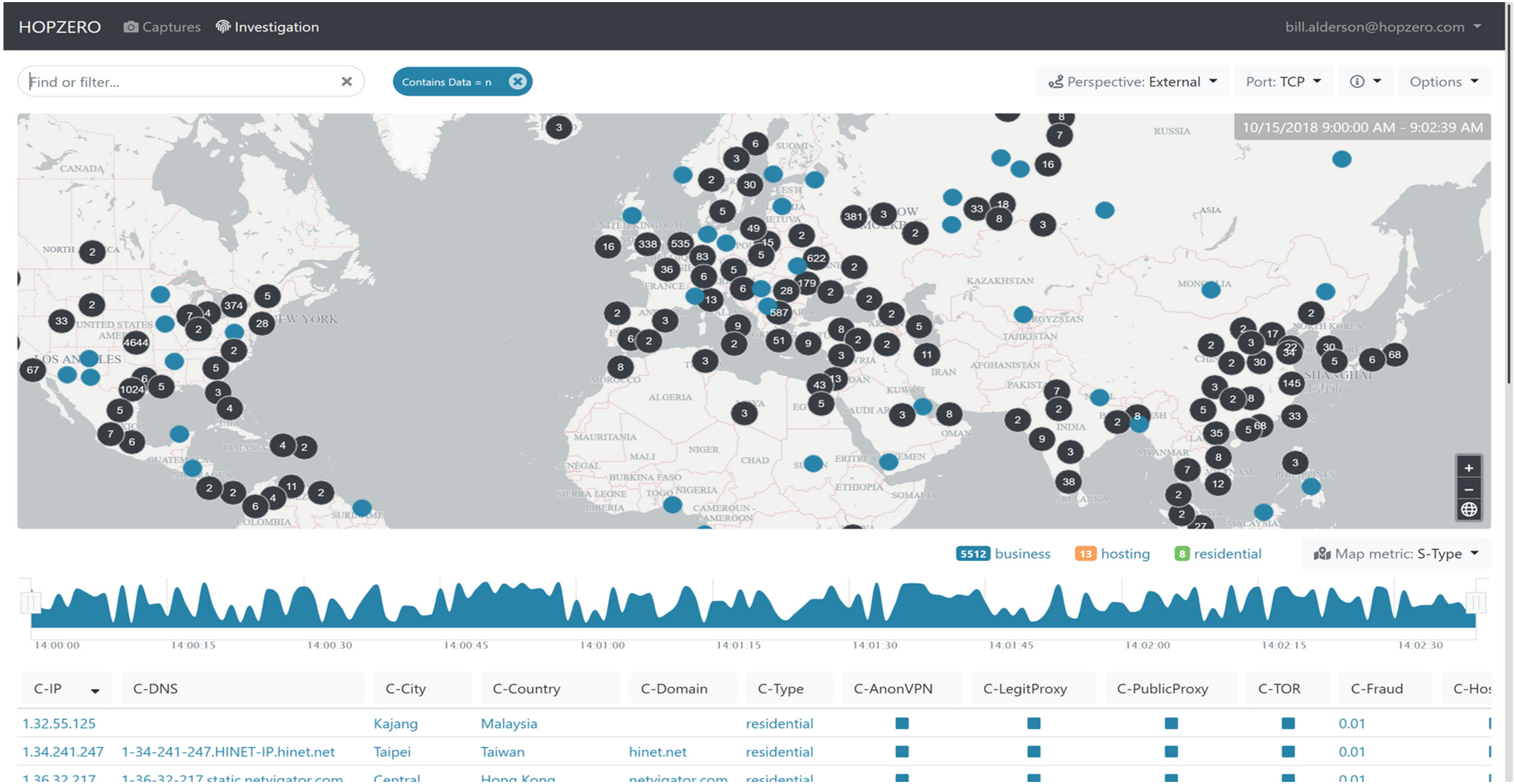
Keeps Data Inside Data Center



DataTravel™ PATENTED SECURITY



DataTravel™ Audit Interactive Map



HOPZERO Captures Investigation bill.alderson@hopzero.com

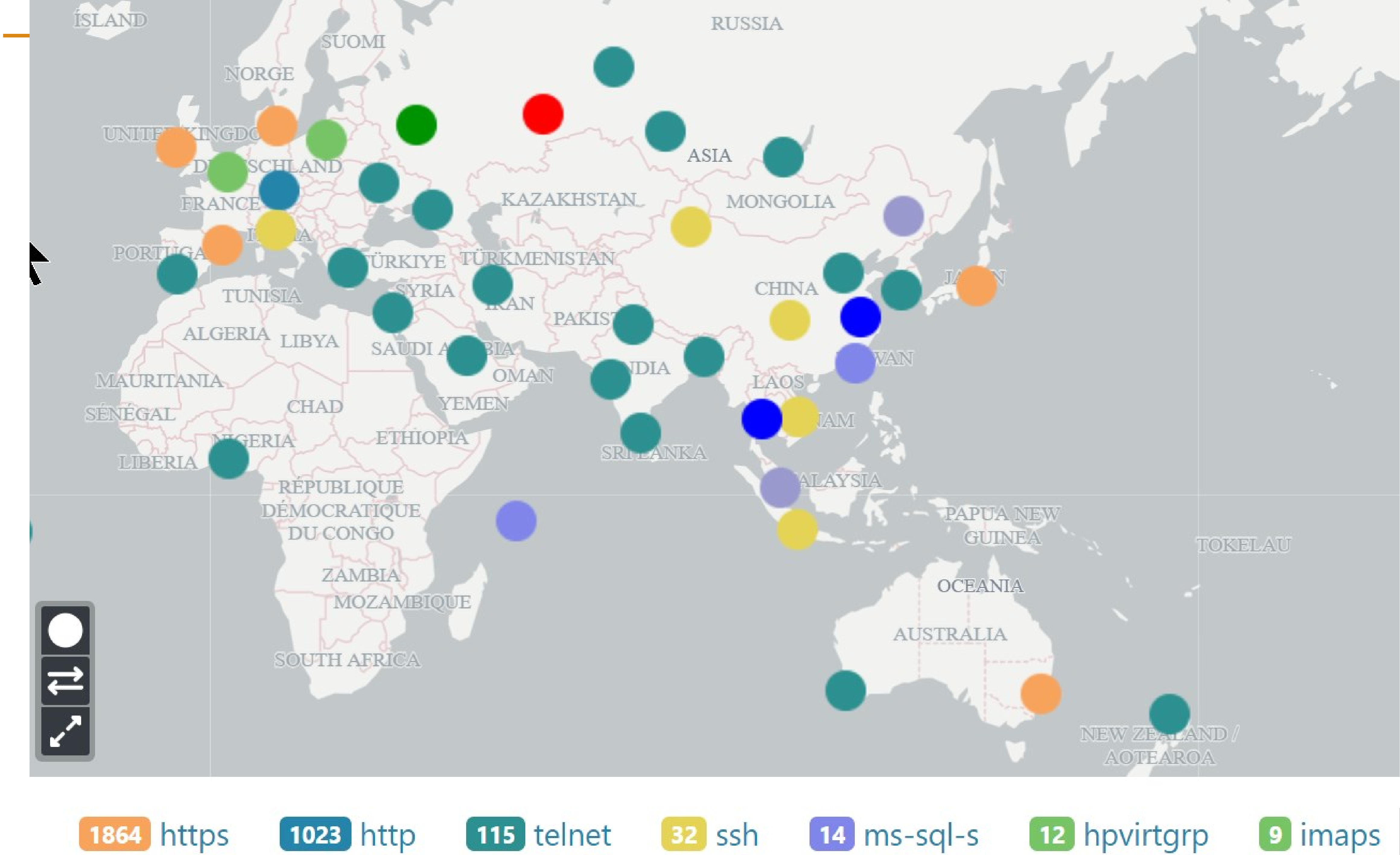
Find or filter... ✕ Contains Data = n ⊗

Perspective: External Port: TCP Options

10/15/2018 9:00:00 AM - 9:02:39 AM

5512 business 13 hosting 8 residential Map metric: S-Type

C-IP	C-DNS	C-City	C-Country	C-Domain	C-Type	C-AnonVPN	C-LegitProxy	C-PublicProxy	C-TOR	C-Fraud	C-Hos
1.32.55.125		Kajang	Malaysia		residential	■	■	■	■	0.01	
1.34.241.247	1-34-241-247.HINET-IP.hinet.net	Taipei	Taiwan	hinet.net	residential	■	■	■	■	0.01	
1.36.32.217	1-36-32-217.static.netvigator.com	Central	Hong Kong	netvigator.com	residential	■	■	■	■	0.01	

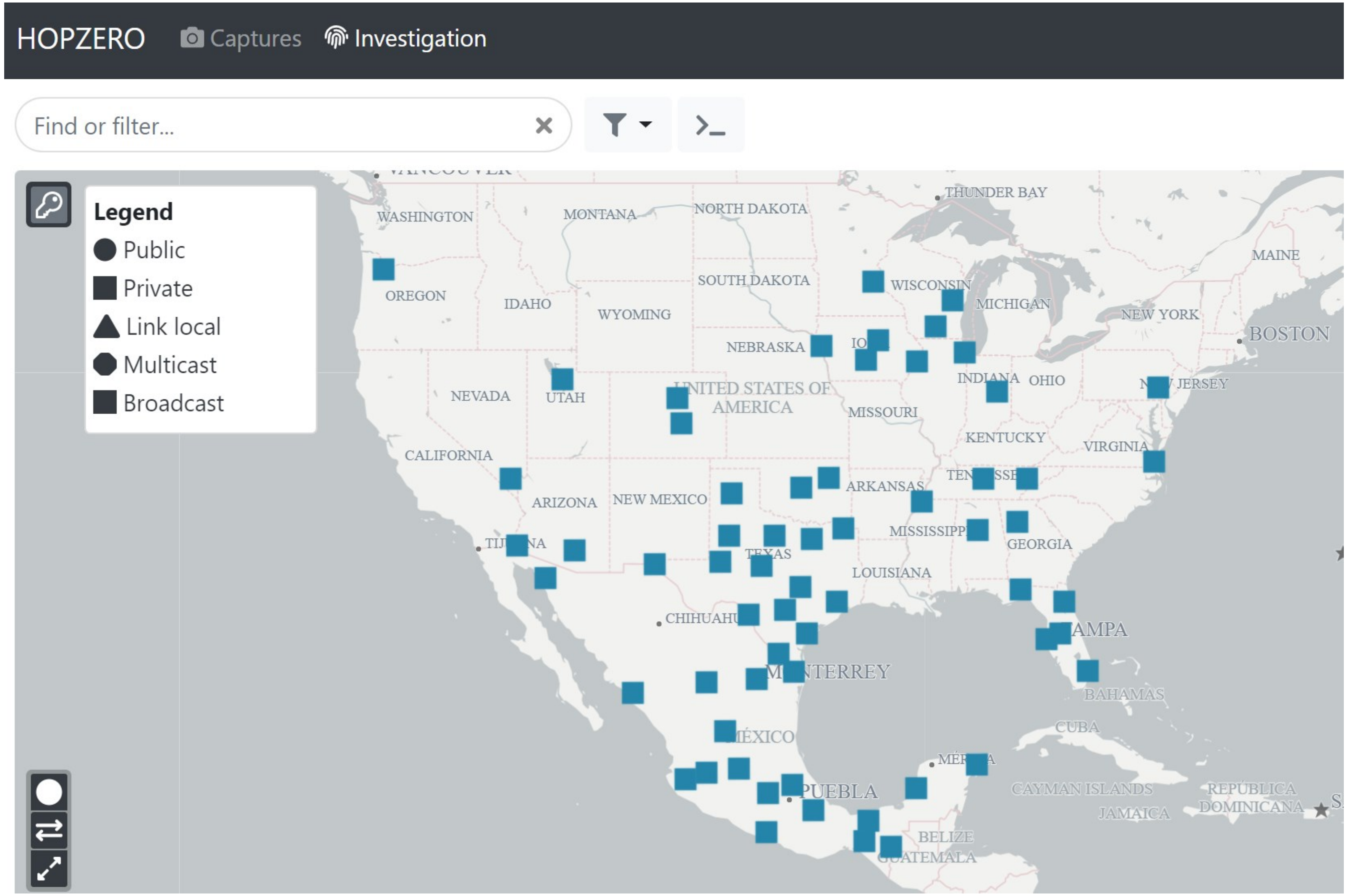


1864 https 1023 http 115 telnet 32 ssh 14 ms-sql-s 12 hpvirtgrp 9 imaps

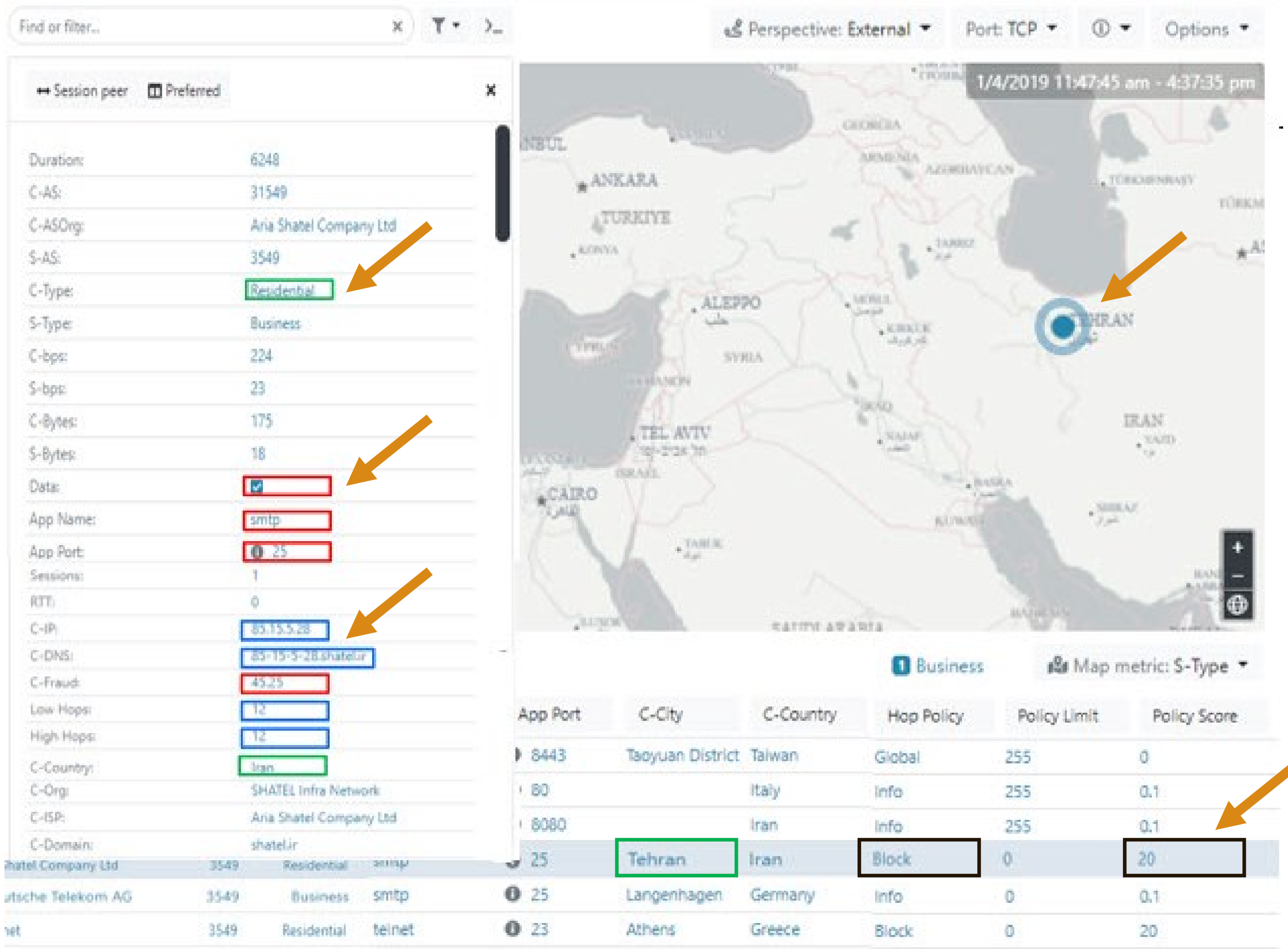
RFC 1918 Internal private address mapping

Corporations have thousands of Internal IP addressed devices at thousands of locations, offices, and retail stores.

The HOPZERO system provides detailed mapping of addresses and filters to see communication session peers.



Vulnerability security research at each click



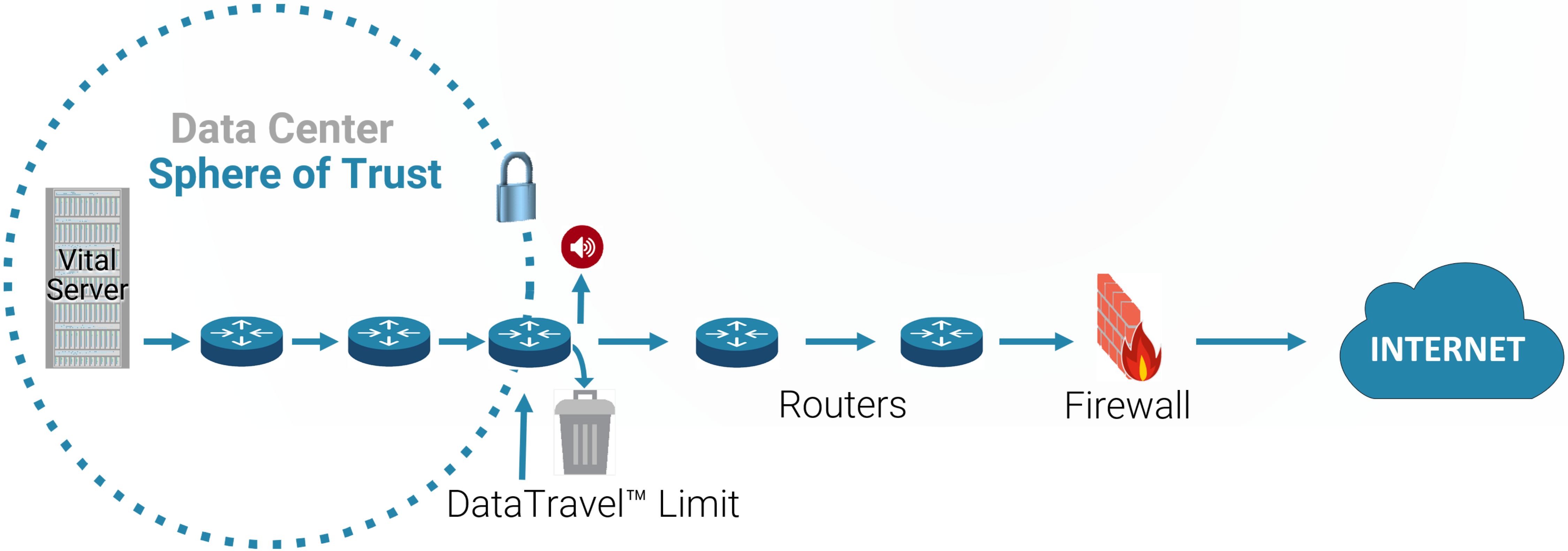
Duration:	6248
C-AS:	31549
C-ASOrg:	Aria Shatel Company Ltd
S-AS:	3549
C-Type:	Residential
S-Type:	Business
C-bps:	224
S-bps:	23
C-Bytes:	175
S-Bytes:	18
Data:	☑
App Name:	smtp
App Port:	25
Sessions:	1
RTT:	0
C-IP:	85.15.5.28
C-DNS:	85-15-5-28.shatel.ir
C-Fraud:	45.25
Low Hops:	12
High Hops:	12
C-Country:	Iran
C-Org:	SHATEL Infra Network
C-ISP:	Aria Shatel Company Ltd
C-Domain:	shatel.ir

				App Port	C-City	C-Country	Hop Policy	Policy Limit	Policy Score
				8443	Taoyuan District	Taiwan	Global	255	0
				80		Italy	Info	255	0.1
				8080		Iran	Info	255	0.1
hatel Company Ltd	3549	Residential	smtp	25	Tehran	Iran	Block	0	20
utsche Telekom AG	3549	Business	smtp	25	Langenhagen	Germany	Info	0	0.1
net	3549	Residential	telnet	23	Athens	Greece	Block	0	20

Description	Value
Client City	Tehran
Client Country	Iran
Location Type	Residential
Data	Yes
App Name	smtp
App Port	25
Client Risk Score	45.25
Client IP Address	85.15.5.28
Client DNS	85-15-5-28.shatel.ir
Low Hops	12
High Hops	12

Policy	Value
Hop Policy	Block
Policy Score	20
High Hops	12

Data Center Sphere of Trust



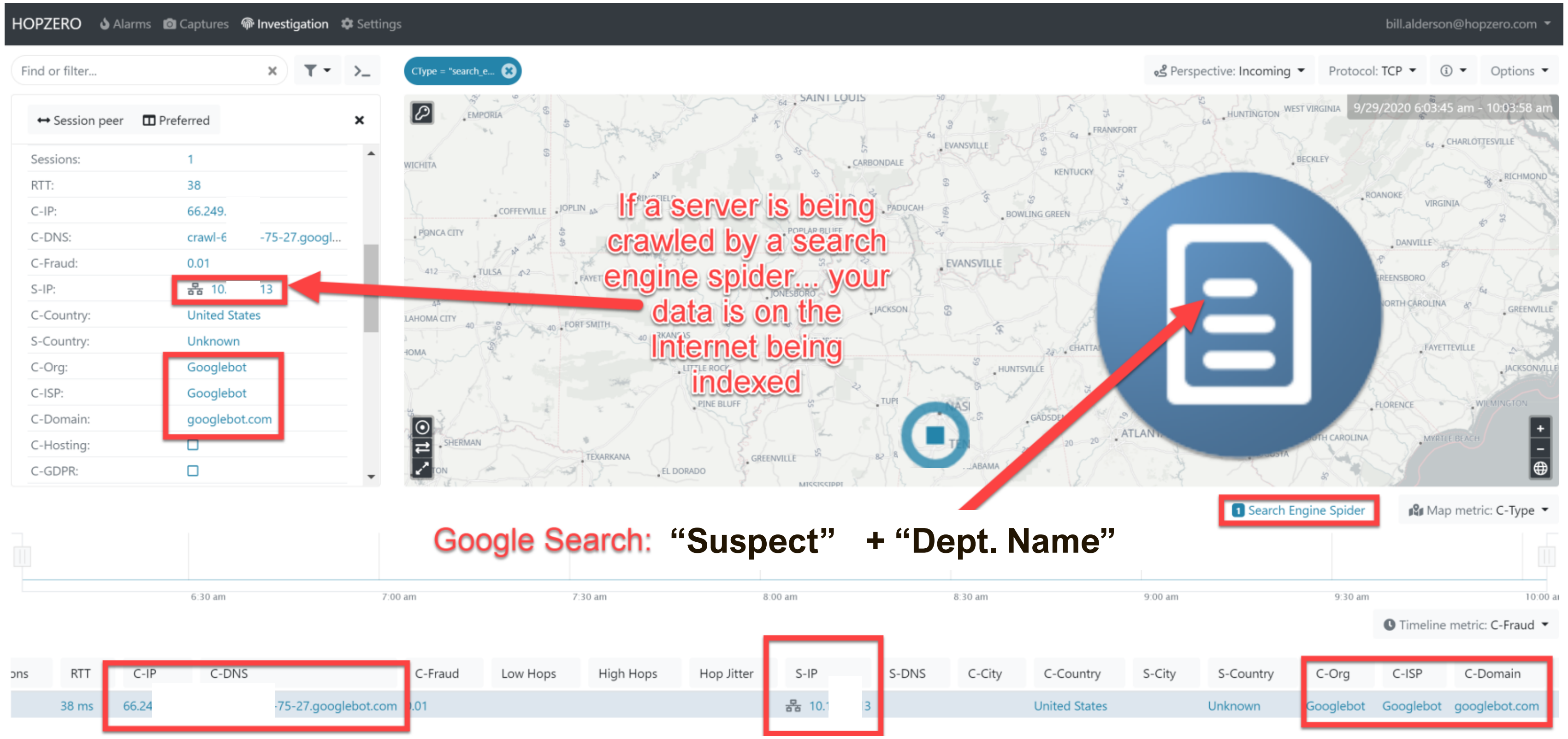
Search Engines

If a Search Engine is connecting to your servers, it is indexing the data so it can offer it up in the search results.

When this happens reporting is required at some level.

Data must be expunged from Google, Bing, Yahoo

One click shows what Search Engines are indexing your server/s



Sessions:	1
RTT:	38
C-IP:	66.249.[redacted]
C-DNS:	crawl-6[redacted]-75-27.googl...
C-Fraud:	0.01
S-IP:	10.[redacted]13
C-Country:	United States
S-Country:	Unknown
C-Org:	Googlebot
C-ISP:	Googlebot
C-Domain:	googlebot.com
C-Hosting:	□
C-GDPR:	□

If a server is being crawled by a search engine spider... your data is on the Internet being indexed

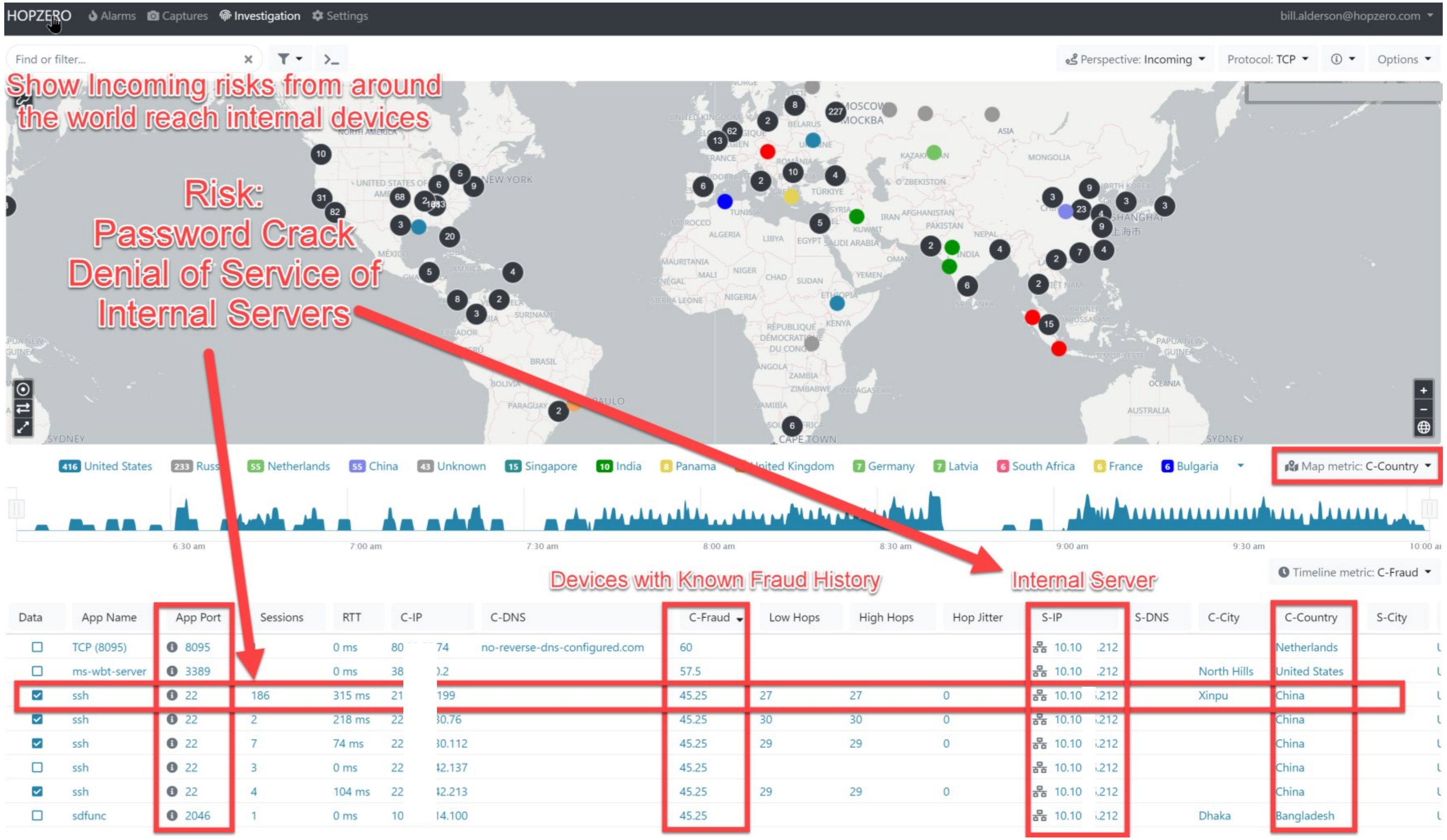
Google Search: “Suspect” + “Dept. Name”

ons	RTT	C-IP	C-DNS	C-Fraud	Low Hops	High Hops	Hop Jitter	S-IP	S-DNS	C-City	C-Country	S-City	S-Country	C-Org	C-ISP	C-Domain
	38 ms	66.24[redacted]	[redacted]-75-27.googlebot.com	.01				10.[redacted]3			United States		Unknown	Googlebot	Googlebot	googlebot.com

Incoming Perspective

Show data coming from around the world visually to comprehend the risk rapidly.

When a device can connect to inside devices it can crack passwords for months and can cause a denial of service on internal devices and across network and firewall infrastructure.



Perspective: Incoming

Protocol: TCP

Show Incoming risks from around the world reach internal devices

Risk: Password Crack Denial of Service of Internal Servers

416 United States · 233 Russ · 55 Netherlands · 55 China · 43 Unknown · 15 Singapore · 10 India · 8 Panama · United Kingdom · 7 Germany · 7 Latvia · 6 South Africa · 6 France · 6 Bulgaria

Map metric: C-Country

Timeline metric: C-Fraud

Devices with Known Fraud History

Internal Server

Data	App Name	App Port	Sessions	RTT	C-IP	C-DNS	C-Fraud	Low Hops	High Hops	Hop Jitter	S-IP	S-DNS	C-City	C-Country	S-City
☐	TCP (8095)	8095		0 ms	80 [redacted] 74	no-reverse-dns-configured.com	60				10.10 [redacted] .212			Netherlands	
☐	ms-wbt-server	3389		0 ms	38 [redacted]).2		57.5				10.10 [redacted] .212		North Hills	United States	
☑	ssh	22	186	315 ms	21 [redacted] 199		45.25	27	27	0	10.10 [redacted] .212		Xinpu	China	
☑	ssh	22	2	218 ms	22 [redacted] 30.76		45.25	30	30	0	10.10 [redacted] .212			China	
☑	ssh	22	7	74 ms	22 [redacted] 30.112		45.25	29	29	0	10.10 [redacted] .212			China	
☐	ssh	22	3	0 ms	22 [redacted] 42.137		45.25				10.10 [redacted] .212			China	
☑	ssh	22	4	104 ms	22 [redacted] 42.213		45.25	29	29	0	10.10 [redacted] .212			China	
☐	sdfunc	2046	1	0 ms	10 [redacted] 14.100		45.25				10.10 [redacted] .212		Dhaka	Bangladesh	

Session connection recording

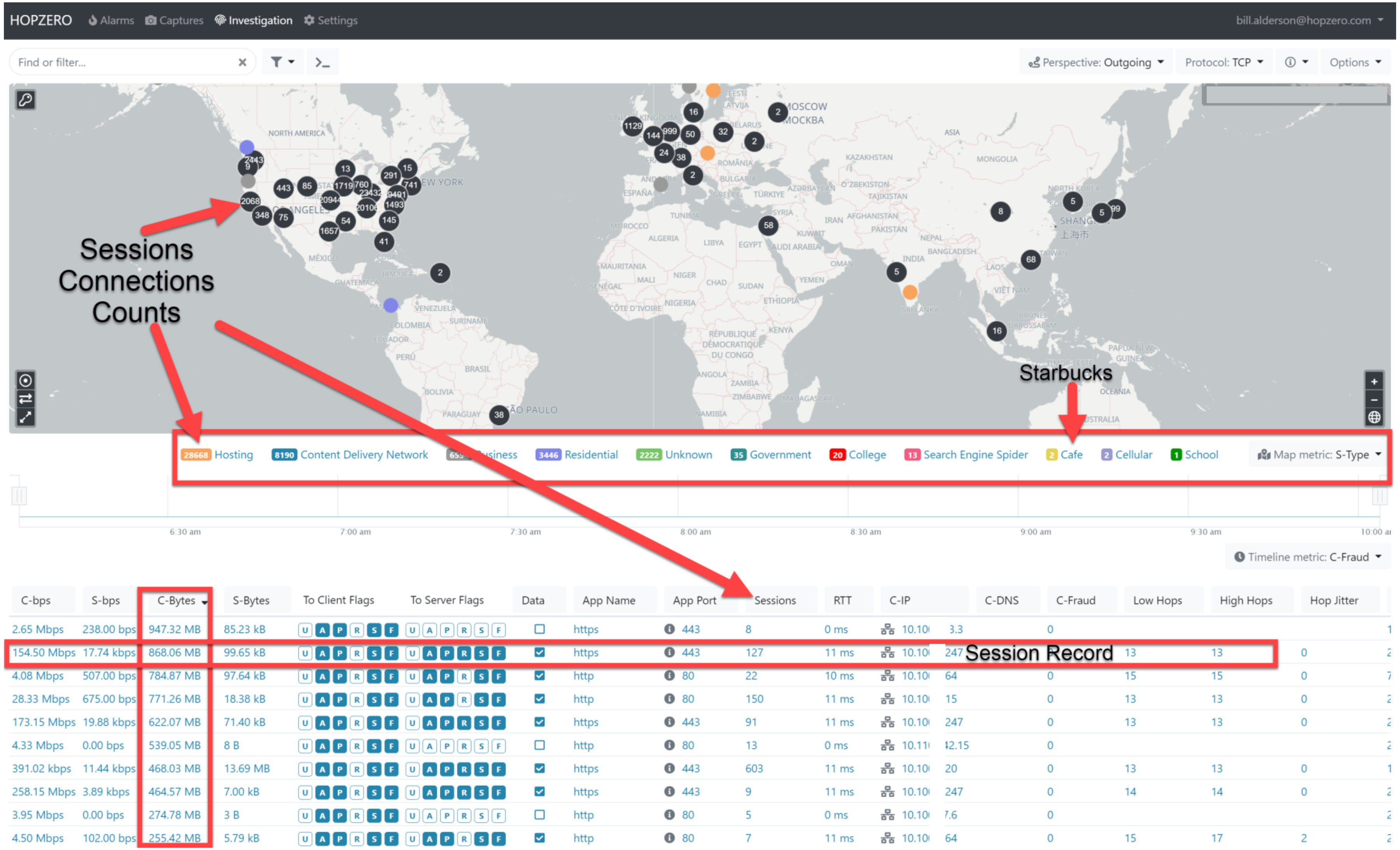
Powerful Sensory Views

A “picture” is worth a thousand logs. You can’t see most system logs, nor correlate information. Log analysis requires expensive experts and mostly manual efforts

Visualizations of:

- Location
- Server Types
- Protocol Apps
- Performance RTT
- Throughput
- Latency

Rapid understanding of complex data security



C-bps	S-bps	C-Bytes	S-Bytes	To Client Flags	To Server Flags	Data	App Name	App Port	Sessions	RTT	C-IP	C-DNS	C-Fraud	Low Hops	High Hops	Hop Jitter	
2.65 Mbps	238.00 bps	947.32 MB	85.23 kB	U A P R S F	U A P R S F	☐	https	443	8	0 ms	10.10 3.3		0				1
154.50 Mbps	17.74 kbps	868.06 MB	99.65 kB	U A P R S F	U A P R S F	☑	https	443	127	11 ms	10.10 247			13	13	0	2
4.08 Mbps	507.00 bps	784.87 MB	97.64 kB	U A P R S F	U A P R S F	☑	http	80	22	10 ms	10.10 64		0	15	15	0	7
28.33 Mbps	675.00 bps	771.26 MB	18.38 kB	U A P R S F	U A P R S F	☑	http	80	150	11 ms	10.10 15		0	13	13	0	2
173.15 Mbps	19.88 kbps	622.07 MB	71.40 kB	U A P R S F	U A P R S F	☑	https	443	91	11 ms	10.10 247		0	13	13	0	2
4.33 Mbps	0.00 bps	539.05 MB	8 B	U A P R S F	U A P R S F	☐	http	80	13	0 ms	10.11 42.15		0				2
391.02 kbps	11.44 kbps	468.03 MB	13.69 MB	U A P R S F	U A P R S F	☑	https	443	603	11 ms	10.10 20		0	13	13	0	1
258.15 Mbps	3.89 kbps	464.57 MB	7.00 kB	U A P R S F	U A P R S F	☑	https	443	9	11 ms	10.10 247		0	14	14	0	2
3.95 Mbps	0.00 bps	274.78 MB	3 B	U A P R S F	U A P R S F	☐	http	80	5	0 ms	10.10 7.6		0				2
4.50 Mbps	102.00 bps	255.42 MB	5.79 kB	U A P R S F	U A P R S F	☑	http	80	7	11 ms	10.10 64		0	15	17	2	2

Session Record

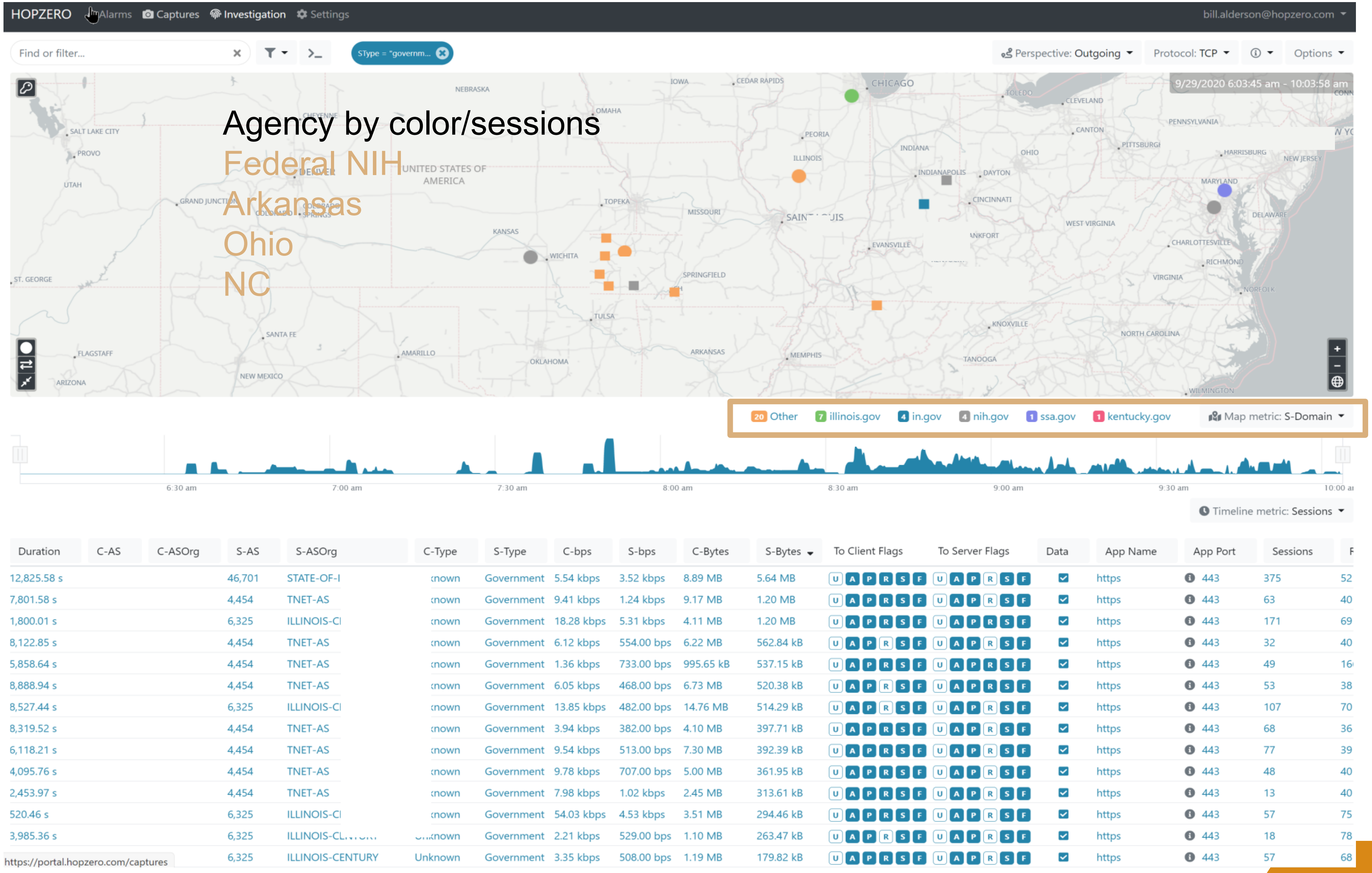
Government customer traffic

If there were a performance issue or a breach with a particular govt agency:

Investigate:
The 5 W’s who, what, when, where, and why
Volume of data
Volume of sessions

One click filters
Agency
User location

By clicking on one location it filters to show only that traffic allowing drill down into the risk or performance to the agency – providing both response time and throughput.



Agency by color/sessions
Federal NIH
Arkansas
Ohio
NC

20 Other | 7 illinois.gov | 4 in.gov | 4 nih.gov | 1 ssa.gov | 1 kentucky.gov | Map metric: S-Domain

Timeline metric: Sessions

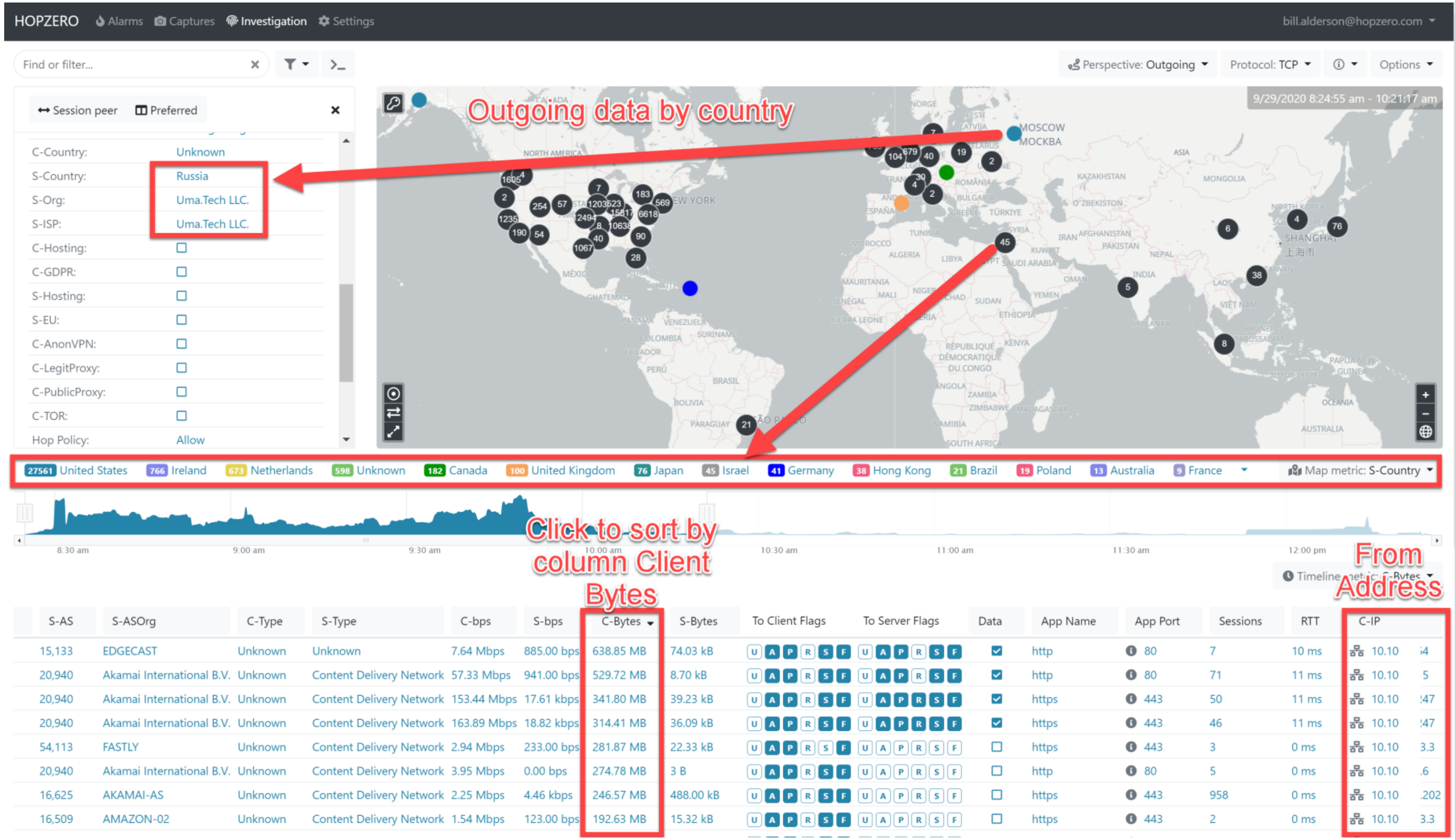
Duration	C-AS	C-ASOrg	S-AS	S-ASOrg	C-Type	S-Type	C-bps	S-bps	C-Bytes	S-Bytes	To Client Flags	To Server Flags	Data	App Name	App Port	Sessions	F
12,825.58 s			46,701	STATE-OF-I	known	Government	5.54 kbps	3.52 kbps	8.89 MB	5.64 MB	U A P R S F	U A P R S F	☑	https	443	375	52
7,801.58 s			4,454	TNET-AS	known	Government	9.41 kbps	1.24 kbps	9.17 MB	1.20 MB	U A P R S F	U A P R S F	☑	https	443	63	40
1,800.01 s			6,325	ILLINOIS-CI	known	Government	18.28 kbps	5.31 kbps	4.11 MB	1.20 MB	U A P R S F	U A P R S F	☑	https	443	171	69
8,122.85 s			4,454	TNET-AS	known	Government	6.12 kbps	554.00 bps	6.22 MB	562.84 kB	U A P R S F	U A P R S F	☑	https	443	32	40
5,858.64 s			4,454	TNET-AS	known	Government	1.36 kbps	733.00 bps	995.65 kB	537.15 kB	U A P R S F	U A P R S F	☑	https	443	49	16
8,888.94 s			4,454	TNET-AS	known	Government	6.05 kbps	468.00 bps	6.73 MB	520.38 kB	U A P R S F	U A P R S F	☑	https	443	53	38
8,527.44 s			6,325	ILLINOIS-CI	known	Government	13.85 kbps	482.00 bps	14.76 MB	514.29 kB	U A P R S F	U A P R S F	☑	https	443	107	70
8,319.52 s			4,454	TNET-AS	known	Government	3.94 kbps	382.00 bps	4.10 MB	397.71 kB	U A P R S F	U A P R S F	☑	https	443	68	36
6,118.21 s			4,454	TNET-AS	known	Government	9.54 kbps	513.00 bps	7.30 MB	392.39 kB	U A P R S F	U A P R S F	☑	https	443	77	39
4,095.76 s			4,454	TNET-AS	known	Government	9.78 kbps	707.00 bps	5.00 MB	361.95 kB	U A P R S F	U A P R S F	☑	https	443	48	40
2,453.97 s			4,454	TNET-AS	known	Government	7.98 kbps	1.02 kbps	2.45 MB	313.61 kB	U A P R S F	U A P R S F	☑	https	443	13	40
520.46 s			6,325	ILLINOIS-CI	known	Government	54.03 kbps	4.53 kbps	3.51 MB	294.46 kB	U A P R S F	U A P R S F	☑	https	443	57	75
3,985.36 s			6,325	ILLINOIS-CL	known	Government	2.21 kbps	529.00 bps	1.10 MB	263.47 kB	U A P R S F	U A P R S F	☑	https	443	18	78
https://portal.hopzero.com/captures			6,325	ILLINOIS-CENTURY	Unknown	Government	3.35 kbps	508.00 bps	1.19 MB	179.82 kB	U A P R S F	U A P R S F	☑	https	443	57	68

outgoing perspective by country

See data being sent by outbound connections around the world to comprehend the exfiltration data risk using powerful human vision that hidden text logs don't illustrate.

Sort by Data Volume or any other column.

Outgoing data is hard to control, as users are free to connect to any site. This is often controlled by egress firewall rules to stop exfiltration for sensitive Apps like SQL databases and File Services.



Outgoing data by country

C-Country:	Unknown
S-Country:	Russia
S-Org:	Uma.Tech LLC.
S-ISP:	Uma.Tech LLC.
C-Hosting:	□
C-GDPR:	□
S-Hosting:	□
S-EU:	□
C-AnonVPN:	□
C-LegitProxy:	□
C-PublicProxy:	□
C-TOR:	□
Hop Policy:	Allow

27561 United States · 766 Ireland · 673 Netherlands · 598 Unknown · 182 Canada · 100 United Kingdom · 76 Japan · 45 Israel · 41 Germany · 38 Hong Kong · 21 Brazil · 19 Poland · 13 Australia · 9 France

Click to sort by column Client Bytes

From Address

S-AS	S-ASOrg	C-Type	S-Type	C-bps	S-bps	C-Bytes	S-Bytes	To Client Flags	To Server Flags	Data	App Name	App Port	Sessions	RTT	C-IP
15,133	EDGECAST	Unknown	Unknown	7.64 Mbps	885.00 bps	638.85 MB	74.03 kB	U A P R S F	U A P R S F	☑	http	80	7	10 ms	10.10 :4
20,940	Akamai International B.V.	Unknown	Content Delivery Network	57.33 Mbps	941.00 bps	529.72 MB	8.70 kB	U A P R S F	U A P R S F	☑	http	80	71	11 ms	10.10 5
20,940	Akamai International B.V.	Unknown	Content Delivery Network	153.44 Mbps	17.61 kbps	341.80 MB	39.23 kB	U A P R S F	U A P R S F	☑	https	443	50	11 ms	10.10 !47
20,940	Akamai International B.V.	Unknown	Content Delivery Network	163.89 Mbps	18.82 kbps	314.41 MB	36.09 kB	U A P R S F	U A P R S F	☑	https	443	46	11 ms	10.10 !47
54,113	FASTLY	Unknown	Content Delivery Network	2.94 Mbps	233.00 bps	281.87 MB	22.33 kB	U A P R S F	U A P R S F	□	https	443	3	0 ms	10.10 3.3
20,940	Akamai International B.V.	Unknown	Content Delivery Network	3.95 Mbps	0.00 bps	274.78 MB	3 B	U A P R S F	U A P R S F	□	http	80	5	0 ms	10.10 .6
16,625	AKAMAI-AS	Unknown	Content Delivery Network	2.25 Mbps	4.46 kbps	246.57 MB	488.00 kB	U A P R S F	U A P R S F	□	https	443	958	0 ms	10.10 .202
16,509	AMAZON-02	Unknown	Content Delivery Network	1.54 Mbps	123.00 bps	192.63 MB	15.32 kB	U A P R S F	U A P R S F	□	https	443	2	0 ms	10.10 3.3

Suspect internal repeated requests

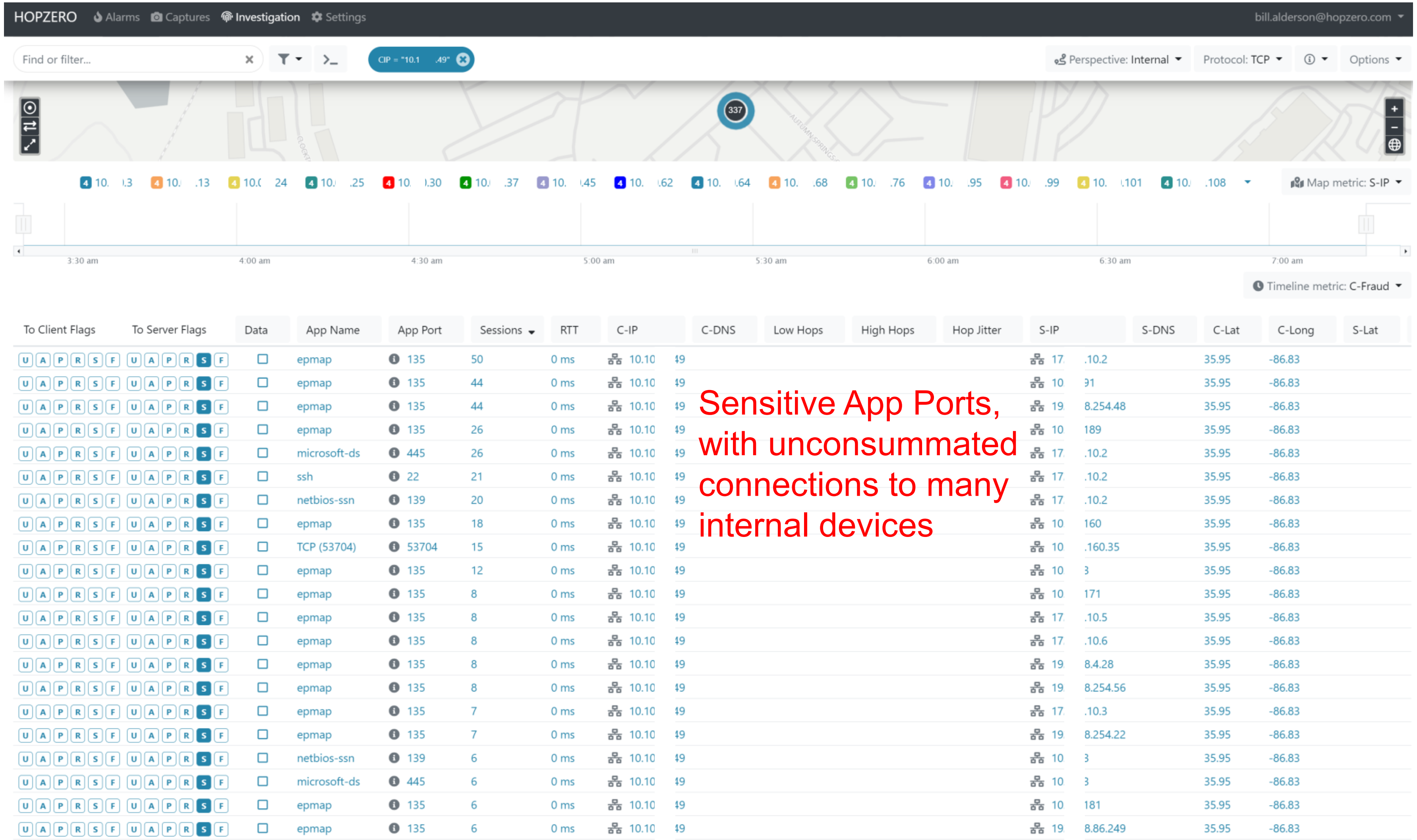
Internal devices

- Misconfigured
- Misbehaving
- Infected
- Malicious
- Compromised

Odd Behaviors: Repetitious, nonresponsive connection / login requests sent to sensitive or random devices

In this example it shows a device making sensitive connection requests in a repeated manner to internal devices.

Finding and vetting this type of behavior often results in solving a problem.



To Client Flags	To Server Flags	Data	App Name	App Port	Sessions	RTT	C-IP	C-DNS	Low Hops	High Hops	Hop Jitter	S-IP	S-DNS	C-Lat	C-Long	S-Lat
U A P R S F	U A P R S F	□	epmap	135	50	0 ms	10.10 49					17. .10.2		35.95	-86.83	
U A P R S F	U A P R S F	□	epmap	135	44	0 ms	10.10 49					10. 91		35.95	-86.83	
U A P R S F	U A P R S F	□	epmap	135	44	0 ms	10.10 49					19. 8.254.48		35.95	-86.83	
U A P R S F	U A P R S F	□	epmap	135	26	0 ms	10.10 49					10. 189		35.95	-86.83	
U A P R S F	U A P R S F	□	microsoft-ds	445	26	0 ms	10.10 49					17. .10.2		35.95	-86.83	
U A P R S F	U A P R S F	□	ssh	22	21	0 ms	10.10 49					17. .10.2		35.95	-86.83	
U A P R S F	U A P R S F	□	netbios-ssn	139	20	0 ms	10.10 49					17. .10.2		35.95	-86.83	
U A P R S F	U A P R S F	□	epmap	135	18	0 ms	10.10 49					10. 160		35.95	-86.83	
U A P R S F	U A P R S F	□	TCP (53704)	53704	15	0 ms	10.10 49					10. .160.35		35.95	-86.83	
U A P R S F	U A P R S F	□	epmap	135	12	0 ms	10.10 49					10. 3		35.95	-86.83	
U A P R S F	U A P R S F	□	epmap	135	8	0 ms	10.10 49					10. 171		35.95	-86.83	
U A P R S F	U A P R S F	□	epmap	135	8	0 ms	10.10 49					17. .10.5		35.95	-86.83	
U A P R S F	U A P R S F	□	epmap	135	8	0 ms	10.10 49					17. .10.6		35.95	-86.83	
U A P R S F	U A P R S F	□	epmap	135	8	0 ms	10.10 49					19. 8.4.28		35.95	-86.83	
U A P R S F	U A P R S F	□	epmap	135	8	0 ms	10.10 49					19. 8.254.56		35.95	-86.83	
U A P R S F	U A P R S F	□	epmap	135	7	0 ms	10.10 49					17. .10.3		35.95	-86.83	
U A P R S F	U A P R S F	□	epmap	135	7	0 ms	10.10 49					19. 8.254.22		35.95	-86.83	
U A P R S F	U A P R S F	□	netbios-ssn	139	6	0 ms	10.10 49					10. 3		35.95	-86.83	
U A P R S F	U A P R S F	□	microsoft-ds	445	6	0 ms	10.10 49					10. 3		35.95	-86.83	
U A P R S F	U A P R S F	□	epmap	135	6	0 ms	10.10 49					10. 181		35.95	-86.83	
U A P R S F	U A P R S F	□	epmap	135	6	0 ms	10.10 49					19. 8.86.249		35.95	-86.83	

Sensitive App Ports, with unconsummated connections to many internal devices

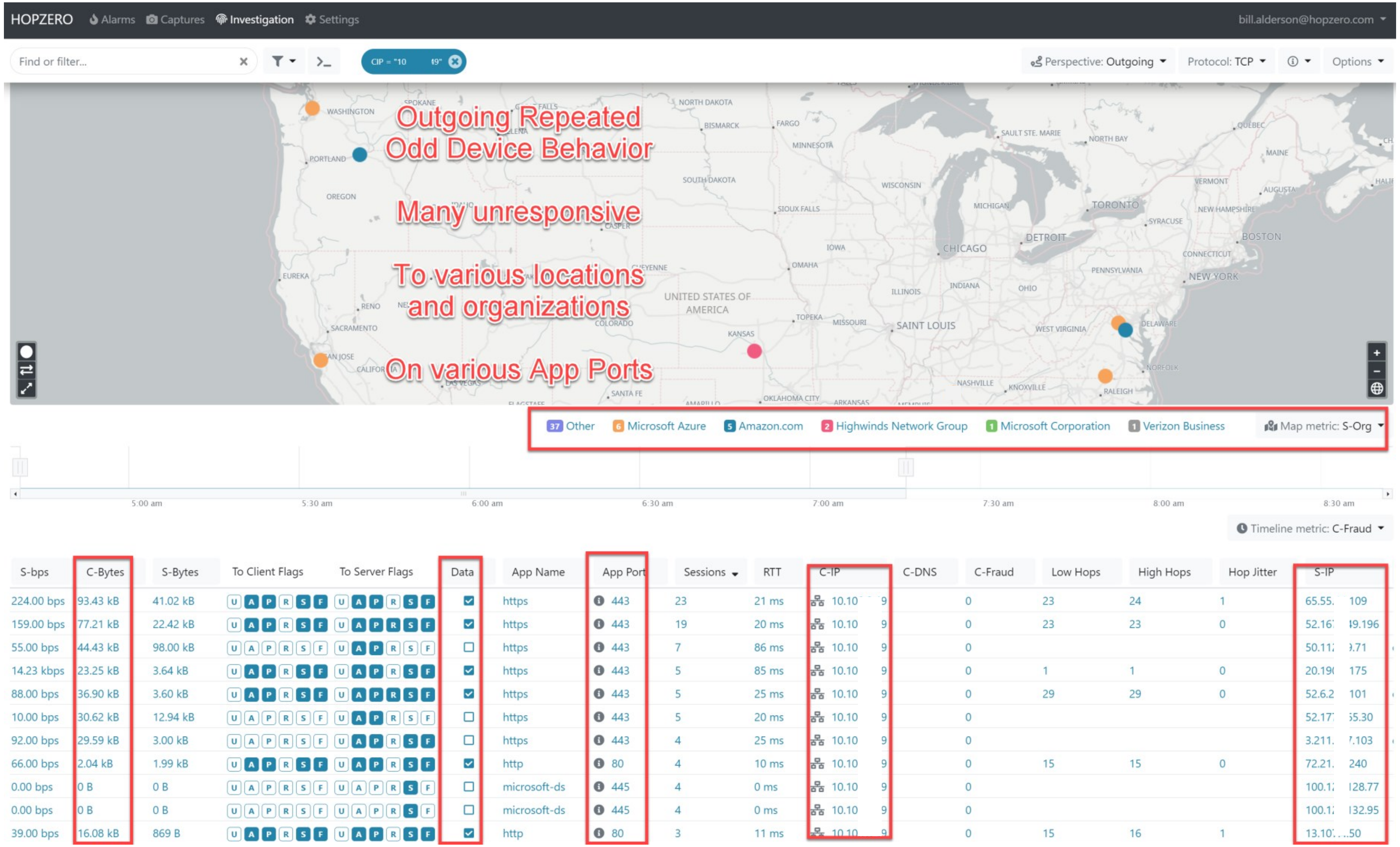
Suspect outgoing external repeated requests

Internal devices
- Misconfigured
- Misbehaving
- Infected
- Malicious
- Compromised

Odd Behaviors: Repetitious, nonresponsive connection / login requests sent to sensitive or random devices

In this example it shows a device making sensitive connection requests in a repeated manner to Internal external devices.

Finding and vetting this type of behavior often results in solving a problem.



Outgoing Repeated Odd Device Behavior

Many unresponsive

To various locations and organizations

On various App Ports

37 Other · 6 Microsoft Azure · 5 Amazon.com · 2 Highwinds Network Group · 1 Microsoft Corporation · 1 Verizon Business

Map metric: S-Org

Timeline metric: C-Fraud

S-bps	C-Bytes	S-Bytes	To Client Flags	To Server Flags	Data	App Name	App Port	Sessions	RTT	C-IP	C-DNS	C-Fraud	Low Hops	High Hops	Hop Jitter	S-IP
224.00 bps	93.43 kB	41.02 kB	U **A** **P** R **S** **F**	U **A** **P** R **S** **F**	☑	https	443	23	21 ms	10.10[redacted]9		0	23	24	1	65.55.[redacted]109
159.00 bps	77.21 kB	22.42 kB	U **A** **P** R **S** **F**	U **A** **P** **R** **S** **F**	☑	https	443	19	20 ms	10.10[redacted]9		0	23	23	0	52.16[redacted]49.196
55.00 bps	44.43 kB	98.00 kB	U A P R S F	U **A** **P** R S F	☐	https	443	7	86 ms	10.10[redacted]9		0				50.11[redacted].71
14.23 kbps	23.25 kB	3.64 kB	U **A** **P** R **S** **F**	U **A** **P** R **S** **F**	☑	https	443	5	85 ms	10.10[redacted]9		0	1	1	0	20.19[redacted]175
88.00 bps	36.90 kB	3.60 kB	U **A** **P** R **S** **F**	U **A** **P** **R** **S** **F**	☑	https	443	5	25 ms	10.10[redacted]9		0	29	29	0	52.6.2[redacted]101
10.00 bps	30.62 kB	12.94 kB	U A P R S F	U **A** **P** R S F	☐	https	443	5	20 ms	10.10[redacted]9		0				52.17[redacted]55.30
92.00 bps	29.59 kB	3.00 kB	U A P R S F	U **A** **P** R **S** **F**	☐	https	443	4	25 ms	10.10[redacted]9		0				3.211.[redacted].103
66.00 bps	2.04 kB	1.99 kB	U **A** **P** R **S** **F**	U **A** **P** R **S** **F**	☑	http	80	4	10 ms	10.10[redacted]9		0	15	15	0	72.21.[redacted]240
0.00 bps	0 B	0 B	U A P R S F	U A P R **S** F	☐	microsoft-ds	445	4	0 ms	10.10[redacted]9		0				100.1[redacted]128.77
0.00 bps	0 B	0 B	U A P R S F	U A P R **S** F	☐	microsoft-ds	445	4	0 ms	10.10[redacted]9		0				100.1[redacted]132.95
39.00 bps	16.08 kB	869 B	U **A** **P** R **S** **F**	U **A** **P** R **S** **F**	☑	http	80	3	11 ms	10.10[redacted]9		0	15	16	1	13.10[redacted].50

2nd Suspect outgoing external repeated requests

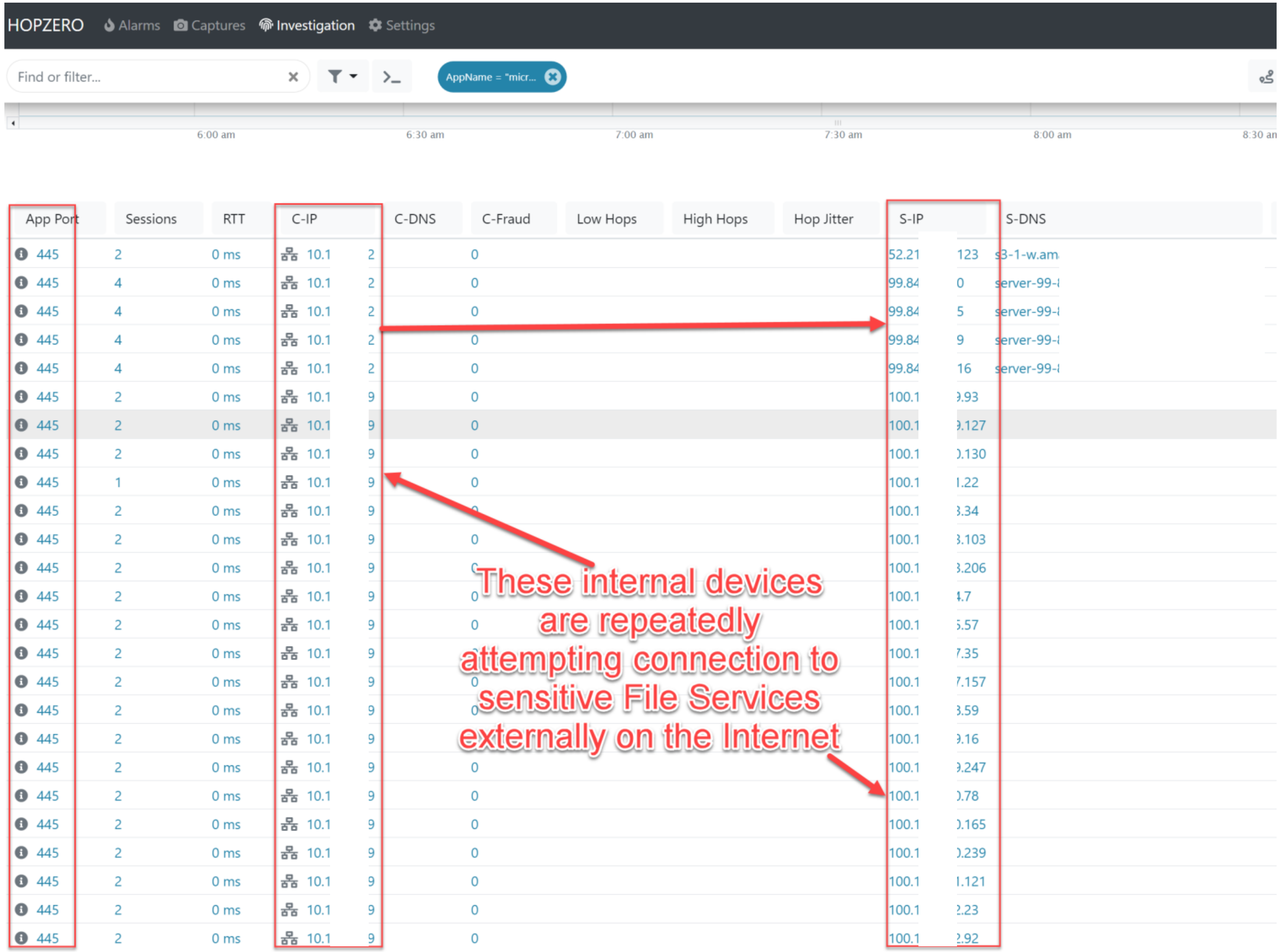
Internal devices

- Misconfigured
- Misbehaving
- Infected
- Malicious
- Compromised

Odd Behaviors: Repetitious, nonresponsive connection / login requests sent to sensitive or random devices

In this example it shows a device making sensitive connection requests in a repeated manner to Internal external devices.

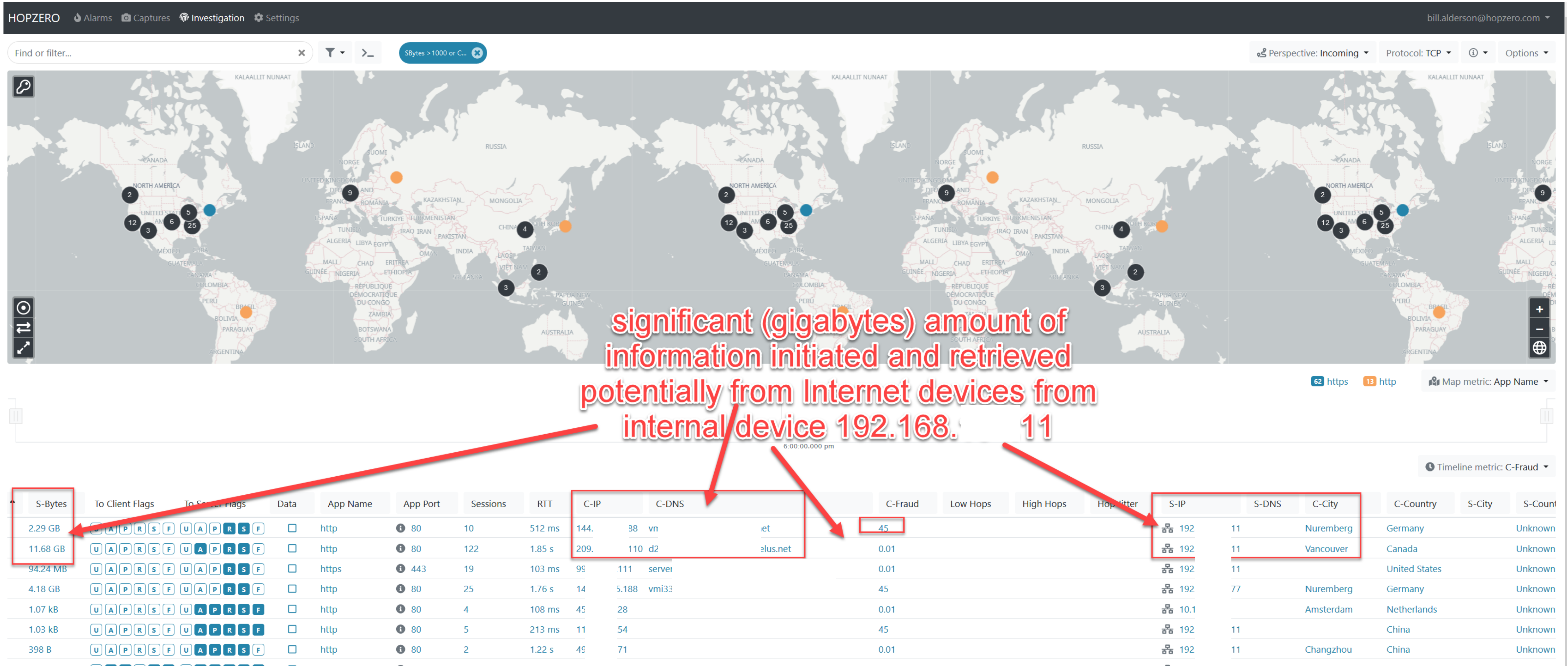
Finding and vetting this type of behavior often results in solving a problem.



App Port	Sessions	RTT	C-IP	C-DNS	C-Fraud	Low Hops	High Hops	Hop Jitter	S-IP	S-DNS
445	2	0 ms	10.1 2		0				52.21 123	s3-1-w.am
445	4	0 ms	10.1 2		0				99.84 0	server-99-
445	4	0 ms	10.1 2		0				99.84 5	server-99-
445	4	0 ms	10.1 2		0				99.84 9	server-99-
445	4	0 ms	10.1 2		0				99.84 16	server-99-
445	2	0 ms	10.1 9		0				100.1 9.93	
445	2	0 ms	10.1 9		0				100.1 9.127	
445	2	0 ms	10.1 9		0				100.1 0.130	
445	1	0 ms	10.1 9		0				100.1 1.22	
445	2	0 ms	10.1 9		0				100.1 3.34	
445	2	0 ms	10.1 9		0				100.1 3.103	
445	2	0 ms	10.1 9		0				100.1 3.206	
445	2	0 ms	10.1 9		0				100.1 4.7	
445	2	0 ms	10.1 9		0				100.1 5.57	
445	2	0 ms	10.1 9		0				100.1 7.35	
445	2	0 ms	10.1 9		0				100.1 7.157	
445	2	0 ms	10.1 9		0				100.1 3.59	
445	2	0 ms	10.1 9		0				100.1 9.16	
445	2	0 ms	10.1 9		0				100.1 9.247	
445	2	0 ms	10.1 9		0				100.1 0.78	
445	2	0 ms	10.1 9		0				100.1 0.165	
445	2	0 ms	10.1 9		0				100.1 0.239	
445	2	0 ms	10.1 9		0				100.1 1.121	
445	2	0 ms	10.1 9		0				100.1 2.23	
445	2	0 ms	10.1 9		0				100.1 2.92	

These internal devices are repeatedly attempting connection to sensitive File Services externally on the Internet

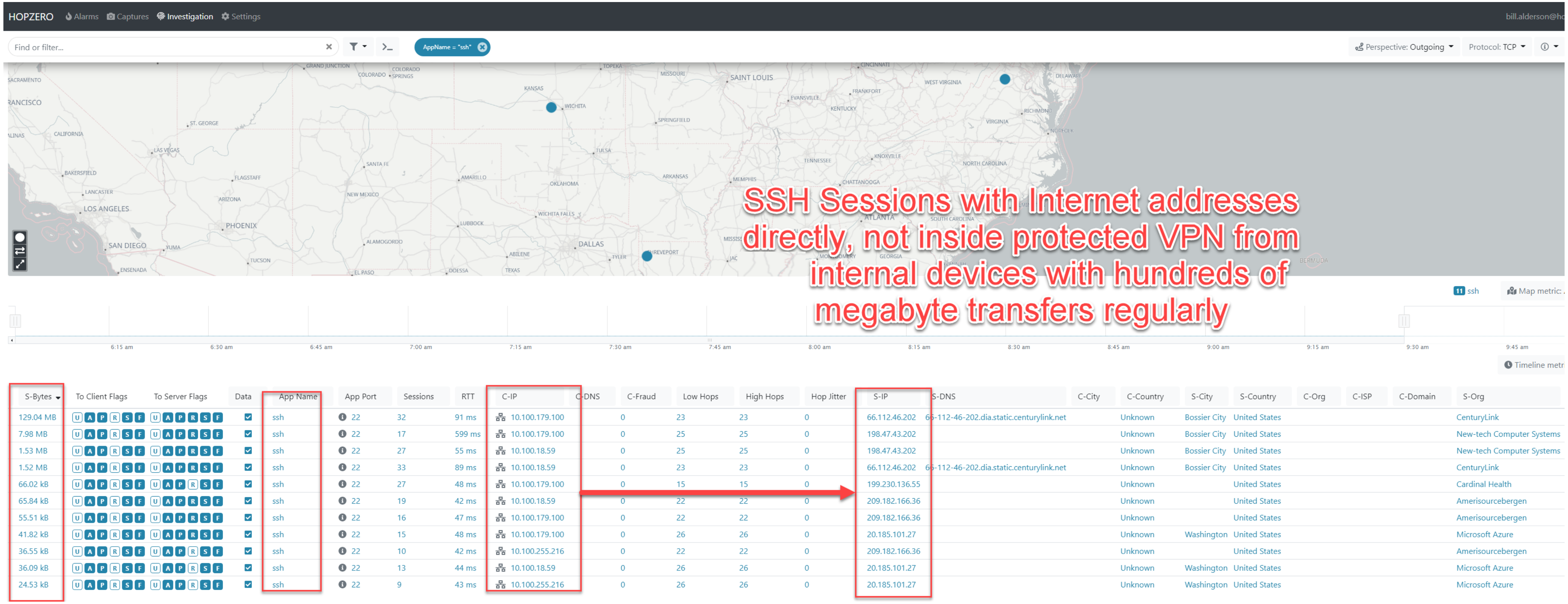
High volume of data retrieved from internet devices



significant (gigabytes) amount of information initiated and retrieved potentially from Internet devices from internal device 192.168.   11

S-Bytes	To Client Flags	To Server Flags	Data	App Name	App Port	Sessions	RTT	C-IP	C-DNS		C-Fraud	Low Hops	High Hops	Hop Jitter	S-IP	S-DNS	C-City		C-Country	S-City	S-Count
2.29 GB	U A P R S F	U A P R S F	□	http	80	10	512 ms	144. 38	vn ıet		45				192 11		Nuremberg		Germany		Unknown
11.68 GB	U A P R S F	U A P R S F	□	http	80	122	1.85 s	209. 110	d2 elus.net		0.01				192 11		Vancouver		Canada		Unknown
94.24 MB	U A P R S F	U A P R S F	□	https	443	19	103 ms	99 .111	server		0.01				192 11				United States		Unknown
4.18 GB	U A P R S F	U A P R S F	□	http	80	25	1.76 s	14 5.188	vmi33		45				192 77		Nuremberg		Germany		Unknown
1.07 kB	U A P R S F	U A P R S F	□	http	80	4	108 ms	45 28			0.01				10.1		Amsterdam		Netherlands		Unknown
1.03 kB	U A P R S F	U A P R S F	□	http	80	5	213 ms	11 54			45				192 11				China		Unknown
398 B	U A P R S F	U A P R S F	□	http	80	2	1.22 s	49 71			0.01				192 11		Changzhou		China		Unknown

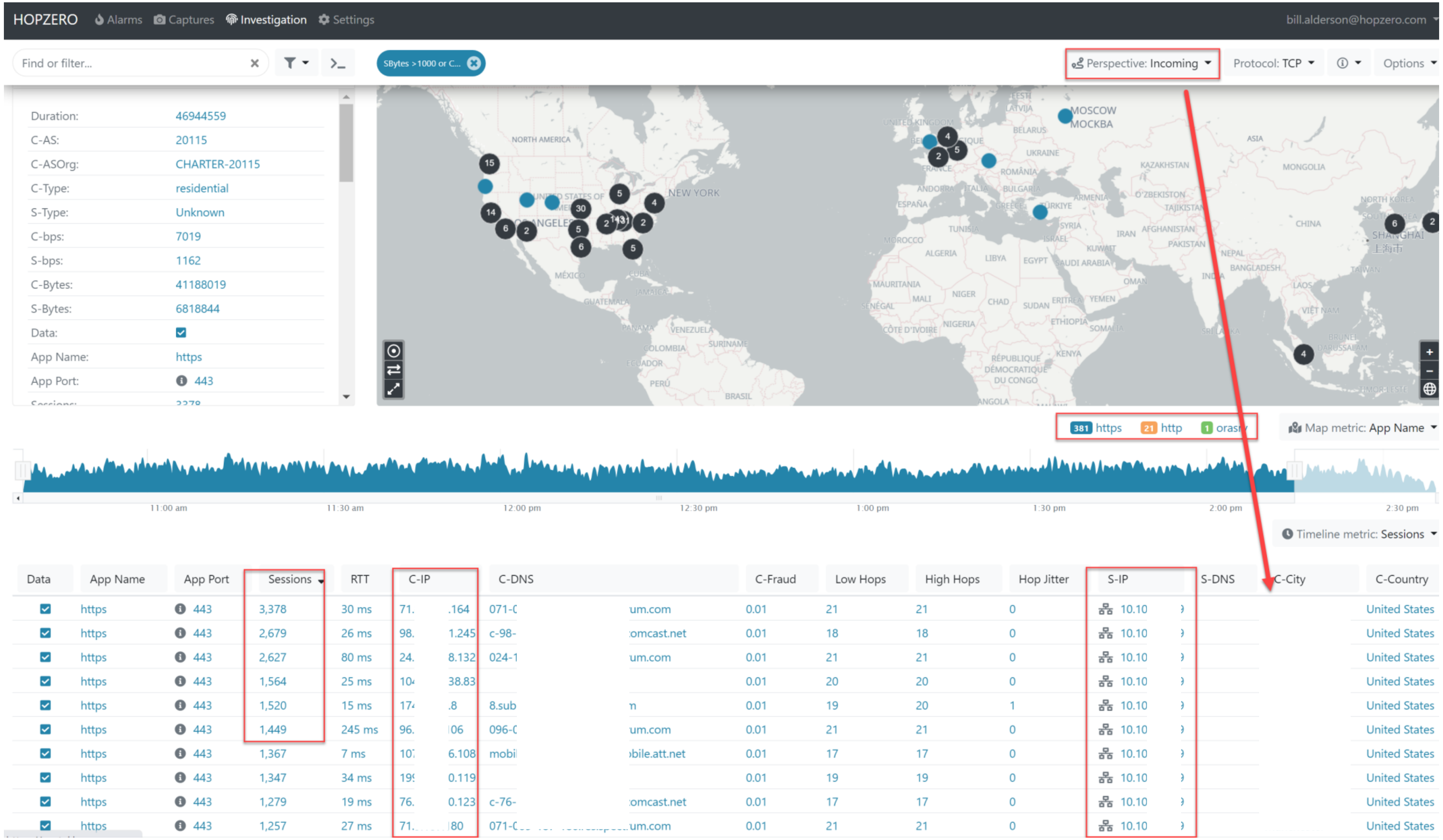
SSH sessions to internet devices outside vpn



SSH Sessions with Internet addresses directly, not inside protected VPN from internal devices with hundreds of megabyte transfers regularly

S-Bytes	To Client Flags	To Server Flags	Data	App Name	App Port	Sessions	RTT	C-IP	C-DNS	C-Fraud	Low Hops	High Hops	Hop Jitter	S-IP	S-DNS	C-City	C-Country	S-City	S-Country	C-Org	C-ISP	C-Domain	S-Org
129.04 MB	U A P R S F	U A P R S F	☑	ssh	22	32	91 ms	10.100.179.100		0	23	23	0	66.112.46.202	66-112-46-202.dia.static.centurylink.net		Unknown	Bossier City	United States				CenturyLink
7.98 MB	U A P R S F	U A P R S F	☑	ssh	22	17	599 ms	10.100.179.100		0	25	25	0	198.47.43.202			Unknown	Bossier City	United States				New-tech Computer Systems
1.53 MB	U A P R S F	U A P R S F	☑	ssh	22	27	55 ms	10.100.18.59		0	25	25	0	198.47.43.202			Unknown	Bossier City	United States				New-tech Computer Systems
1.52 MB	U A P R S F	U A P R S F	☑	ssh	22	33	89 ms	10.100.18.59		0	23	23	0	66.112.46.202	66-112-46-202.dia.static.centurylink.net		Unknown	Bossier City	United States				CenturyLink
66.02 kB	U A P R S F	U A P R S F	☑	ssh	22	27	48 ms	10.100.179.100		0	15	15	0	199.230.136.55			Unknown		United States				Cardinal Health
65.84 kB	U A P R S F	U A P R S F	☑	ssh	22	19	42 ms	10.100.18.59		0	22	22	0	209.182.166.36			Unknown		United States				Amerisourcebergen
55.51 kB	U A P R S F	U A P R S F	☑	ssh	22	16	47 ms	10.100.179.100		0	22	22	0	209.182.166.36			Unknown		United States				Amerisourcebergen
41.82 kB	U A P R S F	U A P R S F	☑	ssh	22	15	48 ms	10.100.179.100		0	26	26	0	20.185.101.27			Unknown	Washington	United States				Microsoft Azure
36.55 kB	U A P R S F	U A P R S F	☑	ssh	22	10	42 ms	10.100.255.216		0	22	22	0	209.182.166.36			Unknown		United States				Amerisourcebergen
36.09 kB	U A P R S F	U A P R S F	☑	ssh	22	13	44 ms	10.100.18.59		0	26	26	0	20.185.101.27			Unknown	Washington	United States				Microsoft Azure
24.53 kB	U A P R S F	U A P R S F	☑	ssh	22	9	43 ms	10.100.255.216		0	26	26	0	20.185.101.27			Unknown	Washington	United States				Microsoft Azure

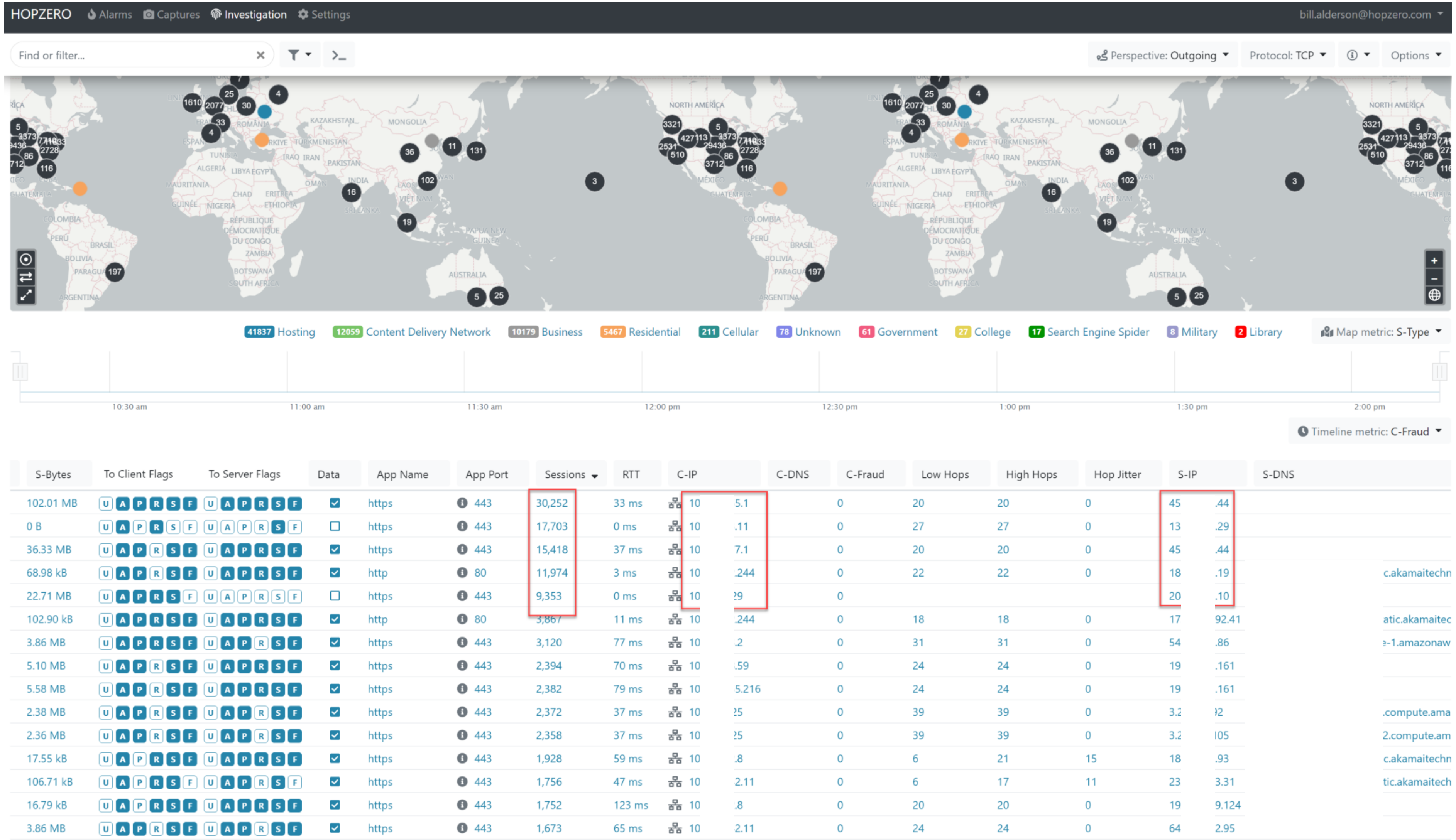
Thousands of incoming sessions passing through firewall



Duration:	46944559
C-AS:	20115
C-ASOrg:	CHARTER-20115
C-Type:	residential
S-Type:	Unknown
C-bps:	7019
S-bps:	1162
C-Bytes:	41188019
S-Bytes:	6818844
Data:	☑
App Name:	https
App Port:	443
Sessions:	3378

Data	App Name	App Port	Sessions	RTT	C-IP	C-DNS	C-Fraud	Low Hops	High Hops	Hop Jitter	S-IP	S-DNS	C-City	C-Country
☑	https	443	3,378	30 ms	71. .164	071-(um.com	0.01	21	21	0	10.10)			United States
☑	https	443	2,679	26 ms	98. 1.245	c-98- :omcast.net	0.01	18	18	0	10.10)			United States
☑	https	443	2,627	80 ms	24. 8.132	024-1 um.com	0.01	21	21	0	10.10)			United States
☑	https	443	1,564	25 ms	10 38.83		0.01	20	20	0	10.10)			United States
☑	https	443	1,520	15 ms	17 .8	8.sub n	0.01	19	20	1	10.10)			United States
☑	https	443	1,449	245 ms	96. 06	096-(um.com	0.01	21	21	0	10.10)			United States
☑	https	443	1,367	7 ms	10 6.108	mobi obile.att.net	0.01	17	17	0	10.10)			United States
☑	https	443	1,347	34 ms	19 0.119		0.01	19	19	0	10.10)			United States
☑	https	443	1,279	19 ms	76. 0.123	c-76- :omcast.net	0.01	17	17	0	10.10)			United States
☑	https	443	1,257	27 ms	71. 80	071-(um.com	0.01	21	21	0	10.10)			United States

10’s of Thousands of outgoing sessions



Perspective: Outgoing

Protocol: TCP

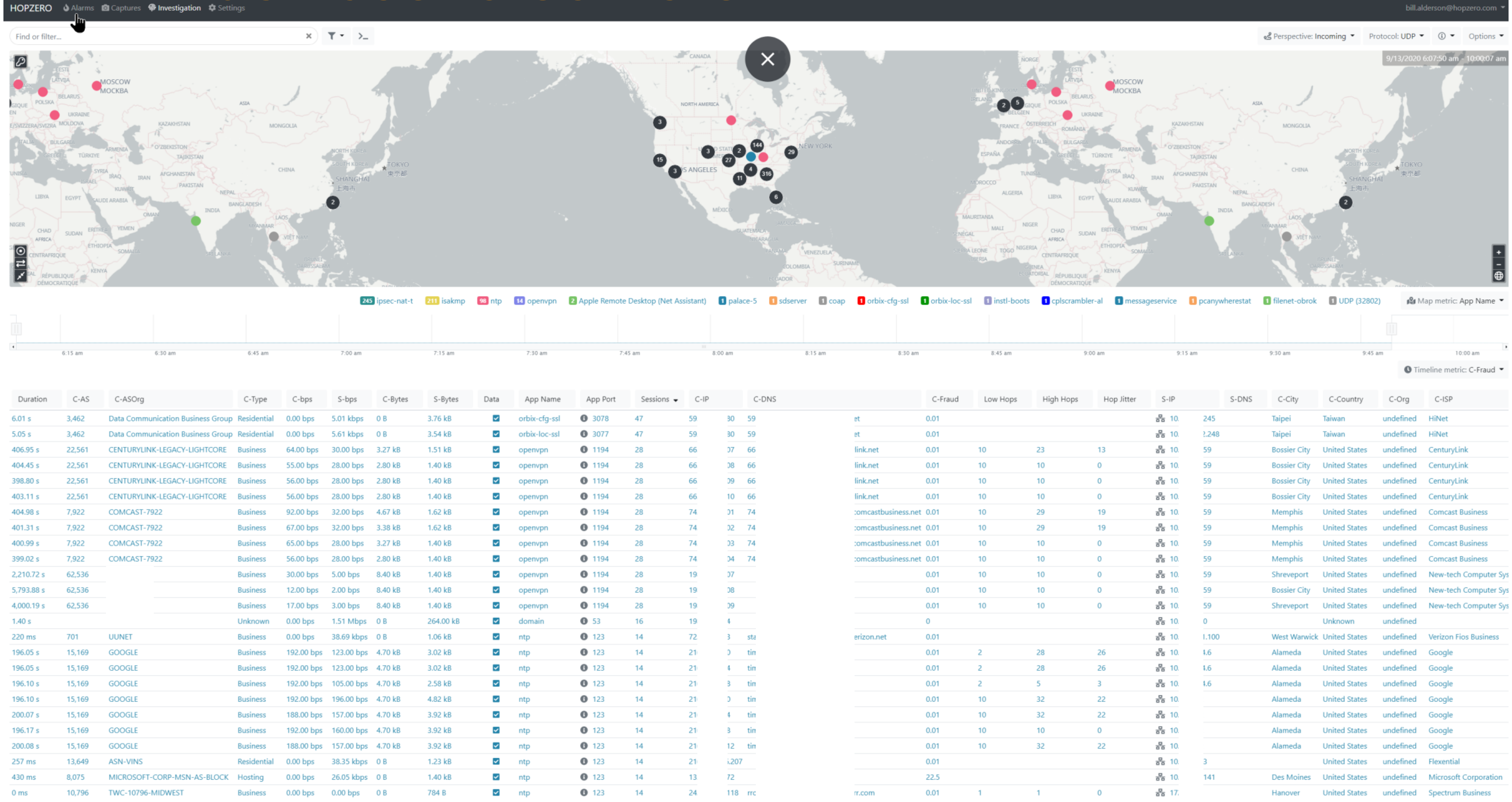
41837 Hosting · 12059 Content Delivery Network · 10179 Business · 5467 Residential · 211 Cellular · 78 Unknown · 61 Government · 27 College · 17 Search Engine Spider · 8 Military · 2 Library

Map metric: S-Type

Timeline metric: C-Fraud

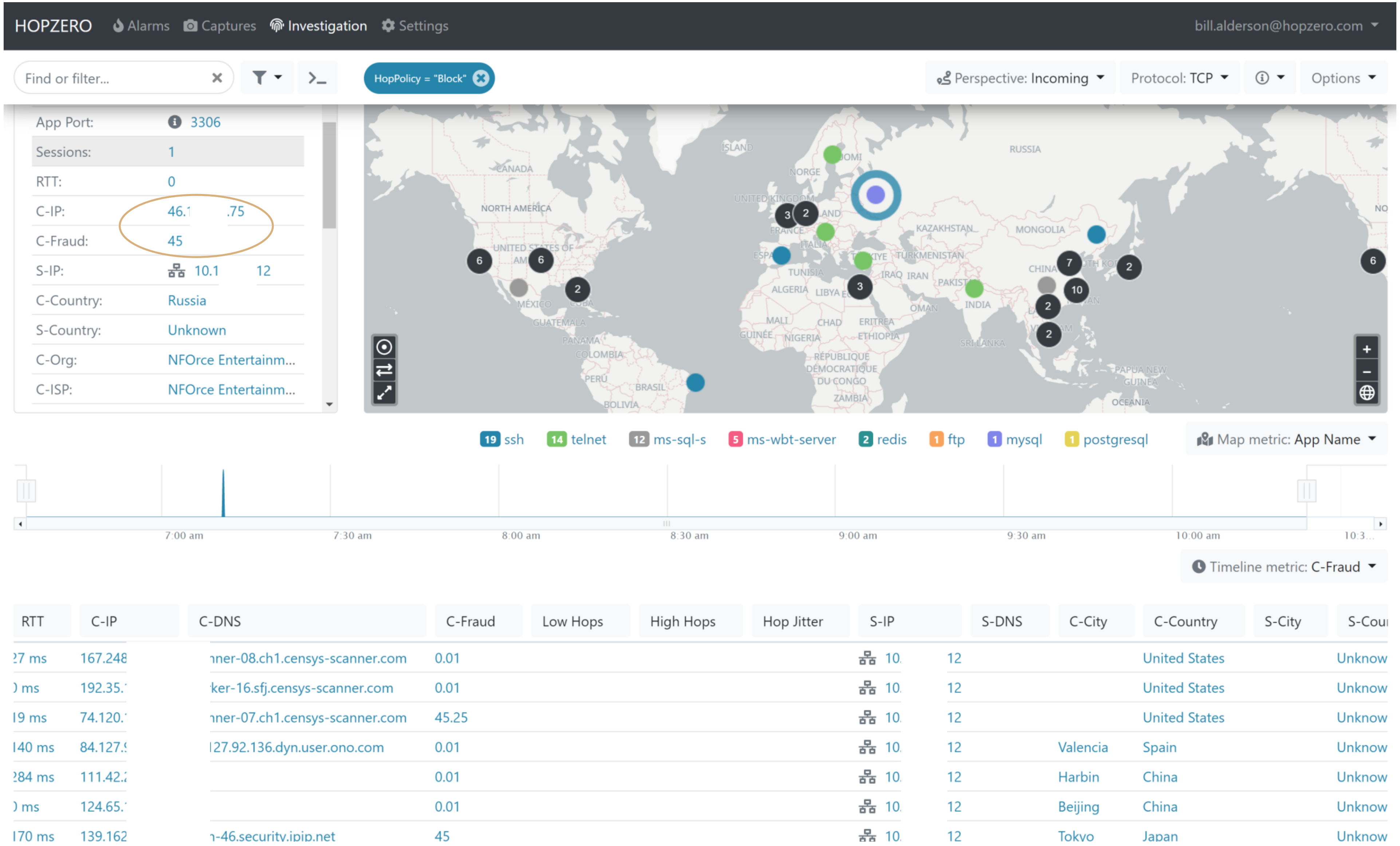
S-Bytes	To Client Flags	To Server Flags	Data	App Name	App Port	Sessions	RTT	C-IP	C-DNS	C-Fraud	Low Hops	High Hops	Hop Jitter	S-IP	S-DNS
102.01 MB	U A P R S F	U A P R S F	☑	https	443	30,252	33 ms	10 5.1		0	20	20	0	45 .44	
0 B	U A P R S F	U A P R S F	☐	https	443	17,703	0 ms	10 .11		0	27	27	0	13 .29	
36.33 MB	U A P R S F	U A P R S F	☑	https	443	15,418	37 ms	10 7.1		0	20	20	0	45 .44	
68.98 kB	U A P R S F	U A P R S F	☑	http	80	11,974	3 ms	10 .244		0	22	22	0	18 .19	c.akamaitechn
22.71 MB	U A P R S F	U A P R S F	☐	https	443	9,353	0 ms	10 29		0				20 .10	
102.90 kB	U A P R S F	U A P R S F	☑	http	80	3,867	11 ms	10 .244		0	18	18	0	17 92.41	atic.akamaitec
3.86 MB	U A P R S F	U A P R S F	☑	https	443	3,120	77 ms	10 .2		0	31	31	0	54 .86	e-1.amazonaw
5.10 MB	U A P R S F	U A P R S F	☑	https	443	2,394	70 ms	10 .59		0	24	24	0	19 .161	
5.58 MB	U A P R S F	U A P R S F	☑	https	443	2,382	79 ms	10 5.216		0	24	24	0	19 .161	
2.38 MB	U A P R S F	U A P R S F	☑	https	443	2,372	37 ms	10 25		0	39	39	0	3.2 92	.compute.ama
2.36 MB	U A P R S F	U A P R S F	☑	https	443	2,358	37 ms	10 25		0	39	39	0	3.2 105	2.compute.am
17.55 kB	U A P R S F	U A P R S F	☑	https	443	1,928	59 ms	10 .8		0	6	21	15	18 .93	c.akamaitechn
106.71 kB	U A P R S F	U A P R S F	☑	https	443	1,756	47 ms	10 2.11		0	6	17	11	23 3.31	tic.akamaitech
16.79 kB	U A P R S F	U A P R S F	☑	https	443	1,752	123 ms	10 .8		0	20	20	0	19 9.124	
3.86 MB	U A P R S F	U A P R S F	☑	https	443	1,673	65 ms	10 2.11		0	24	24	0	64 2.95	

Incoming suspicious sessions from internet devices to servers



Duration	C-AS	C-ASOrg	C-Type	C-bps	S-bps	C-Bytes	S-Bytes	Data	App Name	App Port	Sessions ▾	C-IP	C-DNS	C-Fraud	Low Hops	High Hops	Hop Jitter	S-IP	S-DNS	C-City	C-Country	C-Org	C-ISP
6.01 s	3,462	Data Communication Business Group	Residential	0.00 bps	5.01 kbps	0 B	3.76 kB	☑	orbix-cfg-ssl	3078	47	59. 30	59 et	0.01				10. 245		Taipei	Taiwan	undefined	HiNet
5.05 s	3,462	Data Communication Business Group	Residential	0.00 bps	5.61 kbps	0 B	3.54 kB	☑	orbix-loc-ssl	3077	47	59. 30	59 et	0.01				10. 2.248		Taipei	Taiwan	undefined	HiNet
406.95 s	22,561	CENTURYLINK-LEGACY-LIGHTCORE	Business	64.00 bps	30.00 bps	3.27 kB	1.51 kB	☑	openvpn	1194	28	66. 07	66 link.net	0.01	10	23	13	10. 59		Bossier City	United States	undefined	CenturyLink
404.45 s	22,561	CENTURYLINK-LEGACY-LIGHTCORE	Business	55.00 bps	28.00 bps	2.80 kB	1.40 kB	☑	openvpn	1194	28	66. 08	66 link.net	0.01	10	10	0	10. 59		Bossier City	United States	undefined	CenturyLink
398.80 s	22,561	CENTURYLINK-LEGACY-LIGHTCORE	Business	56.00 bps	28.00 bps	2.80 kB	1.40 kB	☑	openvpn	1194	28	66. 09	66 link.net	0.01	10	10	0	10. 59		Bossier City	United States	undefined	CenturyLink
403.11 s	22,561	CENTURYLINK-LEGACY-LIGHTCORE	Business	56.00 bps	28.00 bps	2.80 kB	1.40 kB	☑	openvpn	1194	28	66. 10	66 link.net	0.01	10	10	0	10. 59		Bossier City	United States	undefined	CenturyLink
404.98 s	7,922	COMCAST-7922	Business	92.00 bps	32.00 bps	4.67 kB	1.62 kB	☑	openvpn	1194	28	74. 01	74 comcastbusiness.net	0.01	10	29	19	10. 59		Memphis	United States	undefined	Comcast Business
401.31 s	7,922	COMCAST-7922	Business	67.00 bps	32.00 bps	3.38 kB	1.62 kB	☑	openvpn	1194	28	74. 02	74 comcastbusiness.net	0.01	10	29	19	10. 59		Memphis	United States	undefined	Comcast Business
400.99 s	7,922	COMCAST-7922	Business	65.00 bps	28.00 bps	3.27 kB	1.40 kB	☑	openvpn	1194	28	74. 03	74 comcastbusiness.net	0.01	10	10	0	10. 59		Memphis	United States	undefined	Comcast Business
399.02 s	7,922	COMCAST-7922	Business	56.00 bps	28.00 bps	2.80 kB	1.40 kB	☑	openvpn	1194	28	74. 04	74 comcastbusiness.net	0.01	10	10	0	10. 59		Memphis	United States	undefined	Comcast Business
2,210.72 s	62,536		Business	30.00 bps	5.00 bps	8.40 kB	1.40 kB	☑	openvpn	1194	28	19 07		0.01	10	10	0	10. 59		Shreveport	United States	undefined	New-tech Computer Sys
5,793.88 s	62,536		Business	12.00 bps	2.00 bps	8.40 kB	1.40 kB	☑	openvpn	1194	28	19 08		0.01	10	10	0	10. 59		Bossier City	United States	undefined	New-tech Computer Sys
4,000.19 s	62,536		Business	17.00 bps	3.00 bps	8.40 kB	1.40 kB	☑	openvpn	1194	28	19 09		0.01	10	10	0	10. 59		Shreveport	United States	undefined	New-tech Computer Sys
1.40 s			Unknown	0.00 bps	1.51 Mbps	0 B	264.00 kB	☑	domain	53	16	19 4		0				10. 0			Unknown	undefined	
220 ms	701	UUNET	Business	0.00 bps	38.69 kbps	0 B	1.06 kB	☑	ntp	123	14	72. 3	sta erizon.net	0.01				10. 1.100		West Warwick	United States	undefined	Verizon Fios Business
196.05 s	15,169	GOOGLE	Business	192.00 bps	123.00 bps	4.70 kB	3.02 kB	☑	ntp	123	14	21 0	tin	0.01	2	28	26	10. 4.6		Alameda	United States	undefined	Google
196.05 s	15,169	GOOGLE	Business	192.00 bps	123.00 bps	4.70 kB	3.02 kB	☑	ntp	123	14	21 4	tin	0.01	2	28	26	10. 4.6		Alameda	United States	undefined	Google
196.10 s	15,169	GOOGLE	Business	192.00 bps	105.00 bps	4.70 kB	2.58 kB	☑	ntp	123	14	21 3	tin	0.01	2	5	3	10. 4.6		Alameda	United States	undefined	Google
196.10 s	15,169	GOOGLE	Business	192.00 bps	196.00 bps	4.70 kB	4.82 kB	☑	ntp	123	14	21 0	tin	0.01	10	32	22	10.		Alameda	United States	undefined	Google
200.07 s	15,169	GOOGLE	Business	188.00 bps	157.00 bps	4.70 kB	3.92 kB	☑	ntp	123	14	21 4	tin	0.01	10	32	22	10.		Alameda	United States	undefined	Google
196.17 s	15,169	GOOGLE	Business	192.00 bps	160.00 bps	4.70 kB	3.92 kB	☑	ntp	123	14	21 3	tin	0.01	10	10	0	10.		Alameda	United States	undefined	Google
200.08 s	15,169	GOOGLE	Business	188.00 bps	157.00 bps	4.70 kB	3.92 kB	☑	ntp	123	14	21 12	tin	0.01	10	32	22	10.		Alameda	United States	undefined	Google
257 ms	13,649	ASN-VINS	Residential	0.00 bps	38.35 kbps	0 B	1.23 kB	☑	ntp	123	14	21 .207		0.01				10. 3			United States	undefined	Flexential
430 ms	8,075	MICROSOFT-CORP-MSN-AS-BLOCK	Hosting	0.00 bps	26.05 kbps	0 B	1.40 kB	☑	ntp	123	14	13. 72		22.5				10. 141		Des Moines	United States	undefined	Microsoft Corporation
0 ms	10,796	TWC-10796-MIDWEST	Business	0.00 bps	0.00 bps	0 B	784 B	☑	ntp	123	14	24. 118	rrc rr.com	0.01	1	1	0	17.		Hanover	United States	undefined	Spectrum Business

Incoming sessions passing firewall from high fraud intl. internet scanners



HOPZERO   Alarms   Captures   Investigation   Settings   bill.alderson@hopzero.com

Find or filter...   HopPolicy = "Block"   Perspective: Incoming   Protocol: TCP   Options

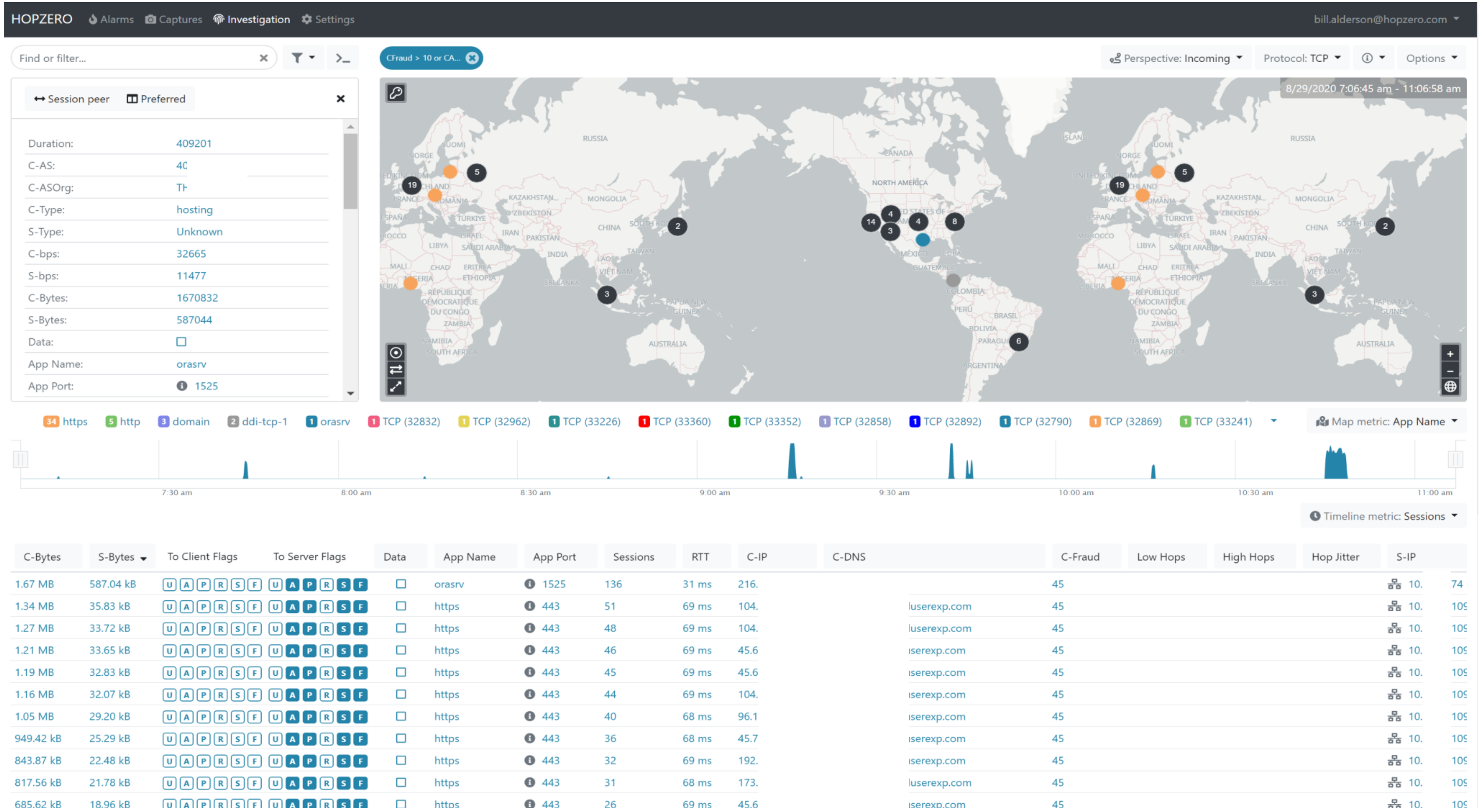
App Port:	3306
Sessions:	1
RTT:	0
C-IP:	46.1 .75
C-Fraud:	45
S-IP:	10.1 12
C-Country:	Russia
S-Country:	Unknown
C-Org:	NFOrce Entertainm...
C-ISP:	NFOrce Entertainm...

19 ssh   14 telnet   12 ms-sql-s   5 ms-wbt-server   2 redis   1 ftp   1 mysql   1 postgresql   Map metric: App Name

Timeline metric: C-Fraud

RTT	C-IP	C-DNS	C-Fraud	Low Hops	High Hops	Hop Jitter	S-IP	S-DNS	C-City	C-Country	S-City	S-Cou
27 ms	167.248	nner-08.ch1.censys-scanner.com	0.01				10. 12			United States		Unknow
) ms	192.35.	ker-16.sfj.censys-scanner.com	0.01				10. 12			United States		Unknow
19 ms	74.120.	nner-07.ch1.censys-scanner.com	45.25				10. 12			United States		Unknow
140 ms	84.127.	127.92.136.dyn.user.ono.com	0.01				10. 12		Valencia	Spain		Unknow
284 ms	111.42.		0.01				10. 12		Harbin	China		Unknow
) ms	124.65.		0.01				10. 12		Beijing	China		Unknow
170 ms	139.162	1-46.security.ipip.net	45				10. 12		Tokyo	Japan		Unknow

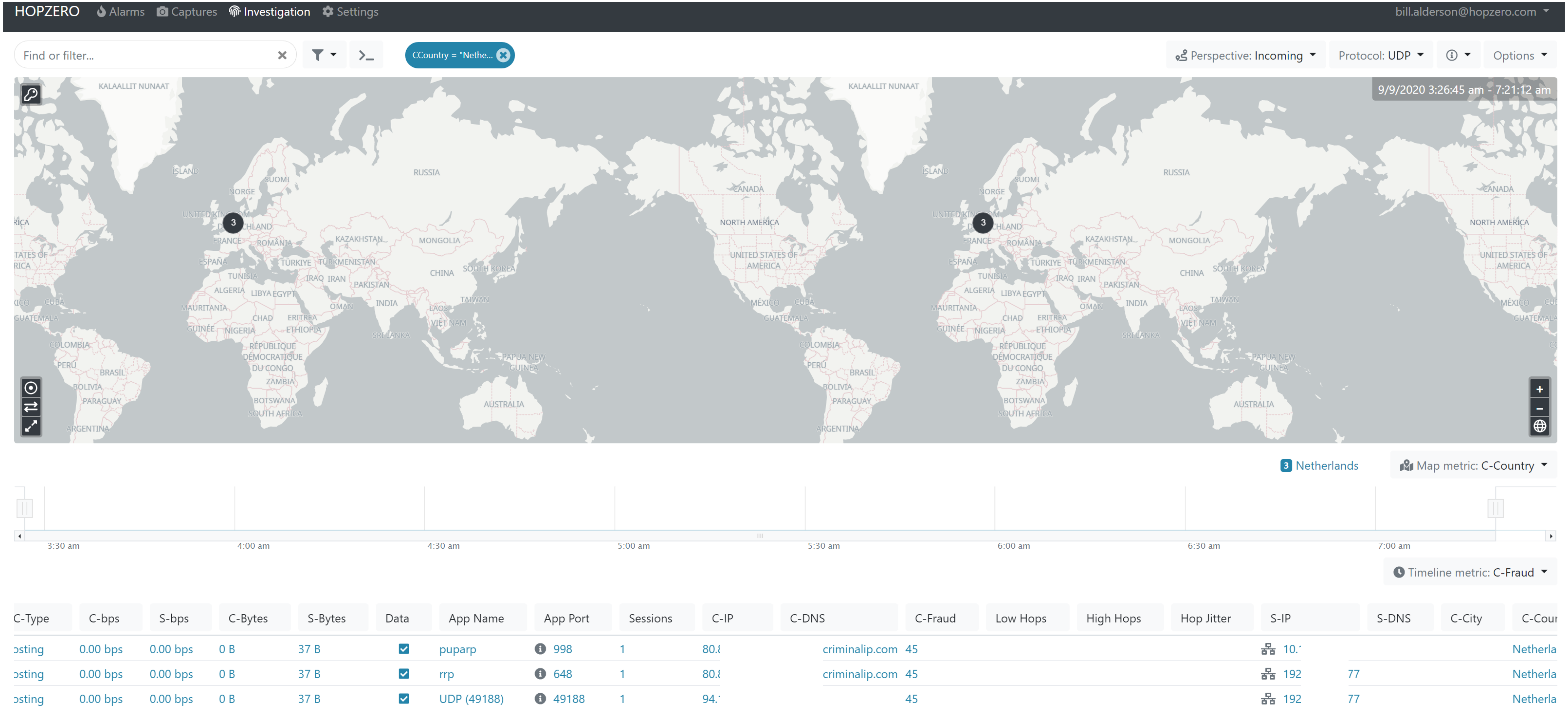
Incoming sessions with data from 45 fraud score sources



Duration:	409201
C-AS:	4C
C-ASOrg:	TH
C-Type:	hosting
S-Type:	Unknown
C-bps:	32665
S-bps:	11477
C-Bytes:	1670832
S-Bytes:	587044
Data:	□
App Name:	orasrv
App Port:	1525

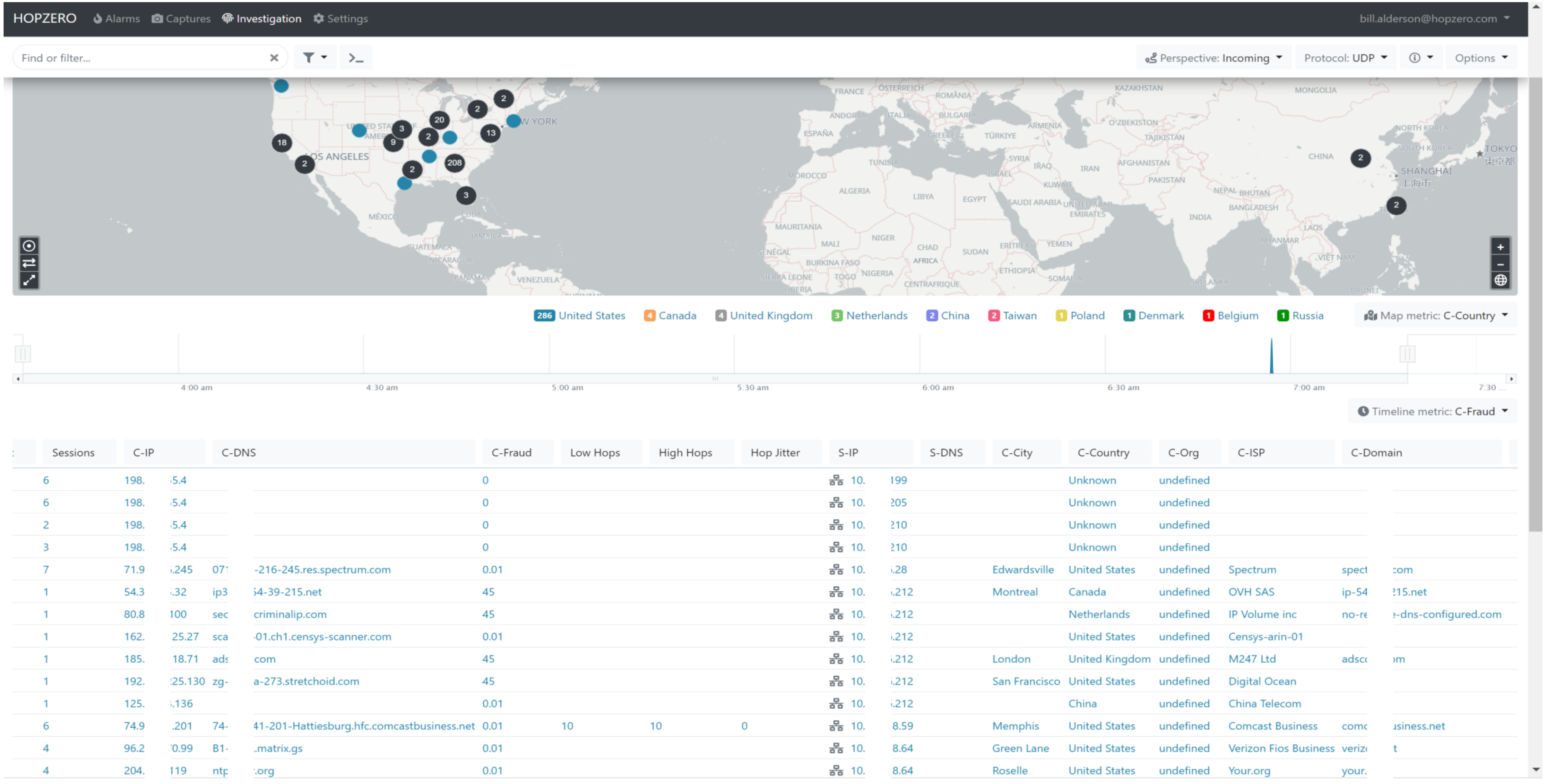
C-Bytes	S-Bytes	To Client Flags	To Server Flags	Data	App Name	App Port	Sessions	RTT	C-IP	C-DNS	C-Fraud	Low Hops	High Hops	Hop Jitter	S-IP	
1.67 MB	587.04 kB	U A P R S F	U A P R S F	□	orasrv	1525	136	31 ms	216.		45				10.	74
1.34 MB	35.83 kB	U A P R S F	U A P R S F	□	https	443	51	69 ms	104.	luserexp.com	45				10.	10
1.27 MB	33.72 kB	U A P R S F	U A P R S F	□	https	443	48	69 ms	104.	luserexp.com	45				10.	10
1.21 MB	33.65 kB	U A P R S F	U A P R S F	□	https	443	46	69 ms	45.6	iserexp.com	45				10.	10
1.19 MB	32.83 kB	U A P R S F	U A P R S F	□	https	443	45	69 ms	45.6	iserexp.com	45				10.	10
1.16 MB	32.07 kB	U A P R S F	U A P R S F	□	https	443	44	69 ms	104.	iserexp.com	45				10.	10
1.05 MB	29.20 kB	U A P R S F	U A P R S F	□	https	443	40	68 ms	96.1	iserexp.com	45				10.	10
949.42 kB	25.29 kB	U A P R S F	U A P R S F	□	https	443	36	68 ms	45.7	iserexp.com	45				10.	10
843.87 kB	22.48 kB	U A P R S F	U A P R S F	□	https	443	32	69 ms	192.	iserexp.com	45				10.	10
817.56 kB	21.78 kB	U A P R S F	U A P R S F	□	https	443	31	68 ms	173.	luserexp.com	45				10.	10
685.62 kB	18.96 kB	U A P R S F	U A P R S F	□	https	443	26	69 ms	45.6	iserexp.com	45				10.	10

Incoming self identifying as criminal “attempts”



C-Type	C-bps	S-bps	C-Bytes	S-Bytes	Data	App Name	App Port	Sessions	C-IP	C-DNS	C-Fraud	Low Hops	High Hops	Hop Jitter	S-IP	S-DNS	C-City	C-Cour
osting	0.00 bps	0.00 bps	0 B	37 B	☑	puparp	998	1	80.8	criminalip.com	45				10.1			Netherla
osting	0.00 bps	0.00 bps	0 B	37 B	☑	rrp	648	1	80.8	criminalip.com	45				192	77		Netherla
osting	0.00 bps	0.00 bps	0 B	37 B	☑	UDP (49188)	49188	1	94.1		45				192	77		Netherla

2nd Incoming self identifying as criminal "attempts"



Sessions	C-IP	C-DNS	C-Fraud	Low Hops	High Hops	Hop Jitter	S-IP	S-DNS	C-City	C-Country	C-Org	C-ISP	C-Domain
6	198. 5.4		0				10. 199			Unknown	undefined		
6	198. 5.4		0				10. 205			Unknown	undefined		
2	198. 5.4		0				10. 210			Unknown	undefined		
3	198. 5.4		0				10. 210			Unknown	undefined		
7	71.9 .245	07 -216-245.res.spectrum.com	0.01				10. .28		Edwardsville	United States	undefined	Spectrum	spect com
1	54.3 .32	ip3 54-39-215.net	45				10. .212		Montreal	Canada	undefined	OVH SAS	ip-54 215.net
1	80.8 100	sec criminalip.com	45				10. .212			Netherlands	undefined	IP Volume inc	no-re e-dns-configured.com
1	162. 25.27	sca 01.ch1.censys-scanner.com	0.01				10. .212			United States	undefined	Censys-arin-01	
1	185. 18.71	ads com	45				10. .212		London	United Kingdom	undefined	M247 Ltd	adsc om
1	192. 25.130	zg- a-273.stretchoid.com	45				10. .212		San Francisco	United States	undefined	Digital Ocean	
1	125. .136		0.01				10. .212			China	undefined	China Telecom	
6	74.9 .201	74- 41-201-Hattiesburg.hfc.comcastbusiness.net	0.01	10	10	0	10. 8.59		Memphis	United States	undefined	Comcast Business	comc usiness.net
4	96.2 0.99	B1- .matrix.gs	0.01				10. 8.64		Green Lane	United States	undefined	Verizon Fios Business	veriz t
4	204. 119	ntp .org	0.01				10. 8.64		Roselle	United States	undefined	Your.org	your.