



360 Overview of Semiconductor from AI and Security Perspective

Claudionor N. Coelho Jr, PhD/MBA

Chief AI Officer / SVP of Engineering

May 2023

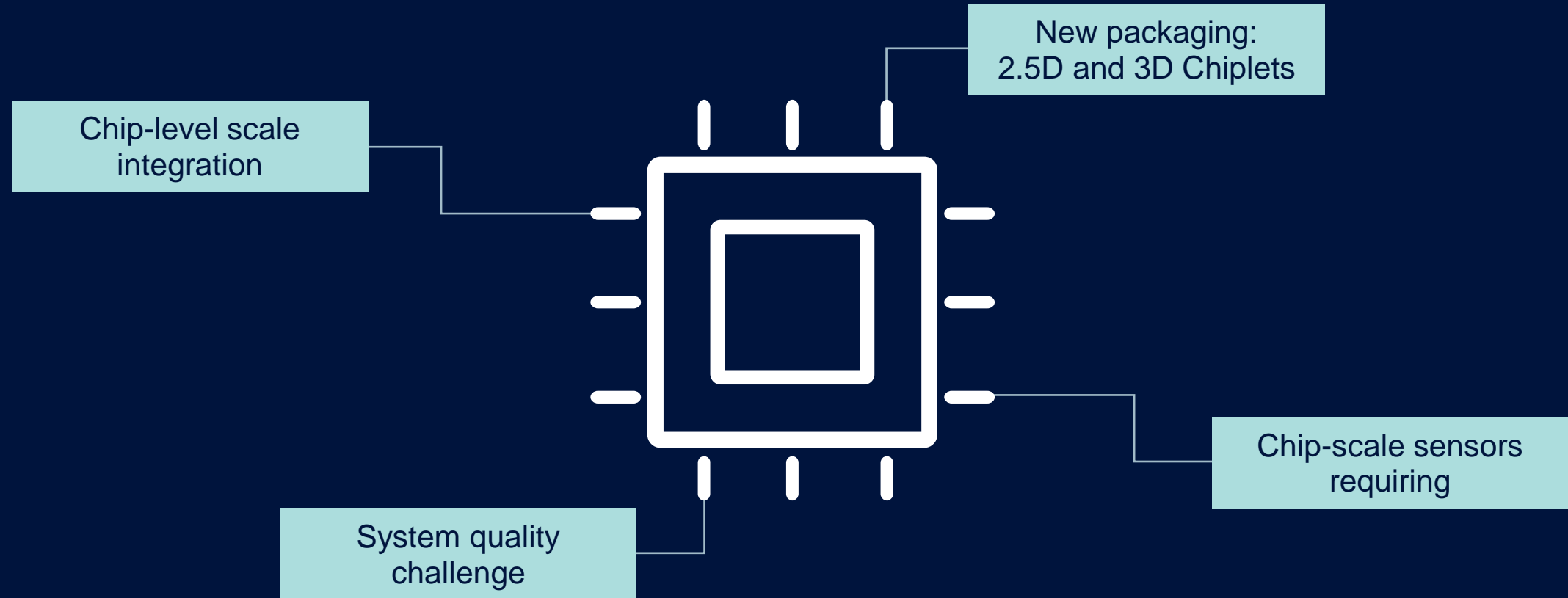


All Rights Reserved - ADVANTEST CORPORATION

Agenda

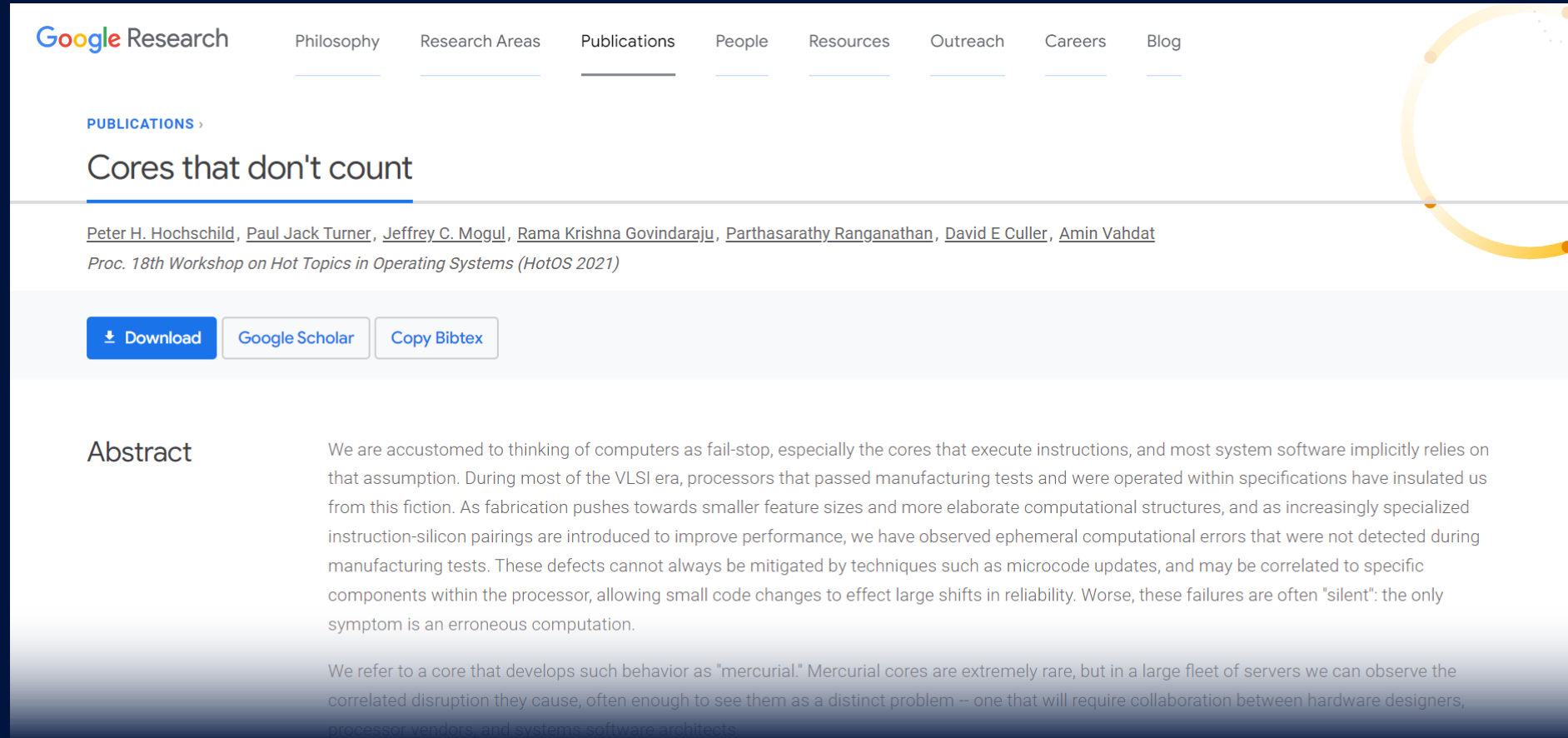
- 1 New Challenges in Semiconductor Manufacturing
- 2 Data is the New Oil
- 3 Security Challenges in Semiconductor Manufacturing
- 4 True Zero Trust™ with Unified Server
- 5 With Information Highway, We Can Embrace AI

New Challenges in Semiconductor Manufacturing



New Challenges in Semiconductor Manufacturing

Cores That Don't Count*



The screenshot shows the Google Research website interface. At the top, the Google Research logo is on the left, and navigation links for Philosophy, Research Areas, Publications, People, Resources, Outreach, Careers, and Blog are on the right. The 'Publications' link is underlined. Below the navigation bar, the word 'PUBLICATIONS' is followed by a right-pointing arrow. The title 'Cores that don't count' is displayed in a large font. Below the title, the authors' names are listed: Peter H. Hochschild, Paul Jack Turner, Jeffrey C. Mogul, Rama Krishna Govindaraju, Parthasarathy Ranganathan, David E Culler, and Amin Vahdat. Below the authors' names is the text 'Proc. 18th Workshop on Hot Topics in Operating Systems (HotOS 2021)'. Below this text are three buttons: 'Download' (with a download icon), 'Google Scholar', and 'Copy Bibtex'. Below the buttons is the 'Abstract' section. The abstract text reads: 'We are accustomed to thinking of computers as fail-stop, especially the cores that execute instructions, and most system software implicitly relies on that assumption. During most of the VLSI era, processors that passed manufacturing tests and were operated within specifications have insulated us from this fiction. As fabrication pushes towards smaller feature sizes and more elaborate computational structures, and as increasingly specialized instruction-silicon pairings are introduced to improve performance, we have observed ephemeral computational errors that were not detected during manufacturing tests. These defects cannot always be mitigated by techniques such as microcode updates, and may be correlated to specific components within the processor, allowing small code changes to effect large shifts in reliability. Worse, these failures are often "silent": the only symptom is an erroneous computation. We refer to a core that develops such behavior as "mercurial." Mercurial cores are extremely rare, but in a large fleet of servers we can observe the correlated disruption they cause, often enough to see them as a distinct problem – one that will require collaboration between hardware designers, processor vendors, and systems software architects.'

Peter H. Hochschild

Paul Turner

Jeffrey C. Mogul

Rama Govindaraju

Parthasarathy Ranganathan

David E. Culler

Amin Vahdat

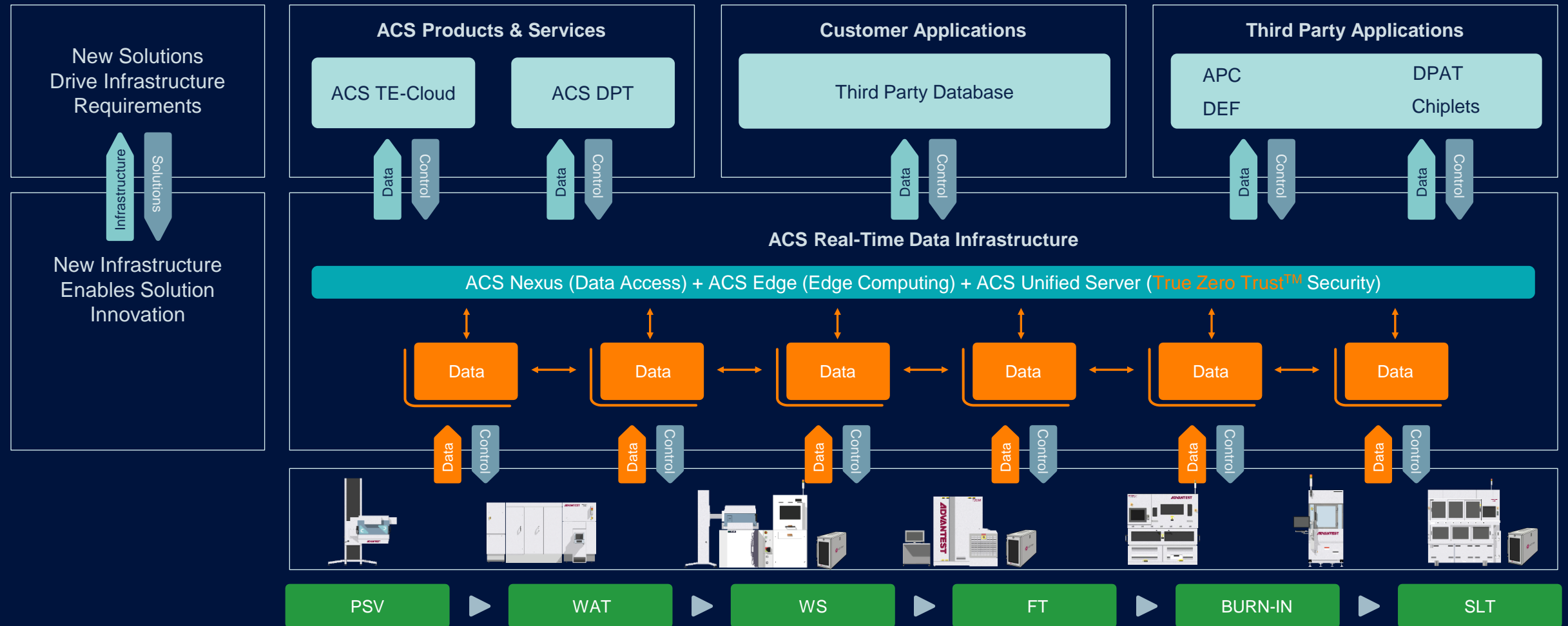


Sunnyvale, CA US

*<https://research.google/pubs/pub50337/>

We Will Need Data from All Sources to Help with New Challenges

Open Solutions Ecosystem



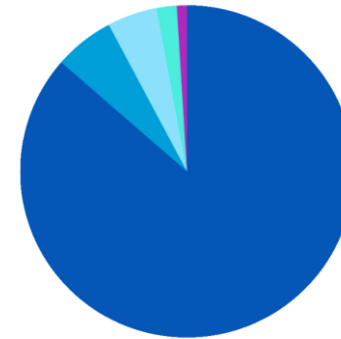
Should I Worry About Security?

Protection

- Security updates
- Removing unnecessary drivers
- Closing unnecessary ports
- Limiting access to systems
- Using firewalls, anti-virus, malware, spyware protection applications
- Encryption
- Password management
- Intrusion prevention systems (IPS)
- Intrusion detection systems (IDS)

We've blocked 522 threats to your network

Since January, 2022



*Result of
protection of
my home against
known threats*



Rubrik CEO: Cyber Attacks Are Inevitable

bloomberg.com • 1 min read

Rubrik CEO: Cyber Attacks Are Inevitable

Bloomberg Technology - TV Shows

April 18th, 2023, 3:02 PM EDT

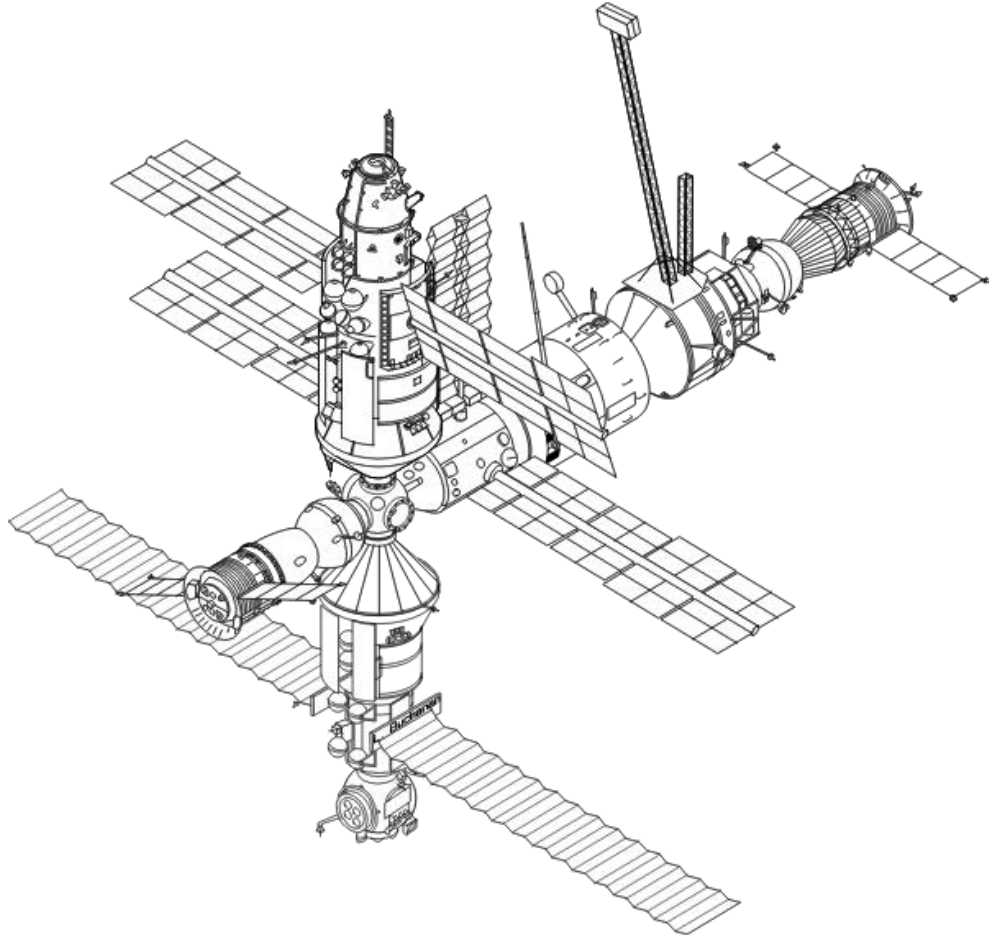
Rubrik CEO Bipul Sinha joins Ed Ludlow to discuss the state of cybersecurity even as the Pentagon leak investigation is still ongoing, what companies can do to better protect themselves and why the company is waiting for the market to "be ready" before going public. (Source: Bloomberg)

[Watch Rubrik CEO: Cyber Attacks Are Inevitable - Bloomberg](#)

Digression: Let's Talk About the ISS



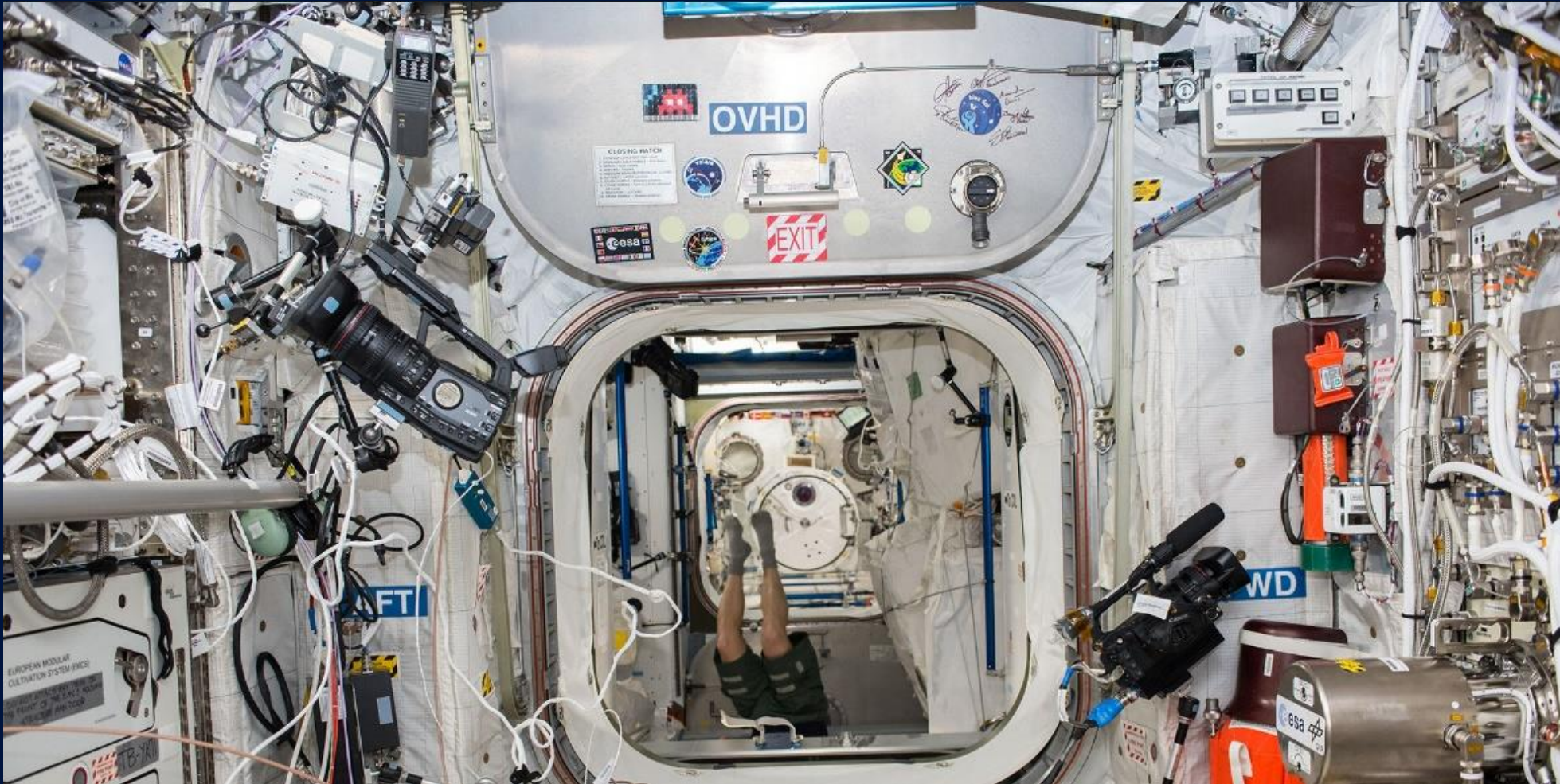
Outer Hull of ISS **Protects** Against Debris



The ISS has shields called Whipple bumpers. They are multi-layered with spaces between the layers. The intent is that impact with a layer will both slow and hopefully break apart the projectile, so that by the time it gets to the bottom layer it is no longer harmful.

<https://freesvg.org/international-space-station-vector-drawing>, <https://www.trtworld.com/life/how-is-nasas-iss-protected-against-space-debris-338800>

Containment Doors Ensure Leaking Areas Can Be Isolated



Eventually, debris will go through, and air leaks will need to be contained

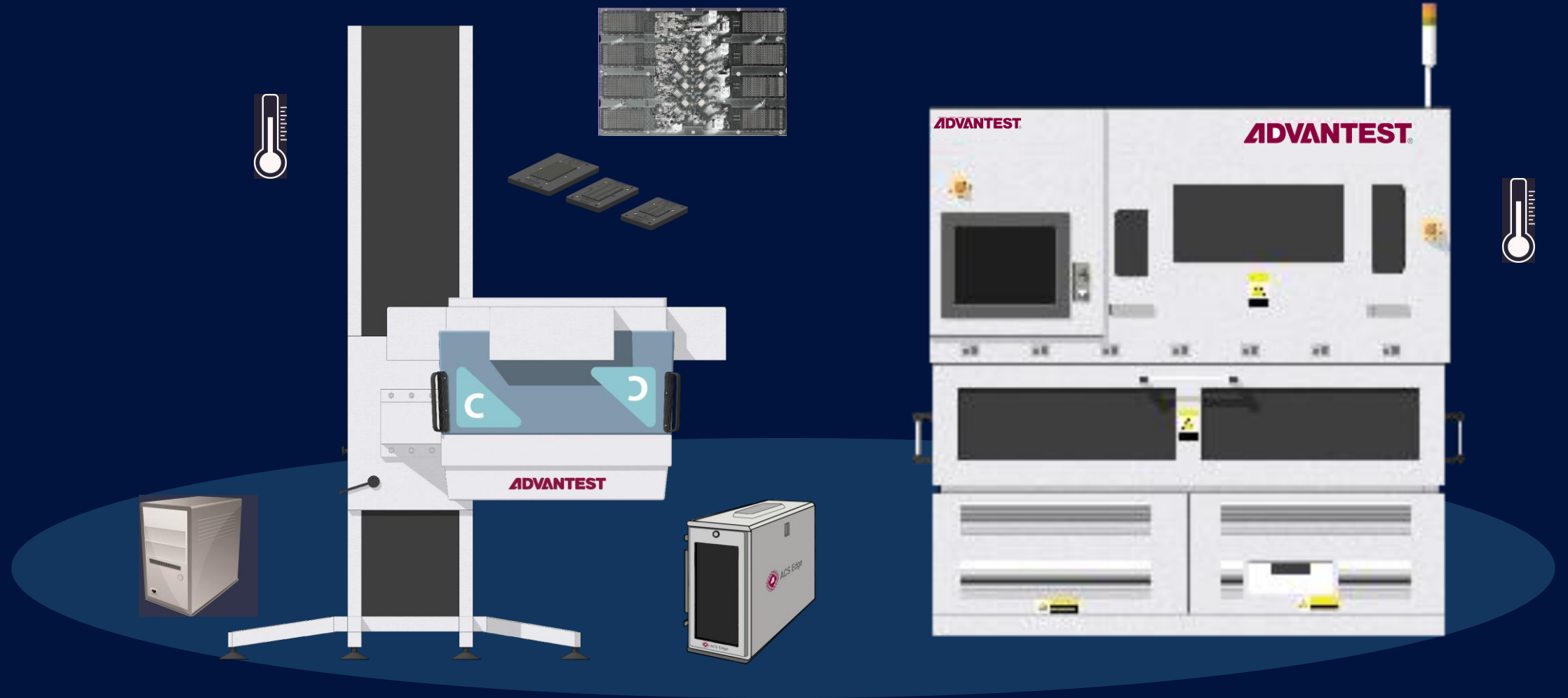
https://www.esa.int/ESA_Multimedia/Images/2015/03/Space2_on_Columbus

... this shows is just **not enough to protect** ...

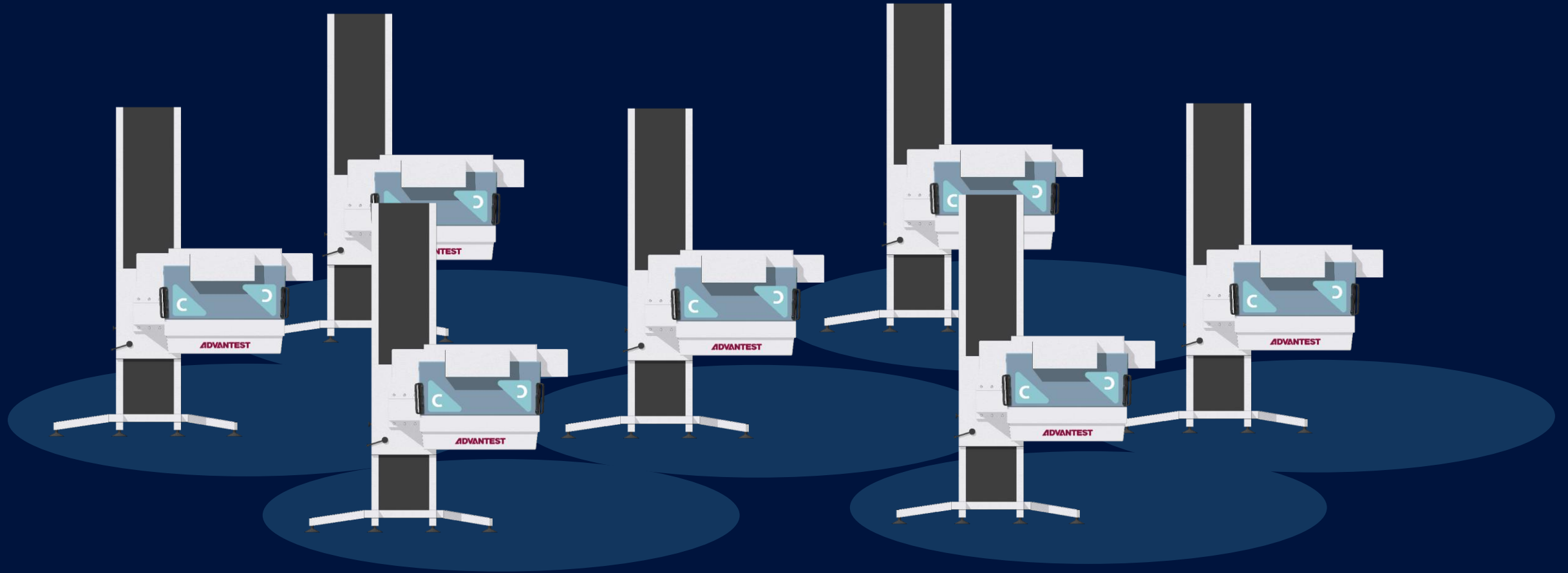


... we also **need to contain**

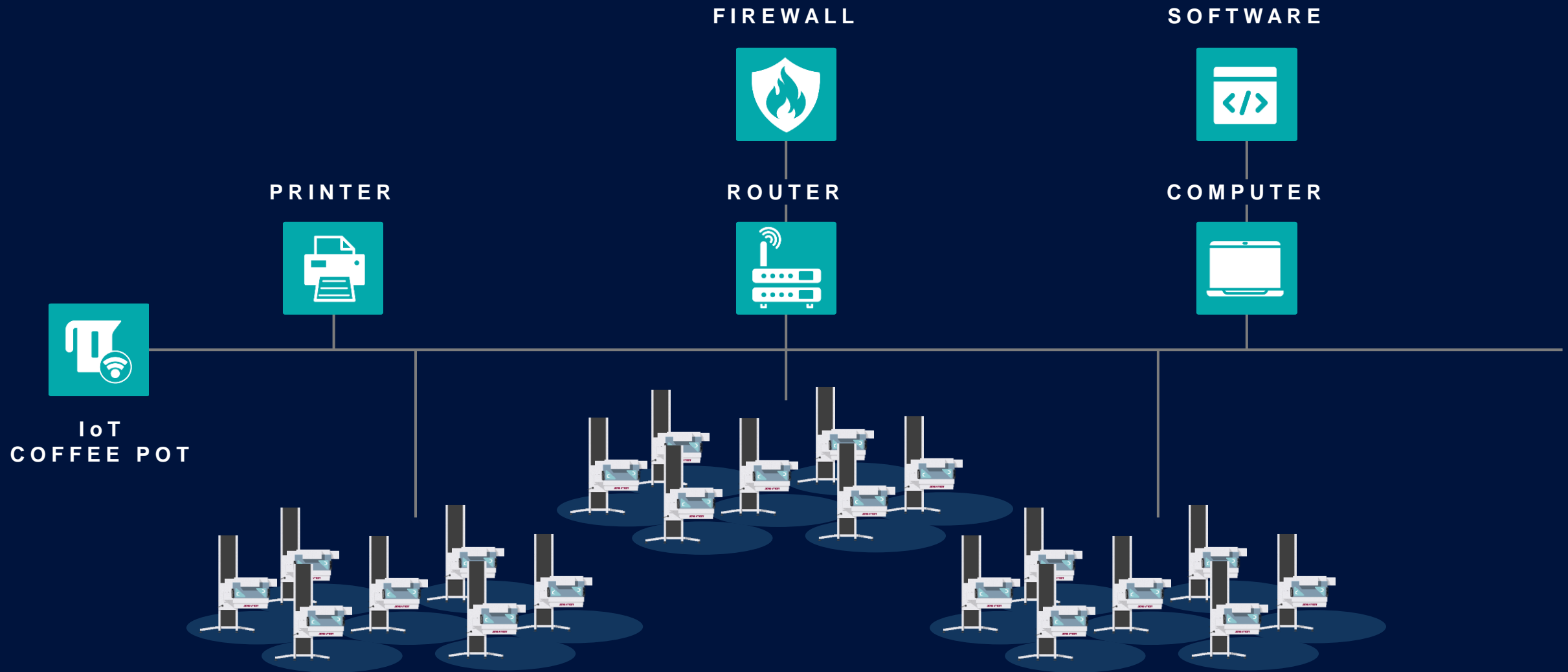
Usually, We Think about Test Cell



... But Test Cell is Included in a Test Floor ...



... And Test Floor is Surrounded by Other Equipment



Target's 2013 Data Hack – What Happened and How?



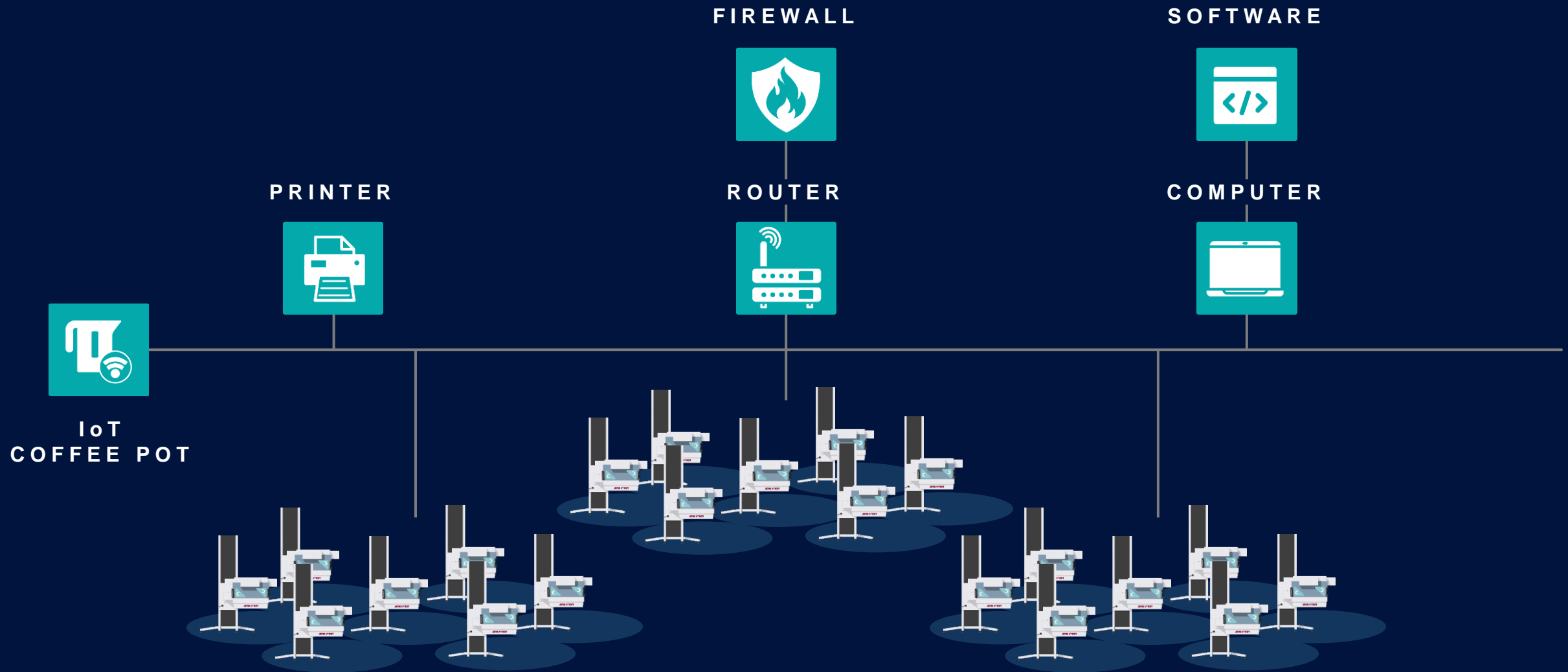
Four years ago, the Target Corporation found itself in the crosshairs of dedicated hackers that resulted in one of the largest attacks on a retail chain in recent years. As a result, 40 million Target customers' records were stolen, and upwards of 70 million further records were compromised. The fallout of this incident was a nationwide lawsuit against the corporation, involving 47 states as well as the District of Columbia. As of May 2017, this [legal battle was settled](#) with Target paying out \$18.5 million in settlement claims. Apart from the legal costs, Target disclosed that the hack cost the company an estimated \$202 million.

Target Corporation claims to yield impressive data security programs that are similarly used by Federal agencies, such as the CIA and the Pentagon, and yet a breach of this magnitude was still successful. Compared to the immediate aftermath of the incident, today we know considerably more about the nature of the hack and, more importantly, how it could have been prevented.

The method of the hack itself was relatively unorthodox, yet clearly effective. Instead of attempting to breach Target's security measures protecting its databases, malware was instead allowed to infiltrate the company [via its point of sale machines](#). The investigation into this attack discovered that the origin of the malware came from a phishing email that was sent to employees of Fazio Mechanical, an HVAC firm that was hired by Target, and was subsequently downloaded (likely by accident) by an employee.

<https://cinteot.com/targets-2013-data-hack-happened/>

... And Test Floor is Surrounded by Other Equipment



EDITORS' PICK

Nearly A Million Printers At Risk Of Attack, Thousands Hacked To Prove It

Lee Mathews Senior Contributor ⓘ

Observing, pondering, and writing about tech. Generally in that order.

[Nearly A Million Printers At Risk Of Attack, Thousands Hacked To Prove It \(forbes.com\)](#)

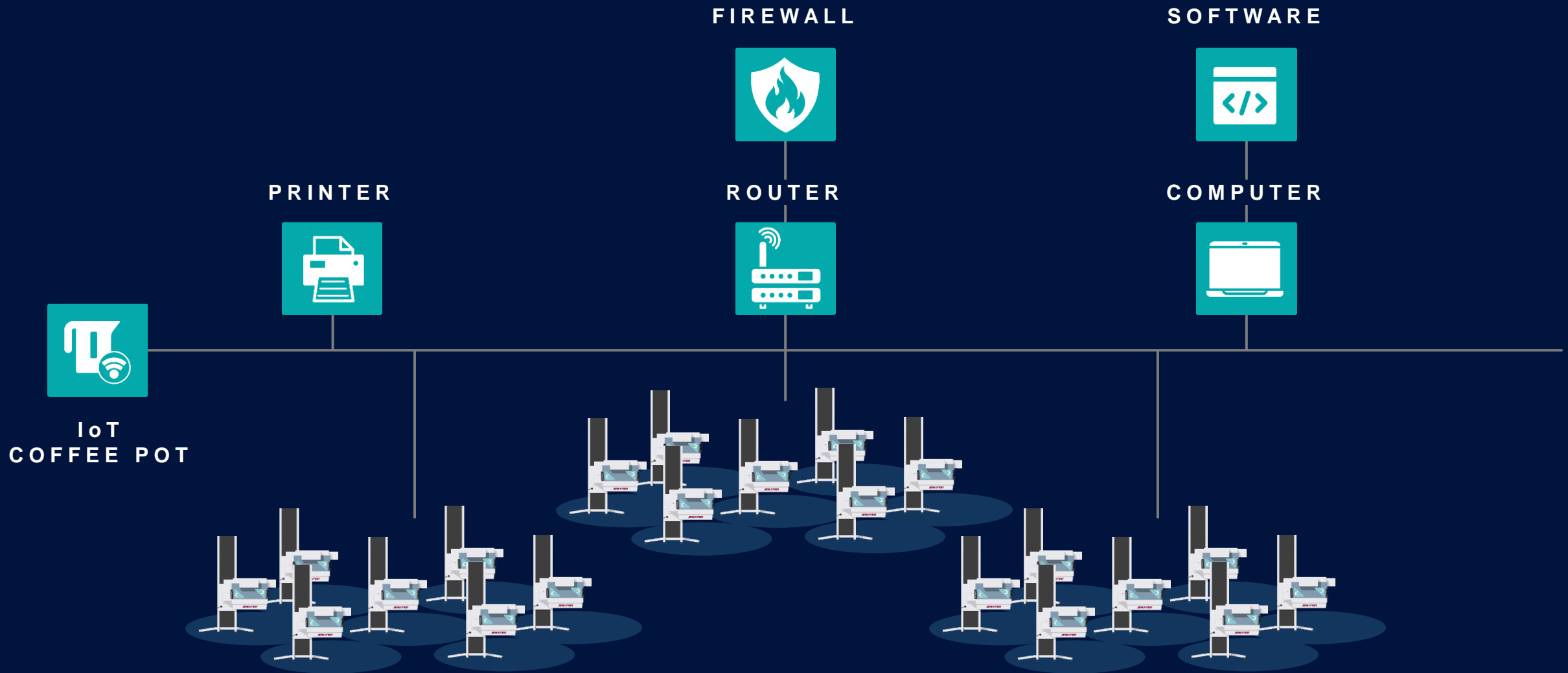
The Lazarus heist: How North Korea almost pulled off a billion-dollar hack

© 21 June 2021



[The Lazarus heist: How North Korea almost pulled off a billion-dollar hack - BBC News](#)

... And Test Floor is Surrounded by Other Equipment



Attacks Can Target Software Update Servers ...

Possible channel

Alan Woodward, a computer scientist from the University of Surrey, said: The ironic thing about this situation (if it proves to be the case) is that we always advise users to keep their software up to date, ideally using automated updates.

"However, it assumes hackers can't take over the update process and misuse it.

"This process is normally a very tightly controlled process, so this is unusual.

"I can imagine many vendors are now triple-checking to make sure they don't end up being an attack vector."

He said that it showed "hackers will probe every possible channel" to find a route into systems.

"As users there isn't a lot we can do as we are in the hands of the software vendors."

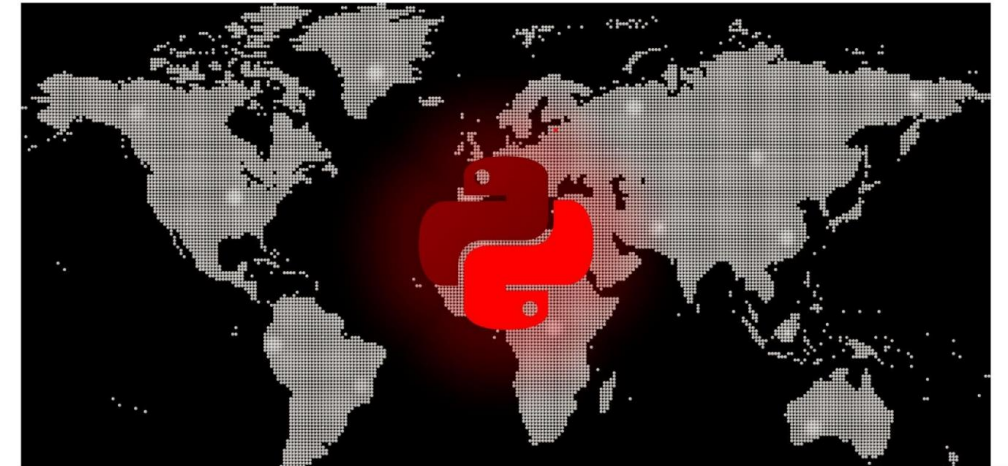
[Tax software blamed for cyber-attack spread - BBC News](#)

Malicious 'Lolipop' PyPi packages install info-stealing malware



By [Bill Toulas](#)

January 16, 2023 11:41 AM



[Malicious 'Lolip0p' PyPi packages install info-stealing malware \(bleepingcomputer.com\)](#)

PyTorch

Get Started

Ecosystem ▾

Mobile

Blog

Tutorials

Docs ▾

Resources ▾

GitHub



December 31, 2022

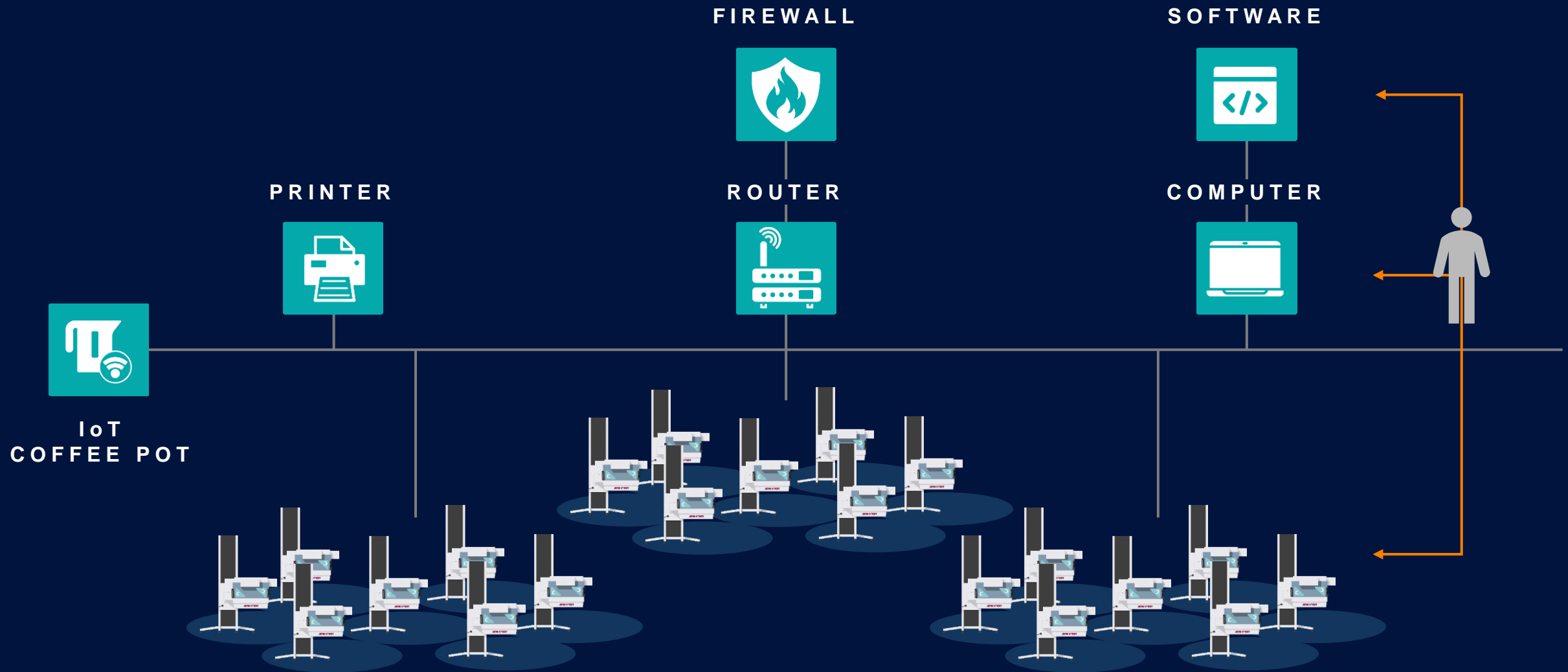
Compromised PyTorch-nightly dependency chain
between December 25th and December 30th, 2022.

[Compromised PyTorch-nightly dependency chain between December 25th and December 30th, 2022. | PyTorch](#)



by The PyTorch Team

... And Test Floor is Surrounded by Other Equipment



Microsoft warns of North Korean crew posing as LinkedIn recruiters

State-sponsored ZINC allegedly passes on malware-laden open source apps

 [Laura Dobberstein](#)

Fri 30 Sep 2022 // 05:53 UTC

Microsoft has claimed a North Korean crew poses as LinkedIn recruiters to distribute poisoned versions of open source software packages.

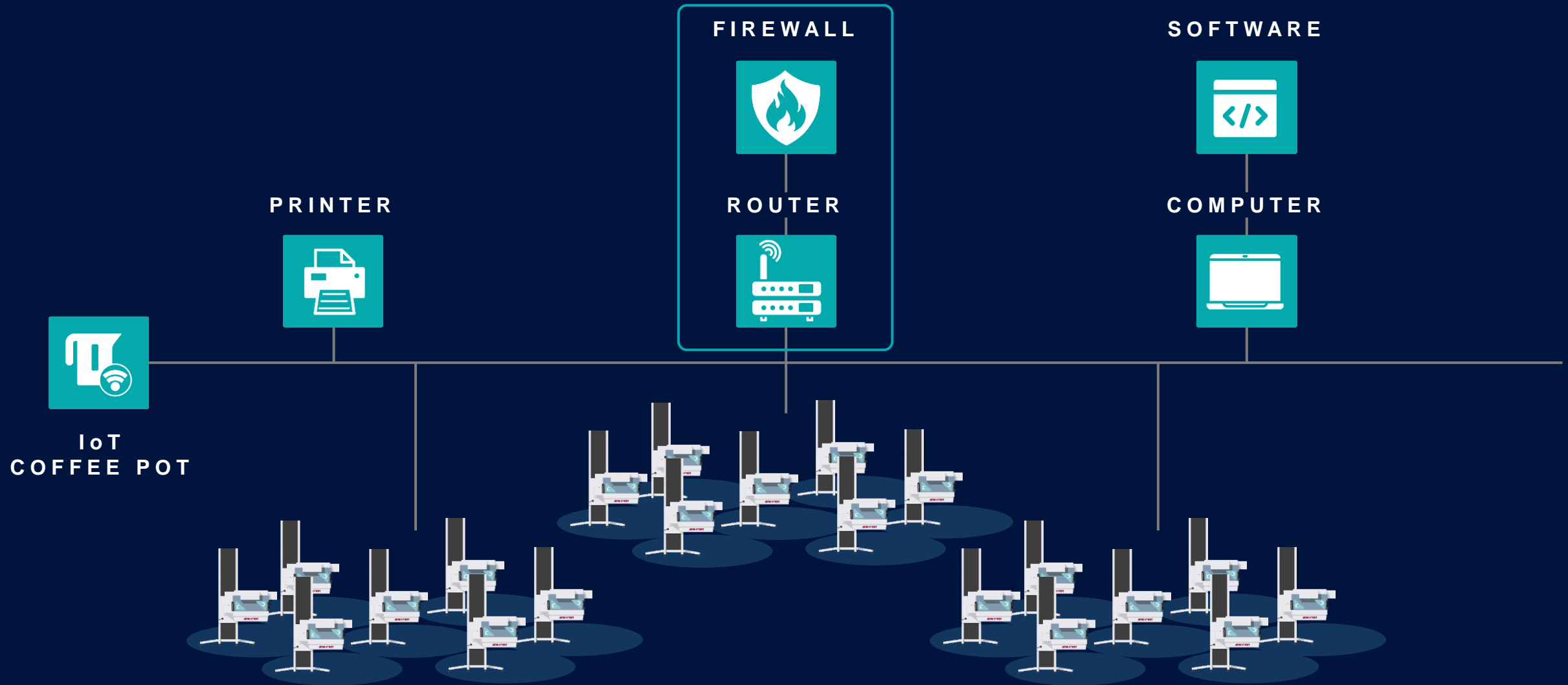
The state-sponsored group has been around since 2009 and was allegedly behind the 2014 attack on Sony Pictures in retaliation for the controversial Seth Rogen comedy *The Interview*.

Dubbed "ZINC", the threat actors have previously run long-term phishing schemes targeting media, defence and aerospace, and IT services organizations in the US, UK, India, and Russia.

Starting in June of this year, ZINC relied on social engineering tactics: contacting targets on LinkedIn and claiming to be a recruiter, establishing trust with targets, and switching communications to WhatsApp where they delivered shellcode from the ZetaNile malware family.

https://www.theregister.com/2022/09/30/microsoft_north_korea_zinc_threat/

... And Test Floor is Surrounded by Other Equipment



Dozens of Netgear routers can easily be hacked — what to do right now [updated]

By [Paul Wagenseil](#) last updated March 30, 2021

Nearly 80 Netgear router models could be hacked over the Internet, but workarounds are trickling out

[f](#) [t](#) [r](#) [p](#) [v](#) [e](#) [m](#) [c](#) [Comments \(0\)](#)



Hello again, old friend. We've met here before. (Image credit: Netgear)

<https://www.tomsguide.com/news/netgear-router-admin-hack>

wikiHow to do anything...



UPGRADE

wikiHow is where trusted research and expert knowledge come together. Learn why people **trust** wikiHow

COMPUTER NETWORKING » VIRTUAL PRIVATE NETWORKS (VPN)

How to Bypass a Firewall or Internet Filter

Written by **Jack Lloyd**

Last Updated: November 25, 2022 ☒ Tested

This wikiHow teaches you how to view blocked websites or content on a restricted computer, as well as on a mobile item if you're using a Virtual Private Network (VPN).

Download Article

METHODS

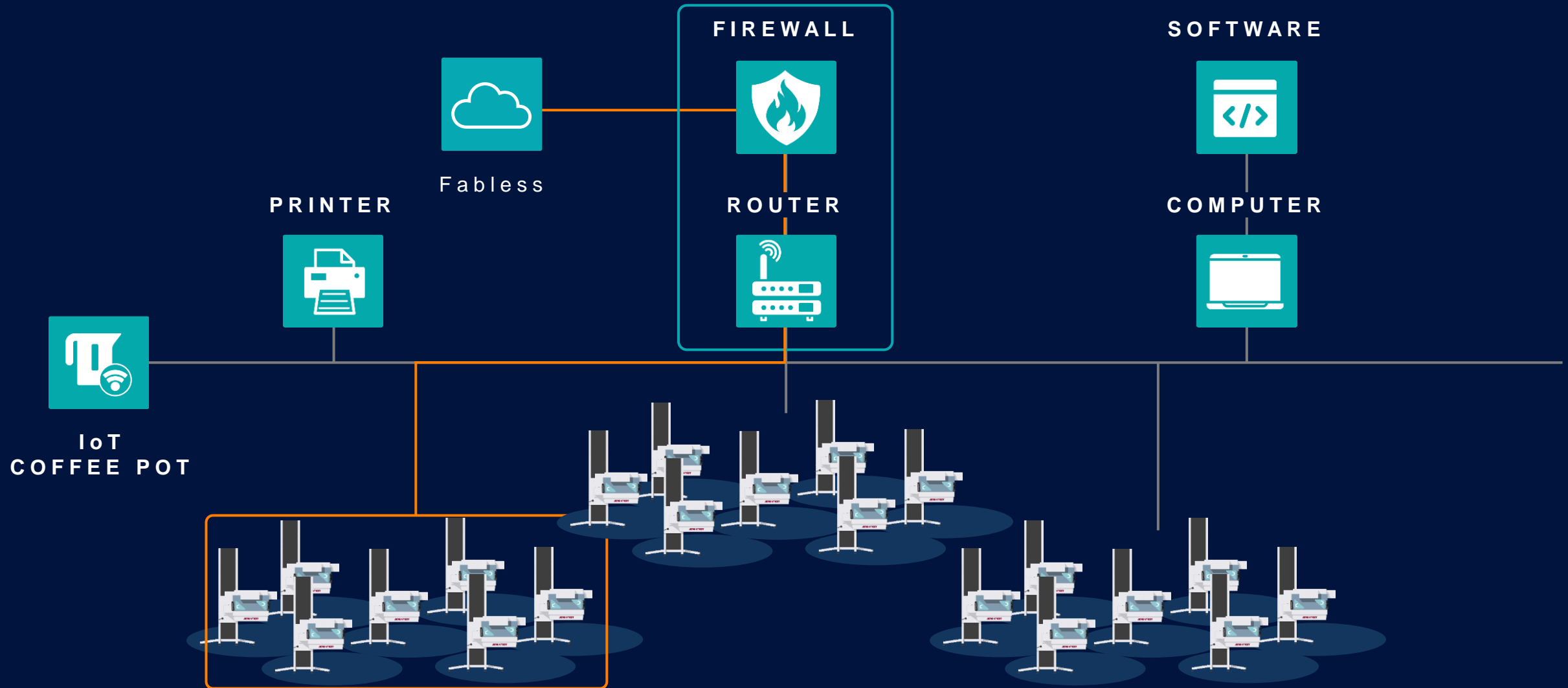
- 1 Using a VPN
- 2 Using UltraSurf
- 3 Using a Web-Based Proxy
- + Show 1 more...

OTHER SECTIONS

- Questions & Answers
- Tips and Warnings
- Related Articles
- Article Summary

<https://www.wikihow.com/Bypass-a-Firewall-or-Internet-Filter>

... Some Test Floors Require Cloud Connection ...



What Your Firewall Won't Protect You From

INSIDER THREATS

Unfortunately, there are plenty of enemies within the gate, sometimes acting intentionally, other times inadvertently creating vulnerabilities.

For example, disgruntled employees can pose a significant threat to your electric cooperative. Already behind the firewall and familiar with the system, they could mass delete files or intentionally install a virus.

A less malevolent (but no less dangerous) threat is shadow IT. This is any software, applications, or firewall exceptions team members install or enable, usually to eliminate steps in a process or make their jobs easier. Though they may not have malicious intent, it's not uncommon for employees to weaken a firewall by adding an excess number of exceptions to it so they can complete a task more quickly. Some of the applications an employee may innocently install may create backdoor access to the co-op's system.

Not every piece of malware gets into your co-op's system through a firewall, either. Computer viruses and other attacks can just as easily get into your system through a USB stick someone has brought in from outside. Again, this may even happen unintentionally.

DATA LEAKAGE

Firewalls may also not be able to protect your co-op from data leakage, or the unauthorized transmission of data leaving your electric co-op. Normally, data leakage happens through the web or email but it is possible to cause data to leak through hardware.

State-sponsored organizations have been known to purposely sabotage equipment so that it leaks data from the organization. Often, this happens in such small amounts even a firewall won't detect something is wrong because the device is supposed to send data as part of its normal operations. Imagine buying a brand-new switch, manufactured overseas, only to discover much later it had been sending sensitive data about you the entire time the leak was unknown. In this situation, even an advanced firewall may not be helpful.

Most data leakage, however, is done using malware specifically designed to slowly leak information out of your cooperative.

Regardless of how it is occurring, data leakage is a very real threat that must be addressed. Simply relying on a firewall to keep your data safe will not keep your electric cooperative safe from this specific kind of cyberattack.

*Shown in
previous
slides*

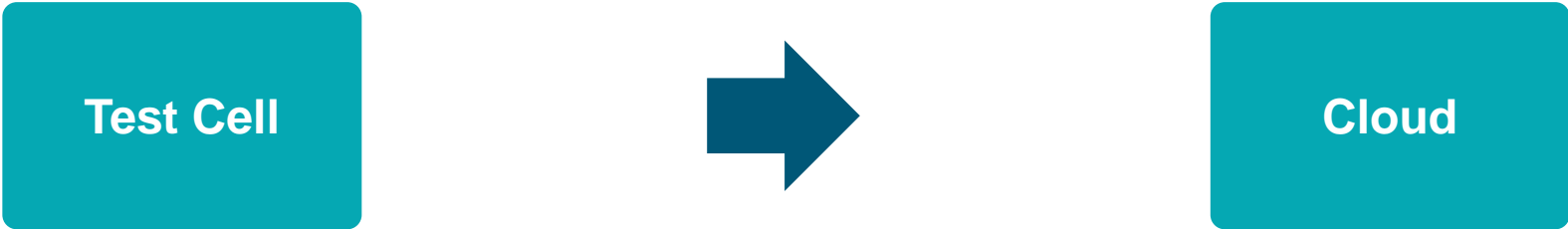
<https://skyhelm.com/cyberattacks-your-firewall-wont-protect-you-from/>

Staging a Data Leakage

secret message

```
hidden_msg = ""
Integrated Annual Report 2022
Advantest has published our Integrated Annual Report 2022.
In addition to financial information, the report includes non-financial
information on our Grand Design, vision, strategy, results, governance,
and sustainability. It provides a comprehensive snapshot of our corporate
value and prospects for medium- to long-term growth.<end>""
```

Insider threat
Data leakage
Web-proxy



measurements

2.2393017	-0.8189581	1.707974	0.91654325	0.53305906	0.22747241
-0.5253728	-1.4496815	0.62295085	-0.4778164		

-0.4778164

```
72 : [ 2.239282 -0.81896126 1.7079598 0.91653633 0.5330567 0.2274721
-0.5253667 -1.4496907 0.622947 -0.47781682] -0.47781682
```

```
Integrated Annual Report 2022
Advantest has published our Integrated Annual Report 2022.
In addition to financial information, the report includes non-financial
information on our Grand Design, vision, strategy, results, governance,
and sustainability. It provides a comprehensive snapshot of our corporate
value and prospects for medium- to long-term growth.
```

Malicious agent can change noise level of measurements and transmit confidential information



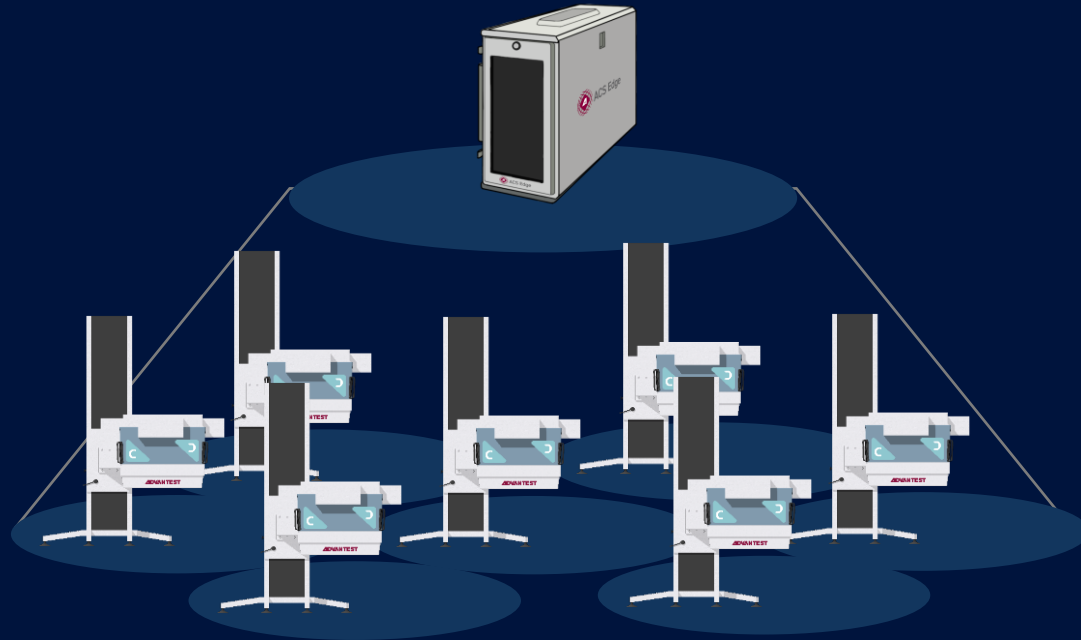
Rubrik CEO: Cyber Attacks Are Inevitable

bloomberg.com • 1 min read



Cyber Attacks are inevitable.
Protection is not enough any longer.
Containment is the only way to secure you have limited leakage.

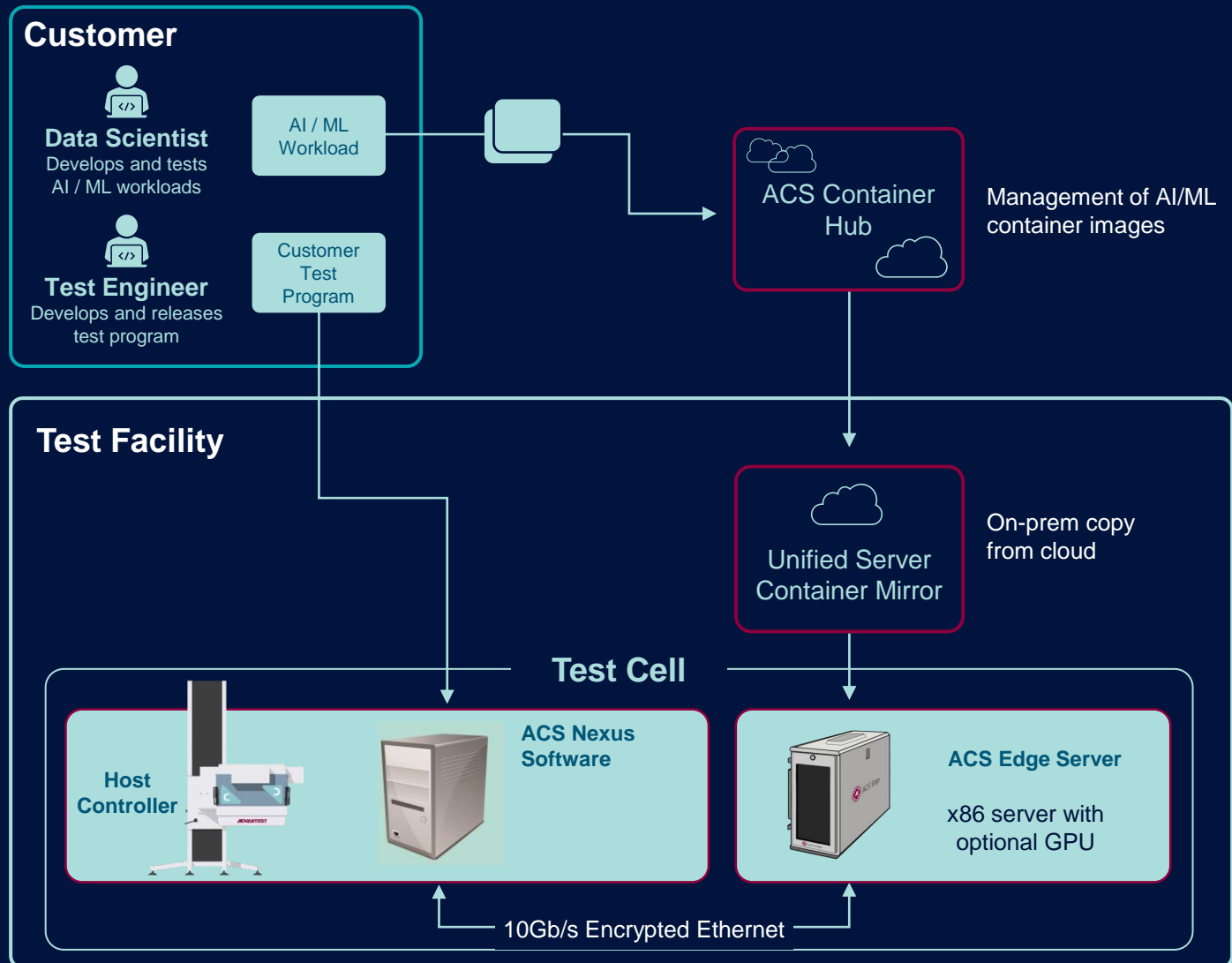
True Zero Trust™ Environment for Test Floor is a Must...



True Zero Trust™ Unified Server

- Provides **containment** environment for Test Floor
- Assumes facility has been compromised upward or downward
- Shared ownership of security by OSAT and Fabless
- Enables packet inspection and logging of transactions
- Provides transaction-level security
- Encrypted traffic to Unified Server
- Third party to provide full SBOM of packages to detect known threats

ACS Real-Time Data Infrastructure (RTDI)



Key Features:

- Communication backplane for Test Floor
- Edge level computing facility
- Floor level True Zero Trust™ with Unified Server Container hub

ACS Real-Time Data Infrastructure Securely Supports...

- Data feed forward / backward with full multi-site integration
- Outlier detection
- Adaptive test
- Predictive modeling
- Optimization of heavy computation test

What Can You do with Edge and Unified Server Infrastructure...

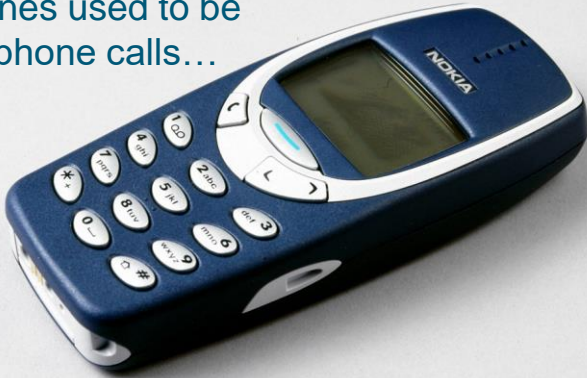
The Brick



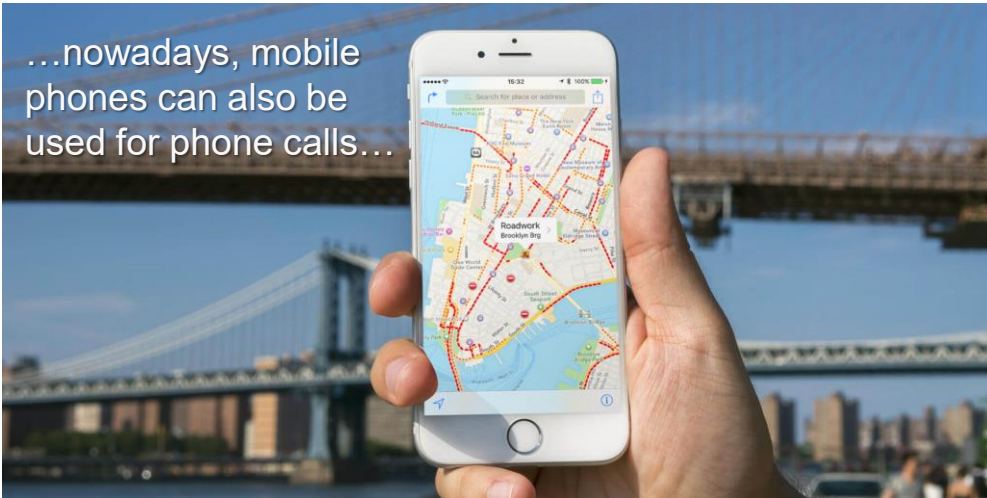
Mobile phones used to be bought for phone calls...

What Can You do with Edge and Unified Server Infrastructure...

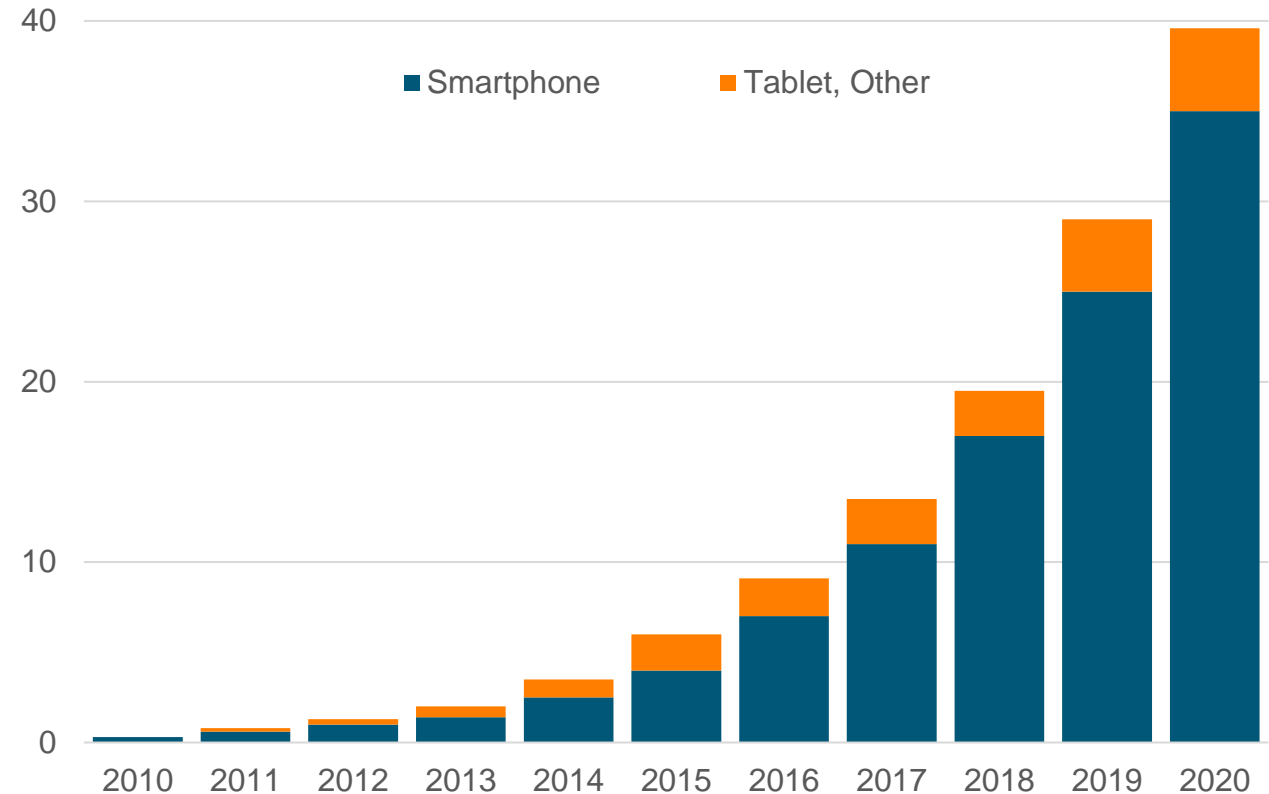
Mobile phones used to be bought for phone calls...



...nowadays, mobile phones can also be used for phone calls...



Global mobile data traffic Exabytes per month



Source: Ericsson Mobility Report

informativ

ADVANTEST®

Embracing AI New Technologies



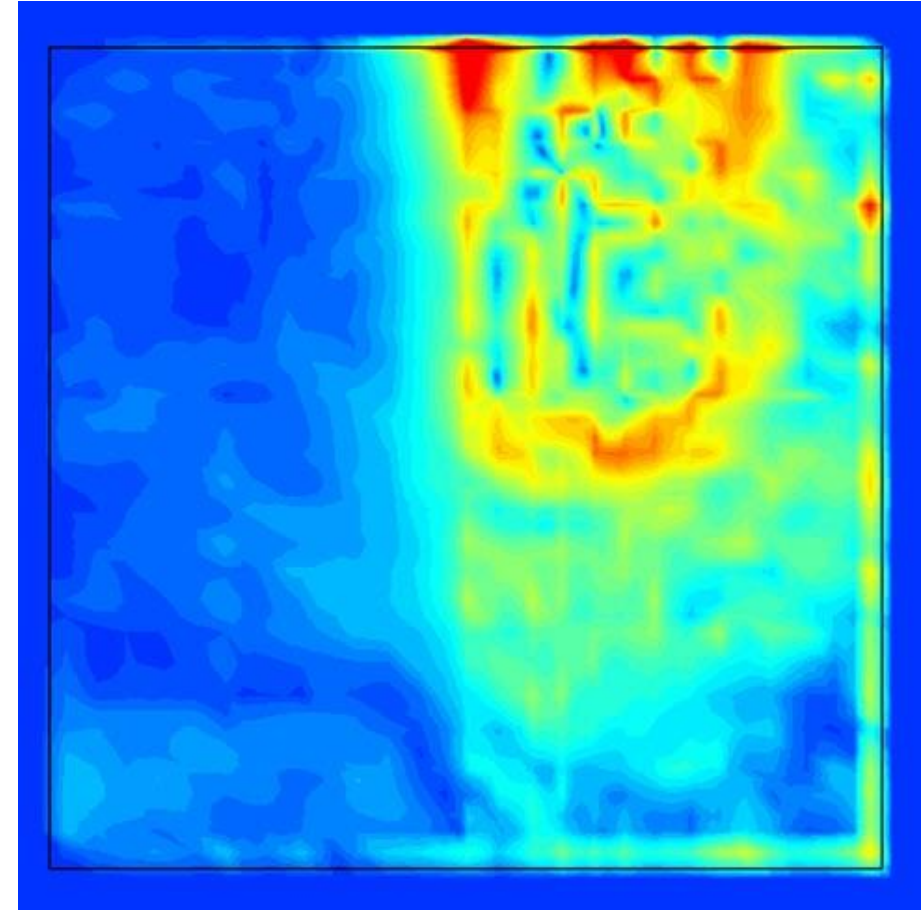
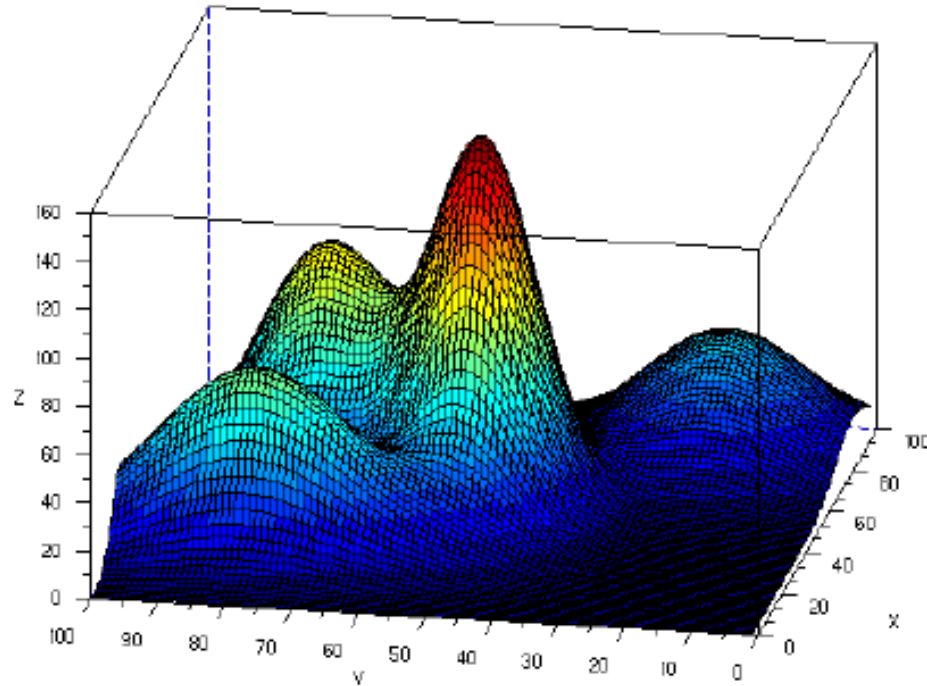
All Rights Reserved - ADVANTEST CORPORATION

Which New AI Technologies Can Be Used With More Data

New chip technologies require new measurements,
relying in multi-dimensional data

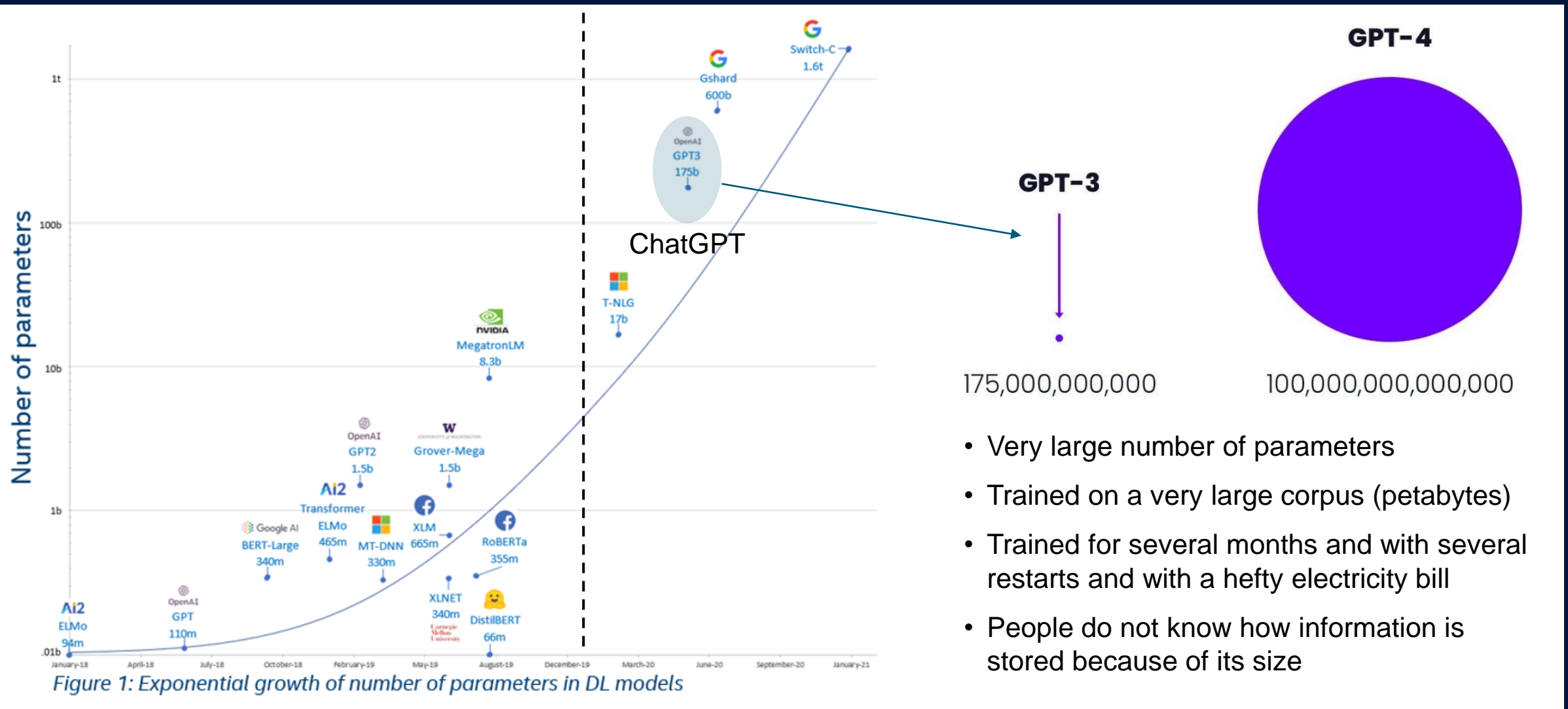
Large Language Models are creating vast new
opportunities in all domains

Thermal Profile of Dies



<https://semiengineering.com/a-high-level-how-to-guide-for-effective-chip-package-thermal-co-design/>

What's an LLM (Large Language Model)?



Using LLMs (Large Language Models)

LLMs can comprehend and link topics and it has “SOME” understanding of math, but ChatGPT does not understand new developments as it is not connected to the Internet

Large Language Models are Zero-Shot Reasoners

Takeshi Kojima

The University of Tokyo

t.kojima@weblab.t.u-tokyo.ac.jp

Shixiang Shane Gu

Google Research, Brain Team

Machel Reid

Google Research*

Yutaka Matsuo

The University of Tokyo

Yusuke Iwasawa

The University of Tokyo

Large Language Models Are Reasoning Teachers

Namgyu Ho, Laura Schmid, and Se-Young Yun

KAIST

{itsnamgyu, laura.schmid, yunseyoung}@kaist.ac.kr

NU

solve $x^2 - 5x + 3 = 0$ for x



This is a second-degree equation and can be solved using the quadratic formula:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Where $a = 1$, $b = -5$, $c = 3$ and the equation is written as:

$$x^2 - 5x + 3 = 0$$

So, plugging in the values, we get:

$$x = \frac{-(-5) \pm \sqrt{(-5)^2 - 4 * 1 * 3}}{2 * 1}$$

$$x = \frac{5 \pm \sqrt{25 - 12}}{2}$$

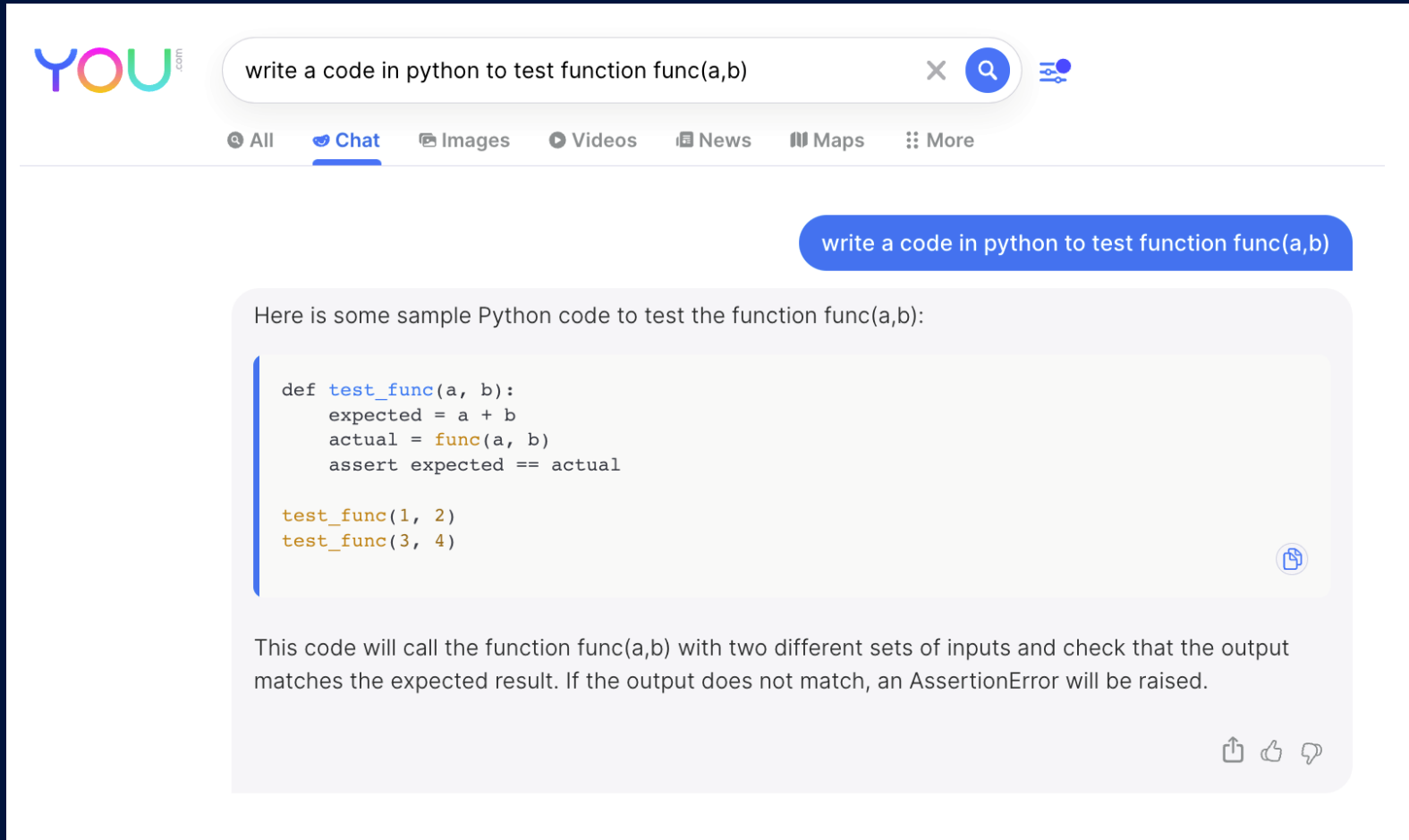
$$x = \frac{5 \pm \sqrt{13}}{2}$$

Therefore, the solutions are:

$$x = \frac{5 + \sqrt{13}}{2} \text{ and } x = \frac{5 - \sqrt{13}}{2}$$

Using LLMs (Large Language Models)

Search Engines list documents. LLMs summarize knowledge.



The screenshot shows the YOU.com search engine interface. At the top, the logo "YOU.com" is on the left. A search bar contains the text "write a code in python to test function func(a,b)". To the right of the search bar are icons for a close button, a search icon, and a filter icon. Below the search bar is a navigation bar with tabs: "All", "Chat" (which is highlighted with a blue underline), "Images", "Videos", "News", "Maps", and "More".

Below the navigation bar, there is a blue pill-shaped button containing the text "write a code in python to test function func(a,b)". Below this button, a light gray box contains the text "Here is some sample Python code to test the function func(a,b):". Inside this box is a code block with the following Python code:

```
def test_func(a, b):  
    expected = a + b  
    actual = func(a, b)  
    assert expected == actual  
  
test_func(1, 2)  
test_func(3, 4)
```

Below the code block, there is a blue icon for copying the code. Below the code block, there is a paragraph of text: "This code will call the function func(a,b) with two different sets of inputs and check that the output matches the expected result. If the output does not match, an AssertionError will be raised." At the bottom right of the text box, there are three icons: a share icon, a thumbs up icon, and a comment icon.

Using LLMs (Large Language Models)

LLMs don't know when it makes mistakes, so it should be considered as an exoskeleton



Conclusions

Over the next few years, we can anticipate a **significant shift** in the types of applications being developed, moving away from traditional statistical machine learning and **towards more sophisticated autonomous or semi-autonomous agents** that can automate testing activities

In order to effectively safeguard the valuable assets and intellectual property of OSAT and Fabless organizations, containment is necessary. **ACS** Real-time Data Infrastructure offers a highly secure containment system called **True Zero Trust™**

Through its innovative design, **ACS** real-time infrastructure establishes a cutting-edge paradigm that allows for the creation of **secure data highways** and paves the way for building novel applications with **enhanced security**

ADVANTEST®

Questions?



All Rights Reserved - ADVANTEST CORPORATION