



Mapping Digital Supply Chain Relationships

Benjamin Edwards, PhD

Principal Research Scientist, Bitsight

May 13, 2025

BITSIGHT

BITSIGHT

©2025, BitSight Technologies, Inc. and its affiliates ("Bitsight"). BITSIGHT® is a registered trademark of Bitsight. All rights reserved.

Who am I?

Security Data Nerd who derives insight from vast stores of cyber data.

Formerly IBM Research, Cyentia Institute

Currently Bitsight

Why are we here today?

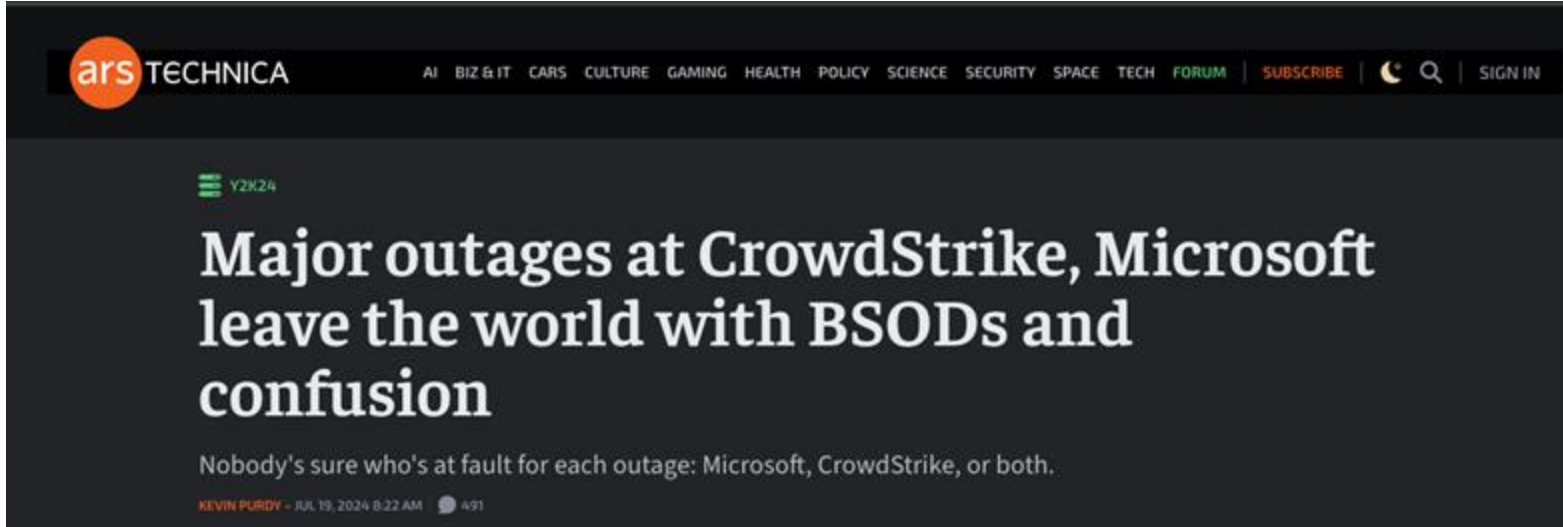
To better understand cyber risks to enterprise generally and the financial sector specifically.

Vulnerability management
Cyber threat intelligence
Supply chain risks



Risky on stage selfie at RSAC 2023

Supply chain incidents abound



Supply chain incidents abound

BLOG

The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years

Released: May 07, 2023

Jen Easterly, CISA Director

Tom Fanning, Chairman and CEO of Southern Company and Chair of [CISA's Cybersecurity Advisory Committee](#)

Supply chain incidents abound

BLOG

TI
Le
Ye

Rele

Jen

Tom

February 8, 2024

Okta October 2023 Security Incident Investigation Closure



David Bradbury

Related Posts: [Recommended Actions](#) - Nov 29, 2023 / [Root Cause Analysis \[RCA\]](#) - Nov 3, 2023 / [Security Incident](#) - Oct 20, 2023

Supply chain incidents abound

BLOG

TI
Le
Ye

Rele

Jen

Tom

CYBERCRIME

SolarWinds Likely Hacked at Least One Year Before Breach Discovery

An analysis of the infrastructure and the malware involved in the [attack targeting SolarWinds](#) indicates that the Texas-based IT management and monitoring company was hacked at least one year prior to the discovery of the breach.



By [Edward Kovacs](#)
December 18, 2020



An analysis of the infrastructure and the malware involved in the attack targeting SolarWinds indicates that the Texas-based IT management and monitoring company was hacked at least one year prior to the discovery of the breach.

SolarWinds has confirmed that sophisticated cyberespionage, which are believed to be

TRENDING

1 China Admitted to Volt Typhoon Cyberattacks on US Critical Infrastructure: Report

How big are supply chains and what do they look like?

Which providers are critical to individual and aggregate supply chains?

What is the security posture of critical providers in the supply chain?



How do we construct supply chain data?

Detecting product use via scanning

Careful, continuous scans of the Internet

Groma Internet Scanning Platform

40M+ monitored organizations

~2.7B hostnames

4.9B routable IP addresses

Not all products are visible!

Non Network Accessible

Client Side Software

Detectable without interference

Can also do security assessments

Vulnerabilities

Exposed Services

Microsoft Products Global Footprint



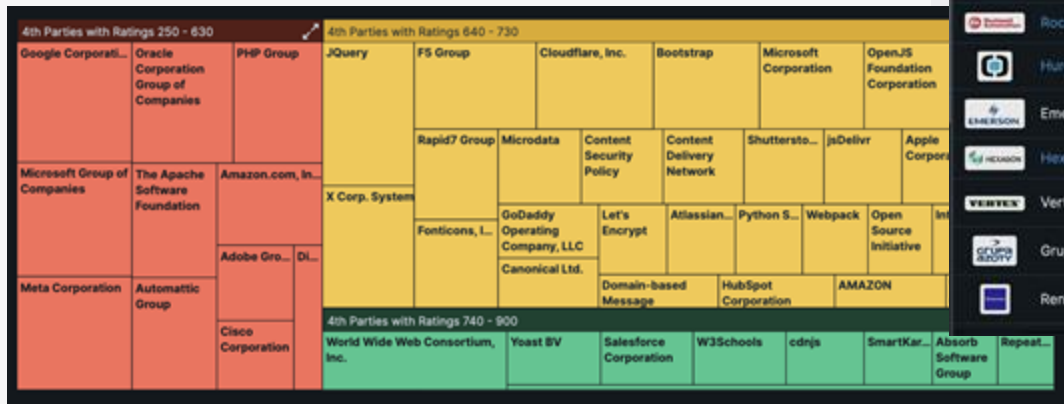
Detecting product use 4th party data

Multiple sources

Specific product usage

Product classification

Expanded set of providers and services



251 Rows				
Service Provider		Trend	Rating	Industry
FedEx Group			700	Transportation
Apache Corporation	Subscribe		620	Energy/Resources
Deutsche Bahn Group			530	Transportation
Siemens AG			510	Manufacturing
Samsung Electronics Group			600	Manufacturing
Tiny	Subscribe		740	Manufacturing
Koch Industries Corporation			570	Energy/Resources
Rockwell Automation Corporation			670	Manufacturing
Hurco Companies, Inc. Corporation			670	Manufacturing
Emerson Electric Corporation	Subscribe		720	Manufacturing
Hexagon Group			570	Engineering
Vertex Environmental Services	Subscribe		660	Engineering
Grupa Azoty Group	Subscribe		680	Manufacturing
Renesas Electronics Corporation.	Subscribe		700	Manufacturing

Building supply chain data

Identify relationships between organizations based on product or service usage.

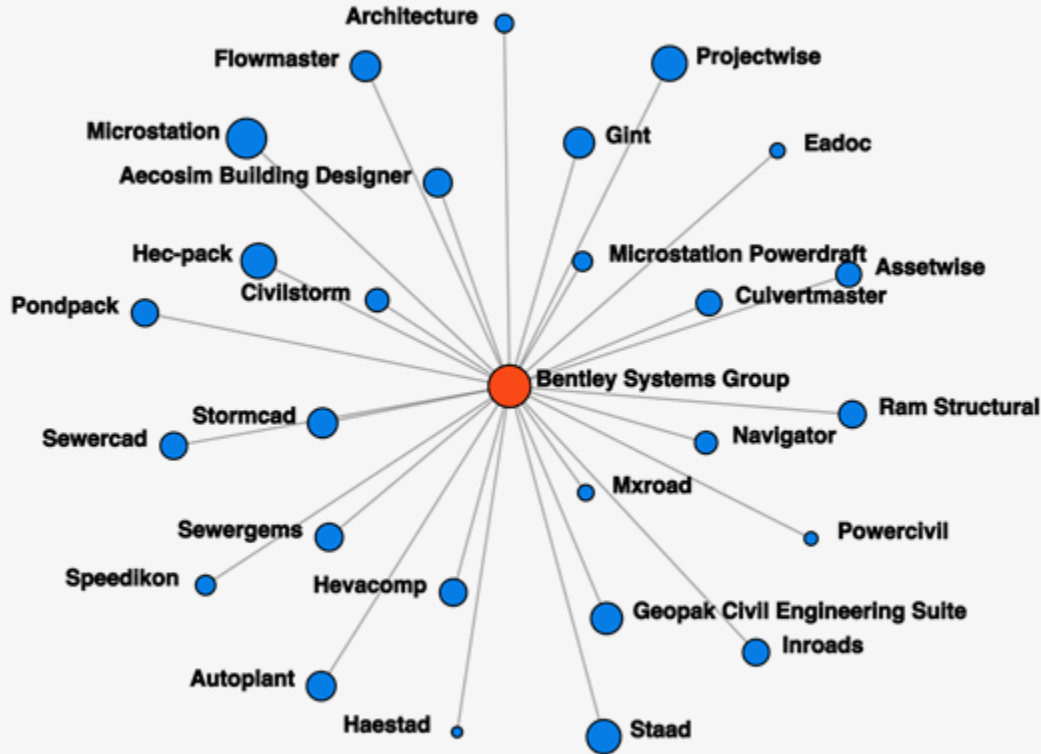
Use Bitsight scanning data as well as 3rd party data

Example

Bentley Systems (Orange circles)
American Based Infrastructure software company, Civil engineering and architectural design software

27 Products (Blue Dots)

Sized by number of consumers



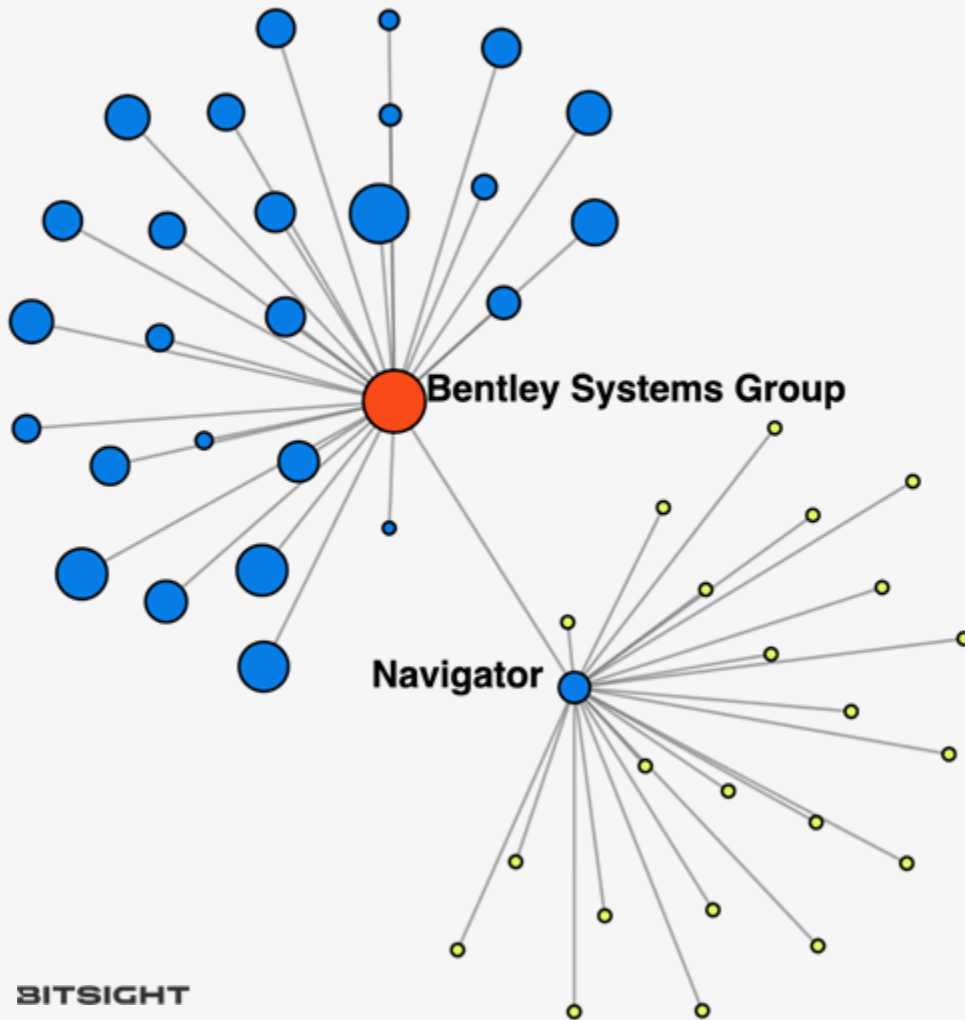
Measuring the supply chain

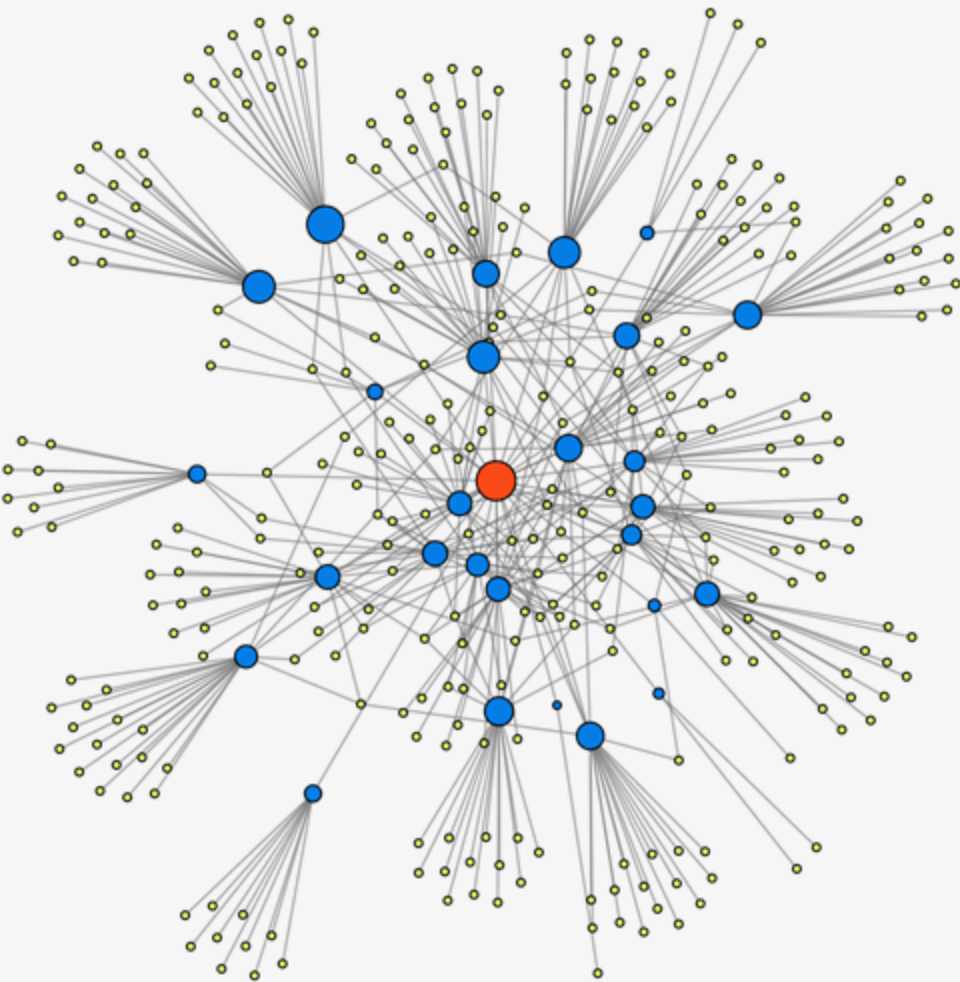
Bentley Systems (Orange circles)
American Based Infrastructure software company

27 Products (Blue Circles)

Sized by number of consumers

Navigator has 23 consumers (yellow circles)





Measuring the supply chain

Bentley Systems (Orange circles)
American Based Infrastructure software company

27 Products (Blue Circles)

Sized by number of consumers

Navigator has 23 consumers (yellow circles)

All products 2634 consumers (visually sampled to max of 20 per product)

Measuring the supply chain

Bentley Systems (Orange circles)
American Based Infrastructure software company

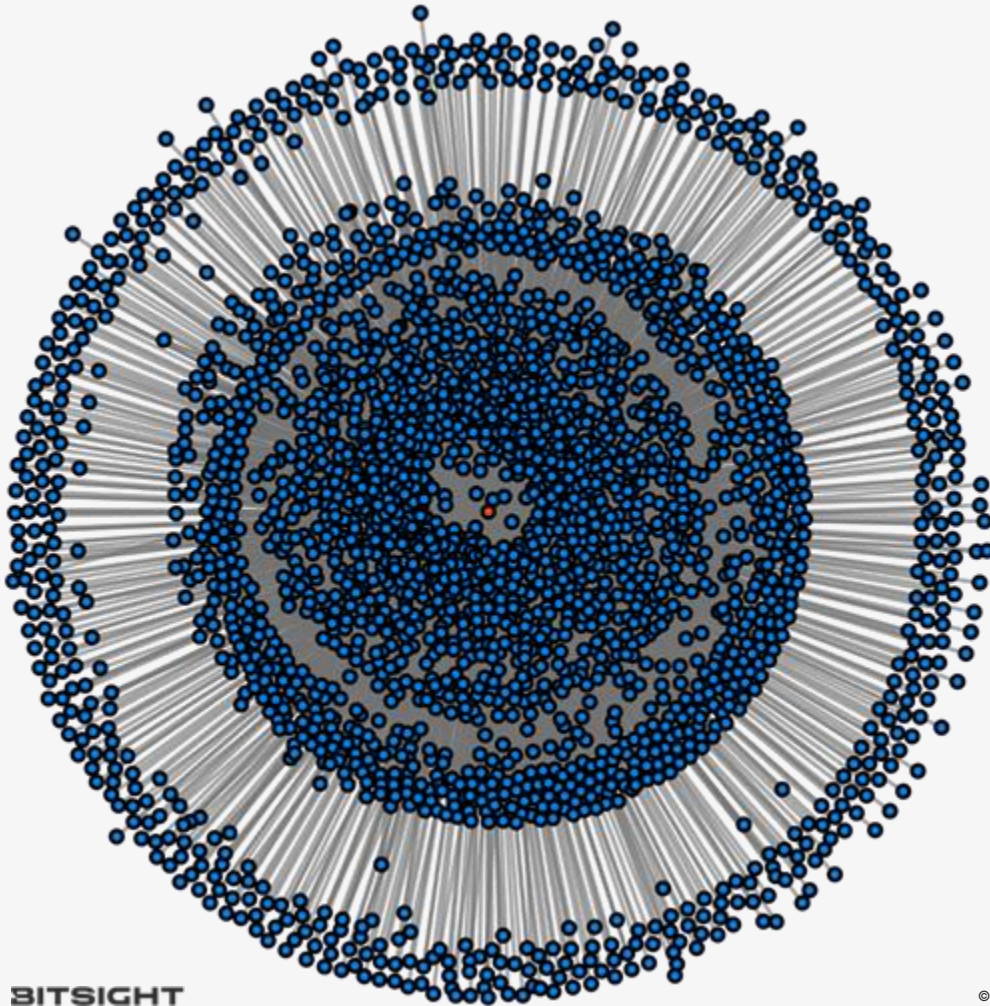
27 Products (Blue Circles)

Sized by number of consumers

Navigator has 23 consumers (yellow circles)

All products 2634 consumers

All connections between consumers



Understanding the global digital supply chain

Data

- 61M connections between
- 42k products
- 528M consumers
- 12k providers

Measuring the Global Supply Chain

- Calibrating supply chain size
- Consumers vs Providers

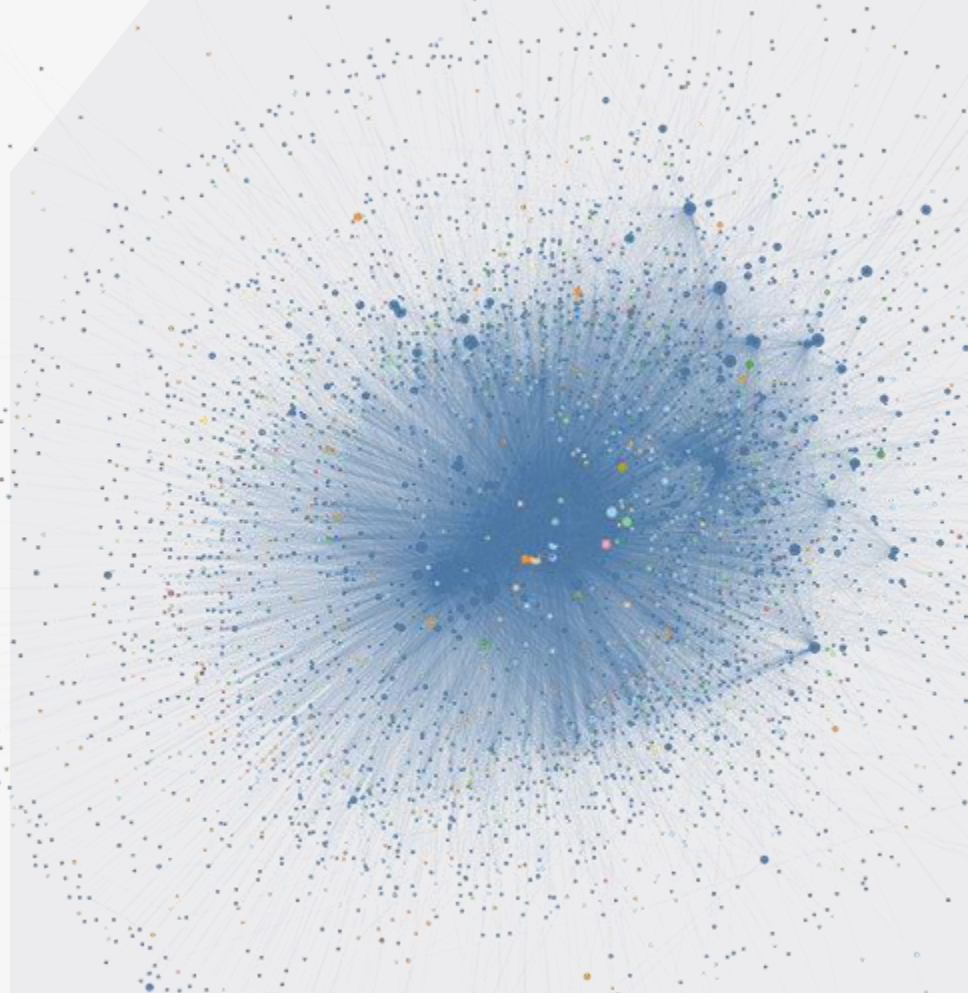
The Critical 99 and Hidden Pillars

- Measuring criticality is not so simple
- Industry specific Criticality

Cyber Risk in the global supply chain

- Geopolitical Risk
- Security Risk

Conclusions and recommendations

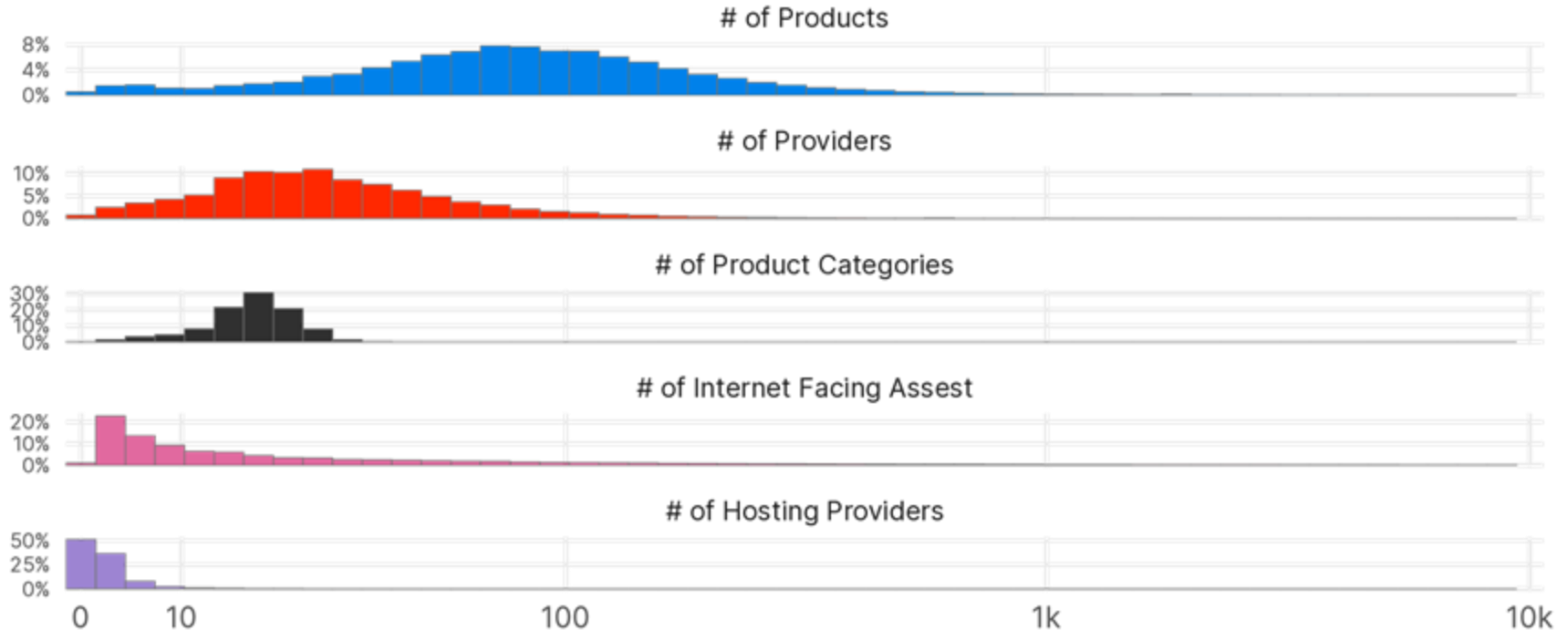




Measuring the Global Supply Chain

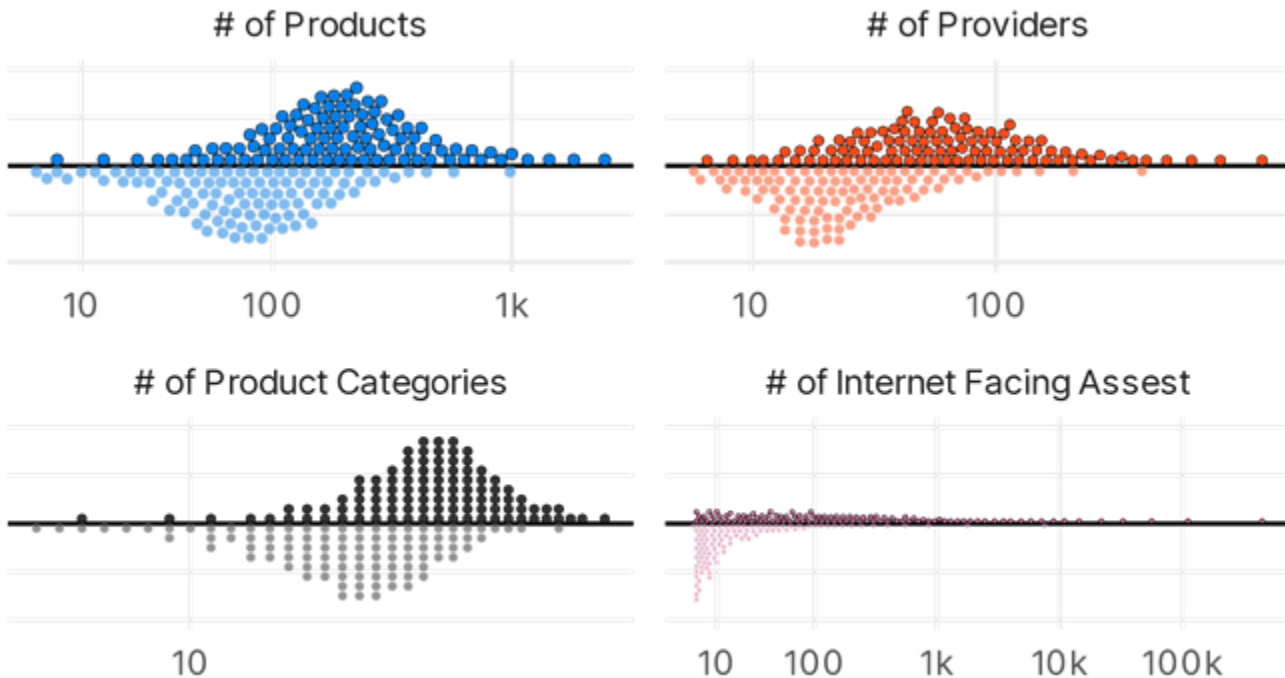
Supply chain size varies... a lot

Distribution of supply chain size measures



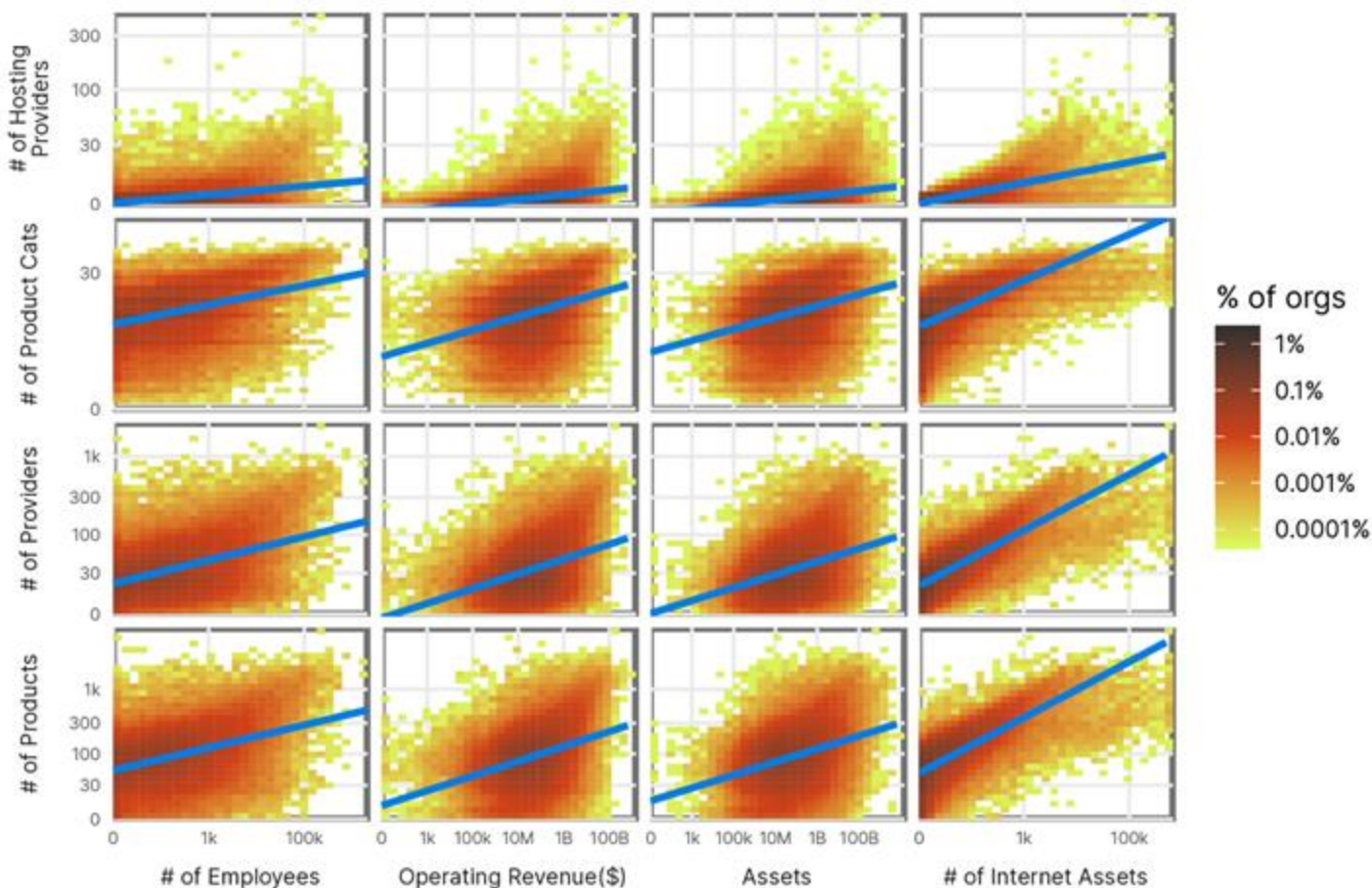
Suppliers have larger supply chains by 2.5x

Distribution of supply chain size measures

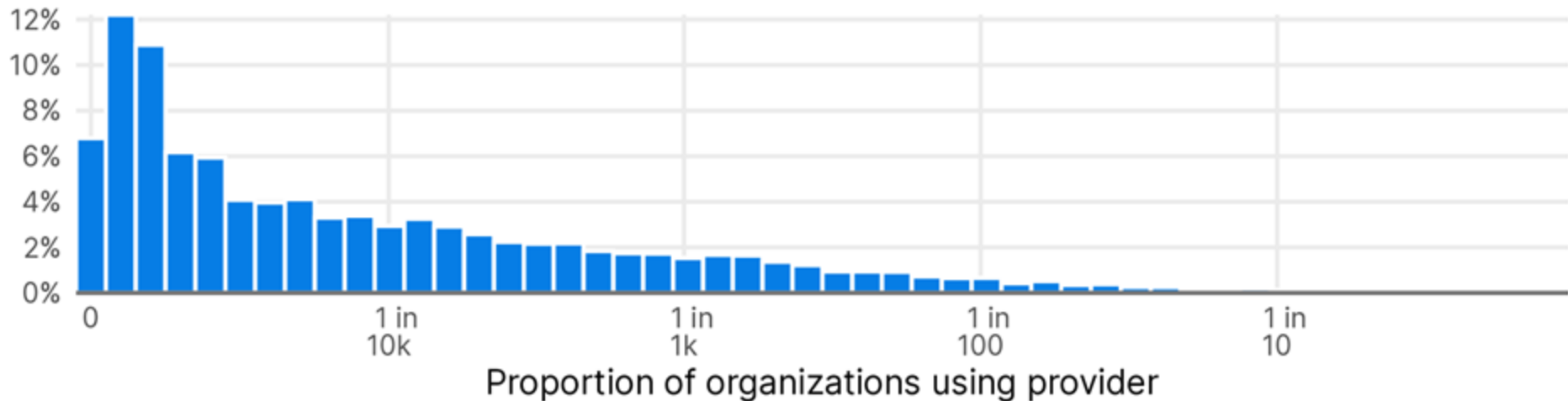


● Consumer ● Provider

Supply chain size varies... a lot



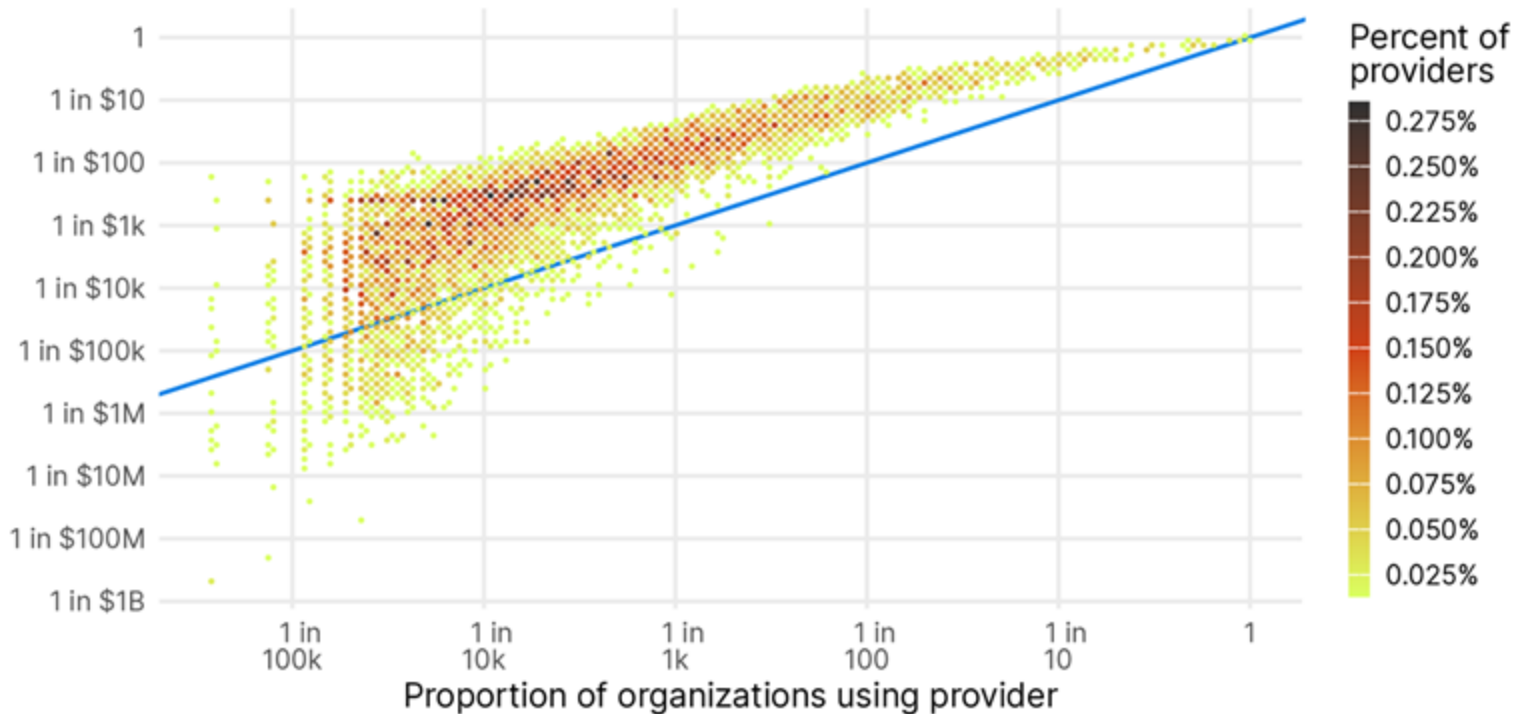
an others



Measuring the importance of a provider is not necessarily a simple task

Some providers are more important than others

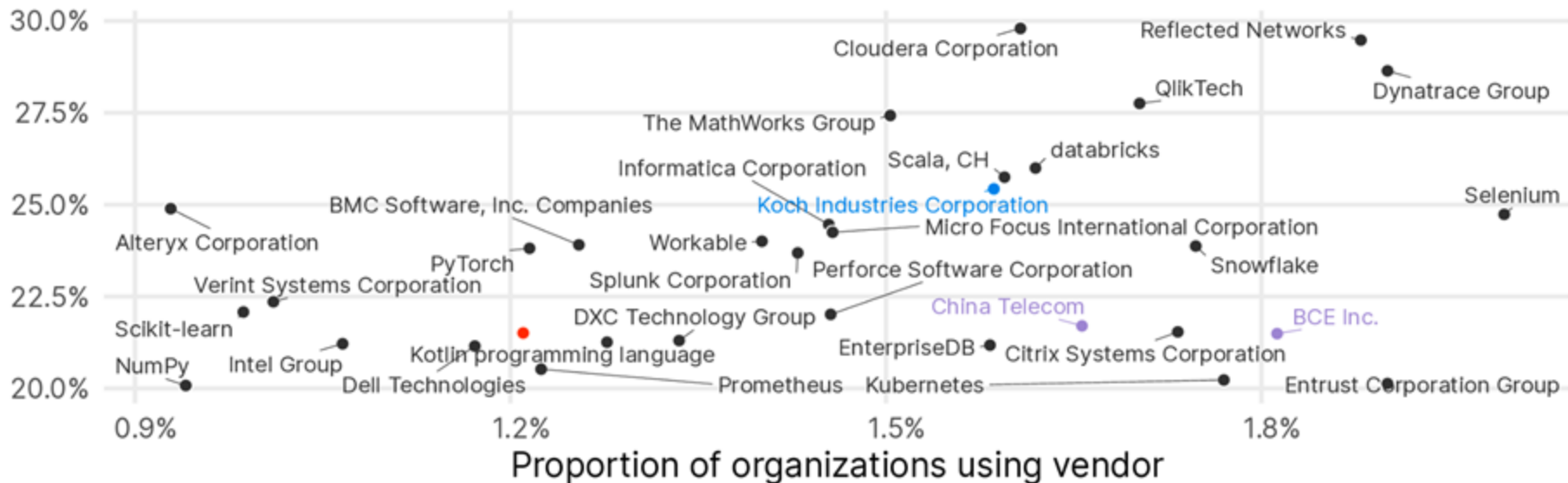
Proportion of organizations using provider by total revenue



Measuring the importance of a provider is not necessarily a simple task

Some providers are more important than others

Percentage of organizations using provider by total revenue



● Energy/Resources ● Manufacturing ● Technology ● Telecommunications

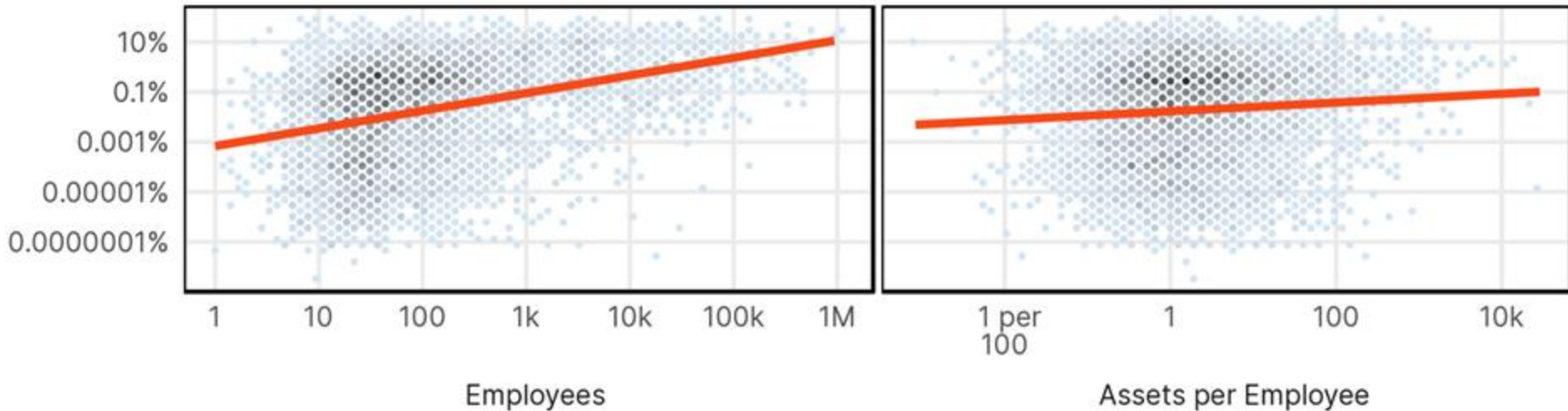
The "Critical 99"

Provider Rank by Market Share

1	JQuery 98.0%	34	Akamai Technologies Corporation 58.0%	67	Hurco Companies, Inc. Corporation 43.3%
2	Microsoft 96.6%	35	Microdata 57.8%	68	Intuit Group 42.8%
3	Google LLC 93.8%	36	GoDaddy Operating Company, LLC 56.3%	69	DocuSign 42.7%
4	Oracle Corporation Group of Companies 92.5%	37	Yeast 55.9%	70	Sentry 41.8%
5	Meta Corporation 88.7%	38	SAP SE 55.8%	71	Nikkei 41.4%
6	F5 Group 87.6%	39	VMware Corporation 55.1%	72	Absorb Software Group 41.0%
7	PHP 82.1%	40	Python Software Foundation 54.9%	73	Node.js 40.9%
8	Bootstrap 81.8%	41	Atlassian Corporation 53.4%	74	c 39.5%
9	Apache Software Foundation 81.4%	42	LightBox 52.3%	75	Almond 38.9%
10	BuiltWith 81.3%	43	Yahoo Corporation 50.8%	76	Fastly Corporation 38.7%
11	AWS 79.7%	44	Broadcom 50.6%	77	Fortinet 38.6%
12	X Corp. System 79.0%	45	GreenSock 50.4%	78	Varnish Software 38.5%
13	Font Awesome 77.6%	46	OpenBSD Project Group 49.6%	79	Autodesk Group 38.4%
14	DigiCert 75.7%	47	fancybox 49.6%	80	Drupal Association 38.3%
15	Cloudflare 75.0%	48	OpenSSL 49.3%	81	PayPal Group of Companies 38.0%
16	Let's Encrypt 74.6%	49	ContentSquare Group 49.1%	82	Apache 37.9%
17	Automattic Group 72.8%	50	UNPKG 48.9%	83	Rackspace Technology Corporation 37.8%
18	jsDelivr 70.9%	51	New Relic Group 48.5%	84	Lumen 37.6%
19	Apple Corporation 69.9%	52	Babel 47.9%	85	Maya Simulation Technologies Group 37.5%
20	Webpack 69.2%	53	JS.ORG 47.7%	86	Twilio Corporation 37.4%
21	Evolink.CDN 68.6%	54	Vimeo.com Corporation 47.4%	87	Envoy Proxy 37.0%
22	cdnjs 67.5%	55	Globalsign 47.2%	88	Docker Corporation 36.9%
23	React 66.3%	56	AngularJS 46.6%	89	Verisk 36.5%
24	Rapid7 65.2%	57	Metafizzy 46.1%	90	Pinterest Corporation 36.3%
25	Adobe Group 64.9%	58	Workday Group 46.0%	91	Sectigo Group 36.2%
26	Cisco Corporation 64.6%	59	OneTrust Corporation 45.2%	92	Search Discovery 36.2%
27	Salesforce Corporation 61.1%	60	Contact Form 7 44.8%	93	DataTables 35.9%
28	International Business Machines Group 60.6%	61	StackPath 44.8%	94	WOW! 35.8%
29	Vue 60.2%	62	Visa 44.6%	95	LightBox Corporation 35.3%
30	Respond 59.3%	63	Newfold Digital Corporation 44.3%	96	Alibaba Group of Companies 35.2%
31	Envato 59.2%	64	HubSpot Corporation 44.0%	97	Shutterstock Group 35.2%
32	SmartKargo 58.2%	65	Symantec Corporation - Corporate 43.9%	98	Progress Software Corporation of Companies 35.2%
33	Canonical 58.1%	66	Cloud Software Group of Companies 43.8%	99	Perl 35.1%

Large providers don't always have large market share

Market Share



% of Providers



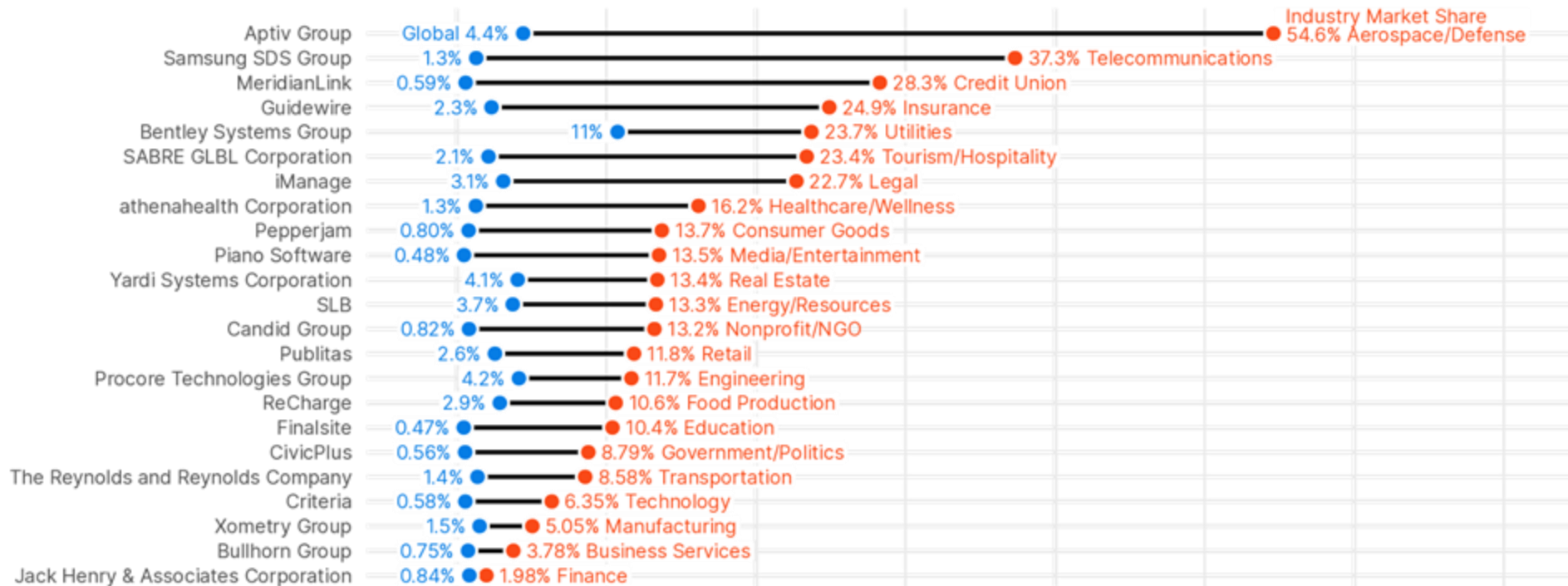


Hidden Pillars

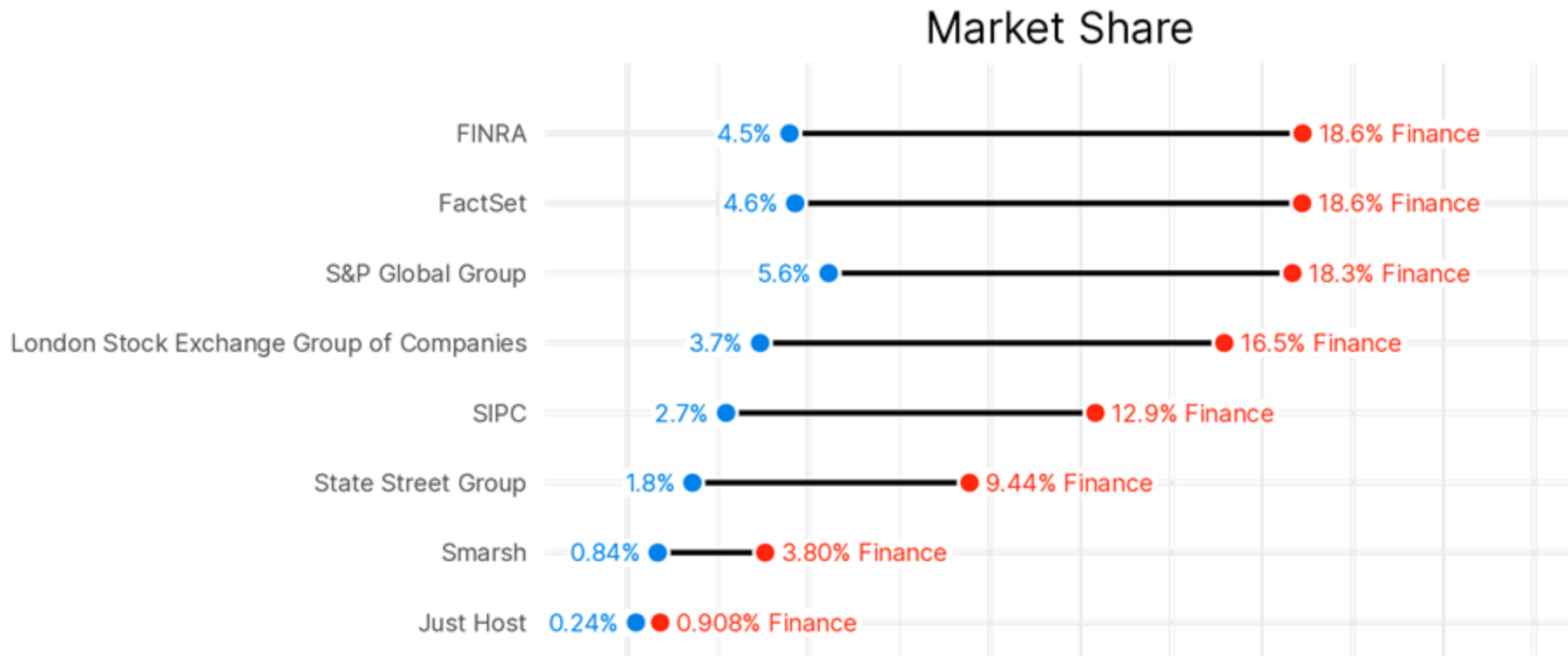
Some providers serve a relatively small segment of the global supply chain, but a larger segment of specific industries

Hidden Pillars

Market Share

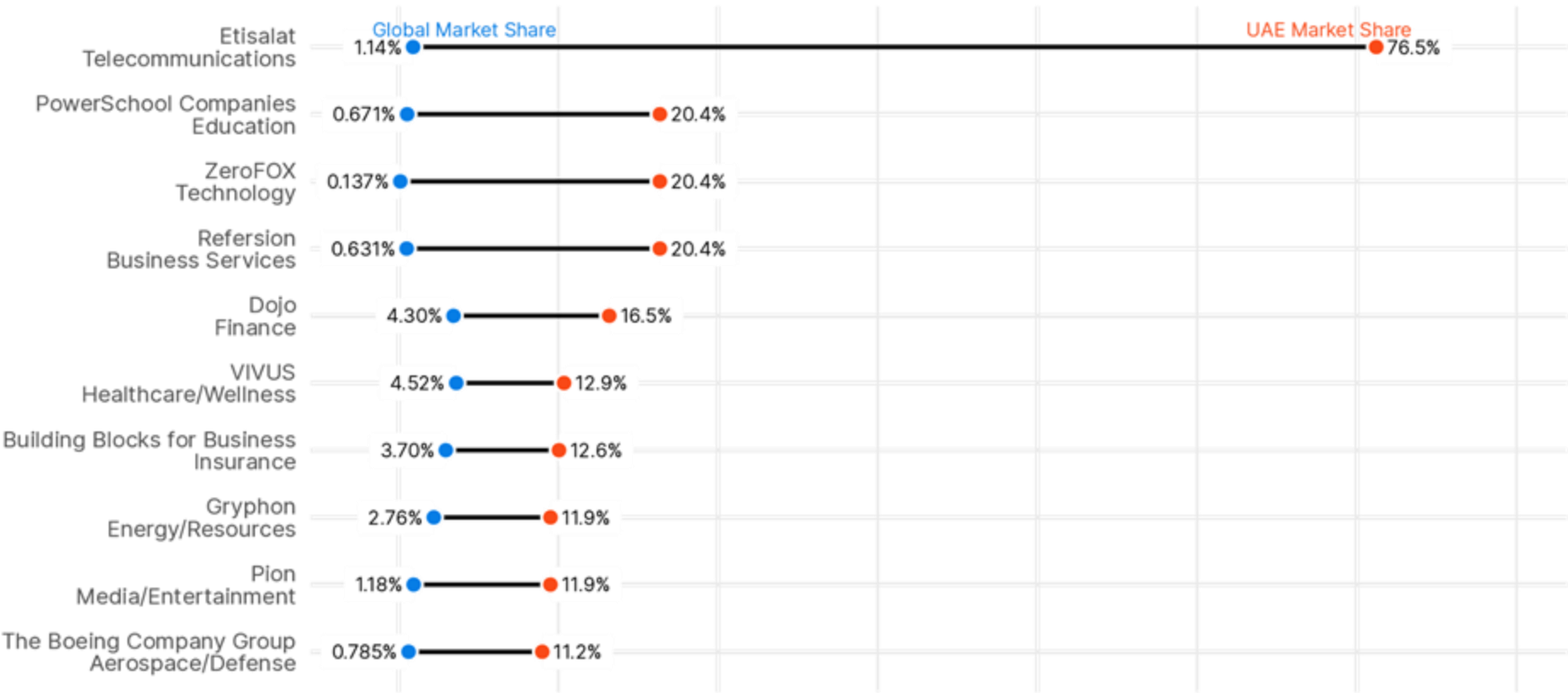


Financial Hidden Pillars



UAE Hidden Pillars

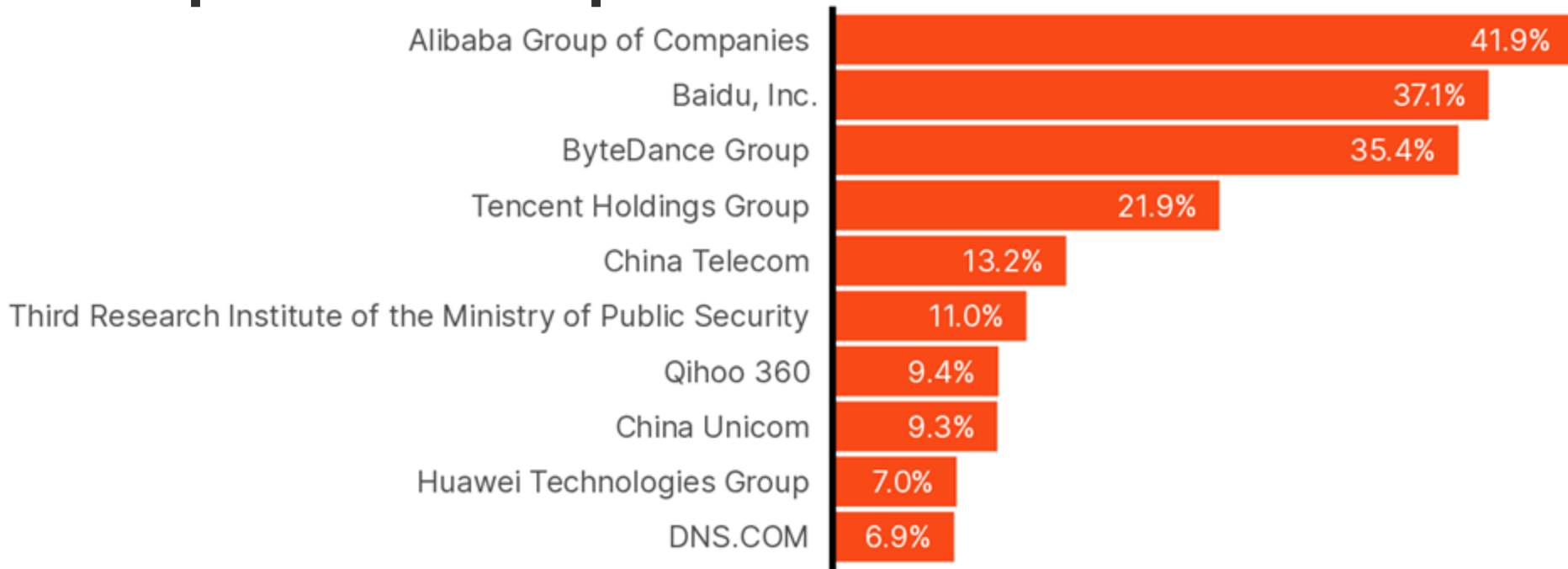
Market Share



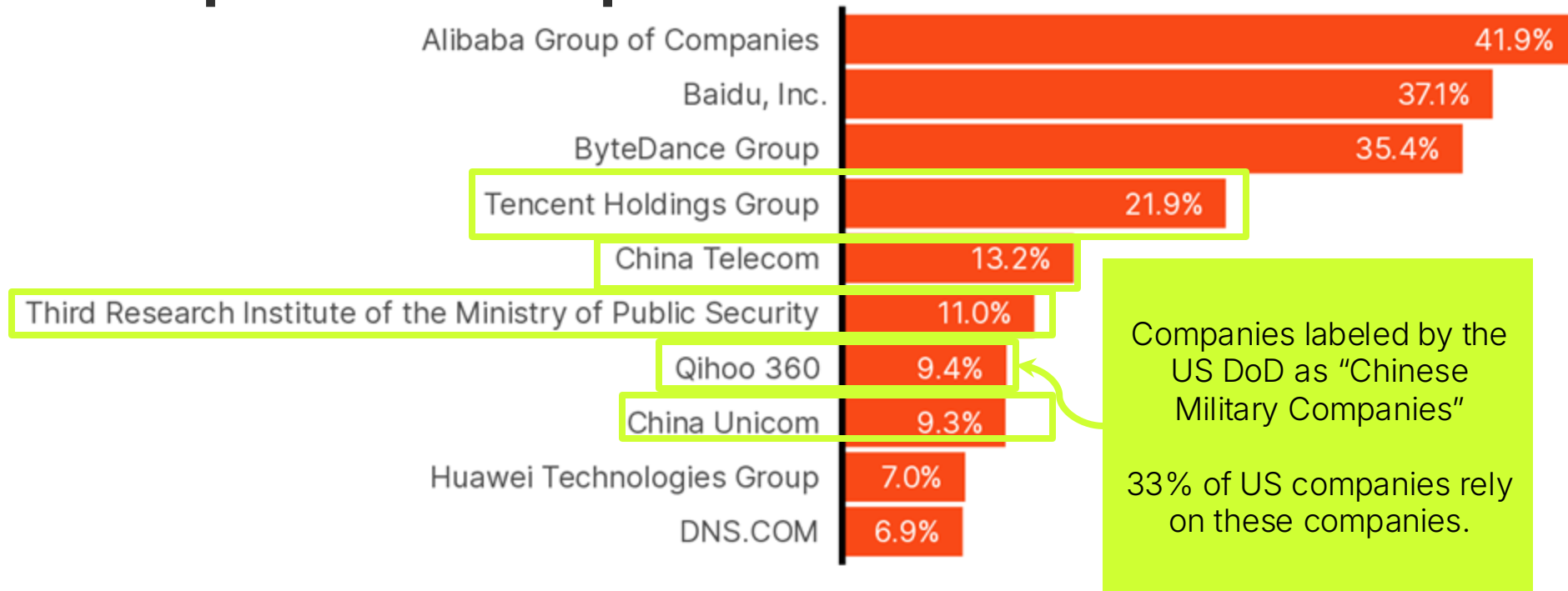


Geopolitical Complications

Geopolitical Complications



Geopolitical Complications

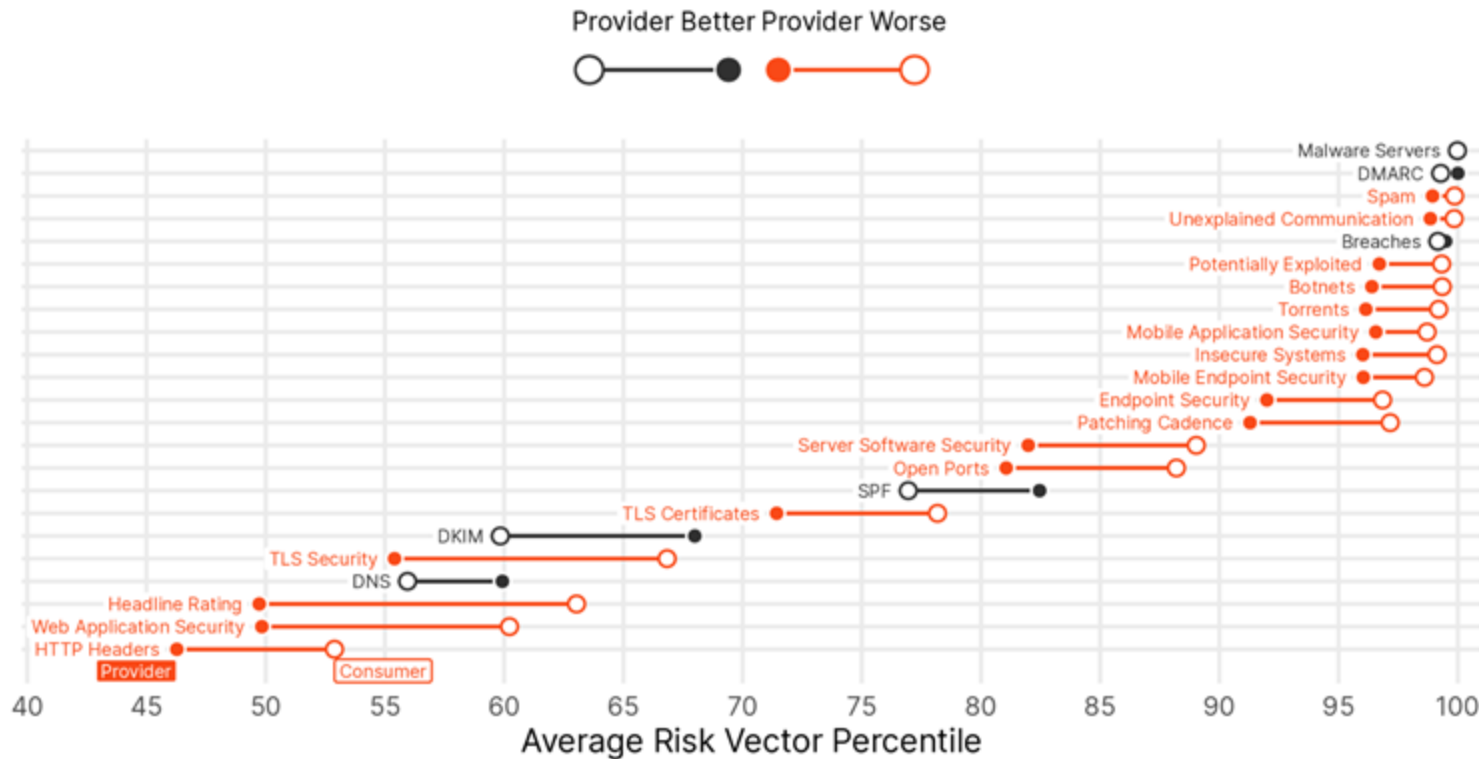




Security in the Global Supply Chain

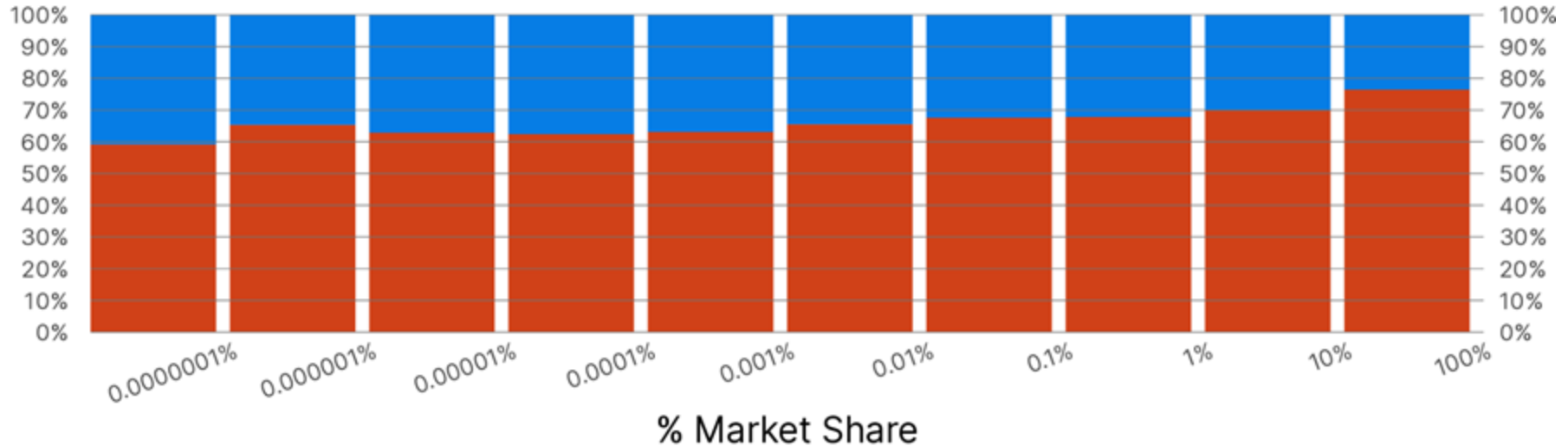
Risk Vectors are aggregate scores computed by Bitsight

Security Performance in the Global Supply Chain



Provider size and security performance

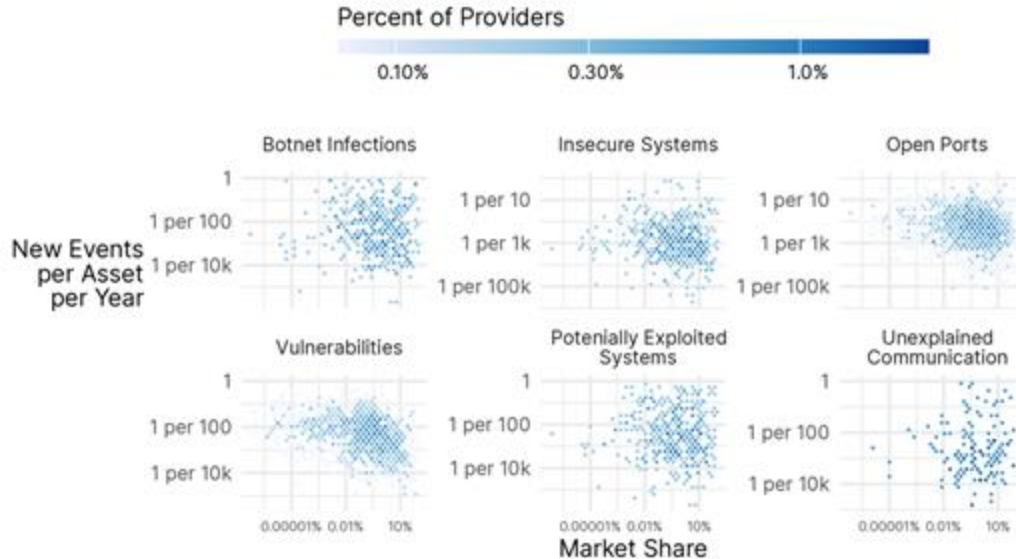
Percent of Providers



Top Half Bottom Half

Headline Rating Percentile

Supply Chain risk at any size



An **EMEA transportation company** with **20% global market share** has an **insecure systems** rate in the **worst 25%** (in a year, 1 in 9 systems has an insecure system finding).

A **US-based marketing corporation** has **14% global market share** in the **worst 25% botnet infection rate** (in a day, 1 in 8 systems would have a botnet infection).

An **APAC manufacturing company** has **10% global market share** and is in the **worst quartile for open ports** (1 in 18 assets has a negative open port finding in a year).

A **Fortune 500 energy company** with **34% global market share** in the **worst quartile of insecure systems**.

Vulnerability risk in Providers



An **EMEA manufacturing company** with **long-standing open vulnerabilities (many over three years old)**, with **five new vulnerabilities added per day**, more than 181k assets on the open internet, and is involved in **26.5% of the global supply chain**.

A **US data center company** that takes **longer than a year to fix** the typical vulnerability, with **four new vulnerabilities per day**, serves more than **10% of the global supply chain**, and has more than 47k publicly facing assets.

Conclusions and Recommendations

Supply chains are large and complex

Criticality is industry and region specific

Even large organizations can struggle with security

Where to go from here

Enumerate your supply chain. Who is enabling your org's mission?

Evaluate criticality. Which providers are indispensable, which are good to have?

Assess your providers' security. Where do they struggle and would an outage impact you?

Reach out. If you can assess their security so can attacker's, let them know what your concerns are.

Look deeper. A third party incident for one of your providers could be impactful, what do their supply chains look like?

Evaluate your own criticality. Are you a critical supplier or hidden pillar?

Under the Surface: Uncovering Cyber Risk in the Global Supply Chain

By Ben Edwards
March 2025





Thank you!

111 Huntington Ave
Suite 2010
Boston, MA 02199
USA

bitsight.com
sales@bitsight.com

BITSIGHT