Optimizing Your Data Strategy to Support Mission Partner Environments

C5 Cyber & IT Forum

Chad Mason – Senior Director, DoD

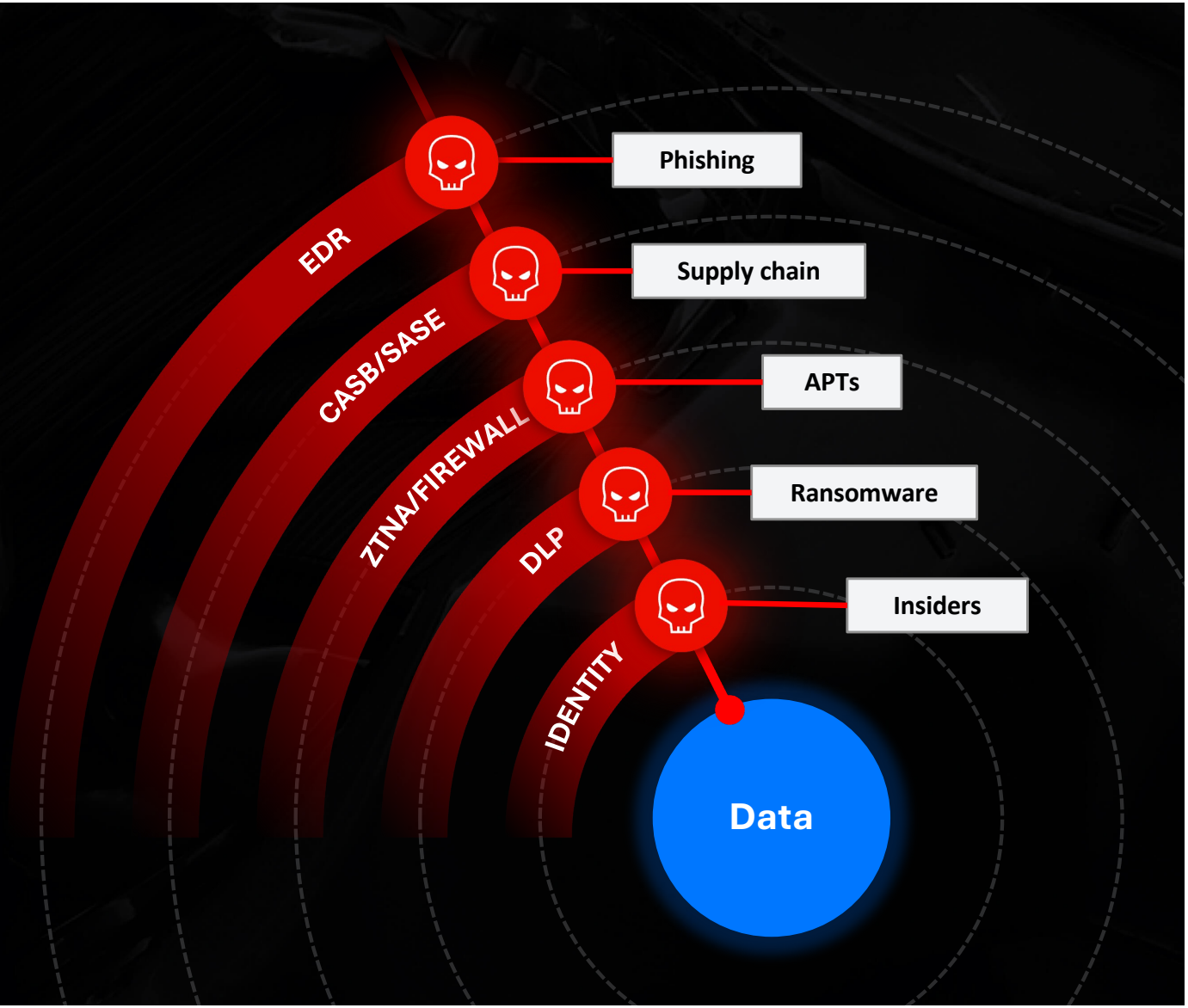
What problem are we solving?

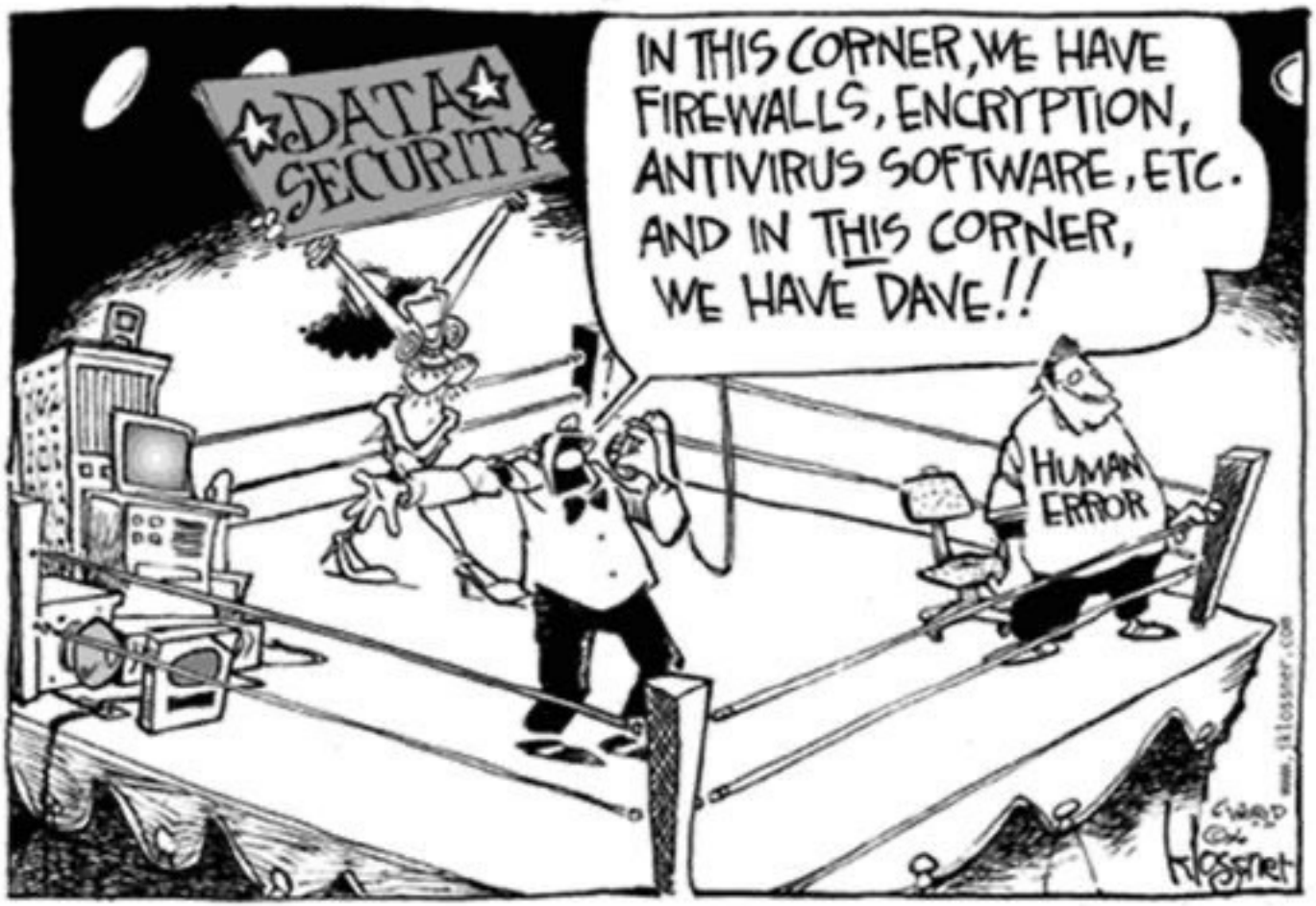

ARE YOU FEELING GUILTY ABOUT
THE KIDS WATCHING TOO MUCH TV?
JUST MUTE IT AND TURN CAPTIONS ON,
AND JUST LIKE THAT, THEY ARE READING
imgflip.com

It’s all about the data.

After our people, data is the most valuable and vulnerable asset.

Data is always the target.




DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR

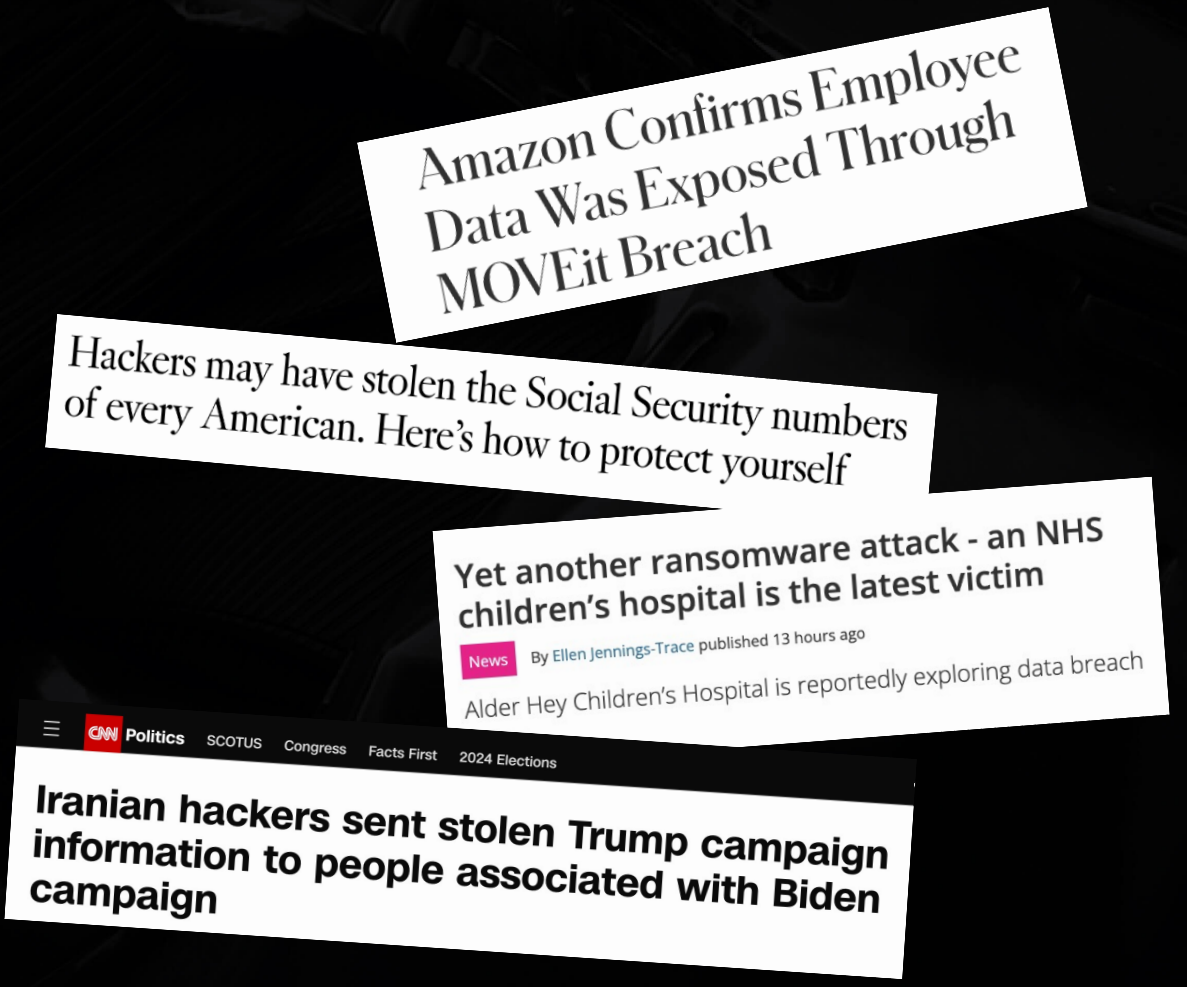
Attackers aren’t breaking in, they’re logging in.

86%

of data breaches involve stolen credentials

Source: Verizon DBIR

Data is where the damage happens.

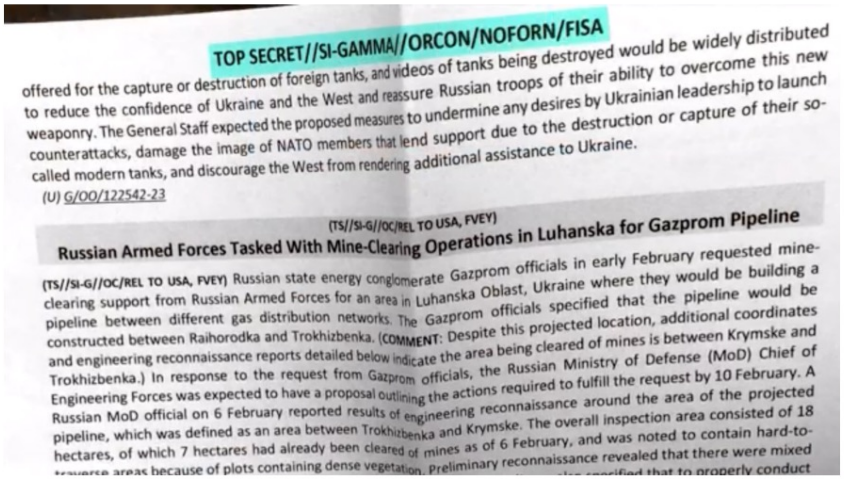


VARONIS

CNN politics

Audio Live TV Log In

Pentagon leak leads to limits on who gets access to military's top secrets



TOP SECRET//SI-GAMMA//ORCON/NOFORN/FISA

offered for the capture or destruction of foreign tanks, and videos of tanks being destroyed would be widely distributed to reduce the confidence of Ukraine and the West and reassure Russian troops of their ability to overcome this new weaponry. The General Staff expected the proposed measures to undermine any desires by Ukrainian leadership to launch counterattacks, damage the image of NATO members that lend support due to the destruction or capture of their so-called modern tanks, and discourage the West from rendering additional assistance to Ukraine.

(U) G/OO/122542-23

(TS//SI-G//OC/REL TO USA, FVEY)

Russian Armed Forces Tasked With Mine-Clearing Operations in Luhanska for Gazprom Pipeline

(TS//SI-G//OC/REL TO USA, FVEY) Russian state energy conglomerate Gazprom officials in early February requested mine-clearing support from Russian Armed Forces for an area in Luhanska Oblast, Ukraine where they would be building a pipeline between different gas distribution networks. The Gazprom officials specified that the pipeline would be constructed between Raihorodka and Trokhizbenka. (COMMENT: Despite this projected location, additional coordinates and engineering reconnaissance reports detailed below indicate the area being cleared of mines is between Krymske and Trokhizbenka.) In response to the request from Gazprom officials, the Russian Ministry of Defense (MoD) Chief of Engineering Forces was expected to have a proposal outlining the actions required to fulfill the request by 10 February. A Russian MoD official on 6 February reported results of engineering reconnaissance around the area of the projected pipeline, which was defined as an area between Trokhizbenka and Krymske. The overall inspection area consisted of 18 hectares, of which 7 hectares had already been cleared of mines as of 6 February, and was noted to contain hard-to-traverse areas because of plots containing dense vegetation. Preliminary reconnaissance revealed that there were mixed

Potentially deadly consequences from the Pentagon leak

CNBC

Search quotes, news & videos WATCHLIST | SIGN IN

MARKETS BUSINESS INVESTING TECH POLITICS CNBC TV INVESTING CLUB PRO

WORLD NEWS

America's allies 'can't trust us' after 'disaster' intelligence leak, former intel officers say

PUBLISHED FRI, APR 14 2023•9:50 AM EDT

Natasha Turak
@NATASHATURAK

Dan Murphy
@DAN_MURPHY

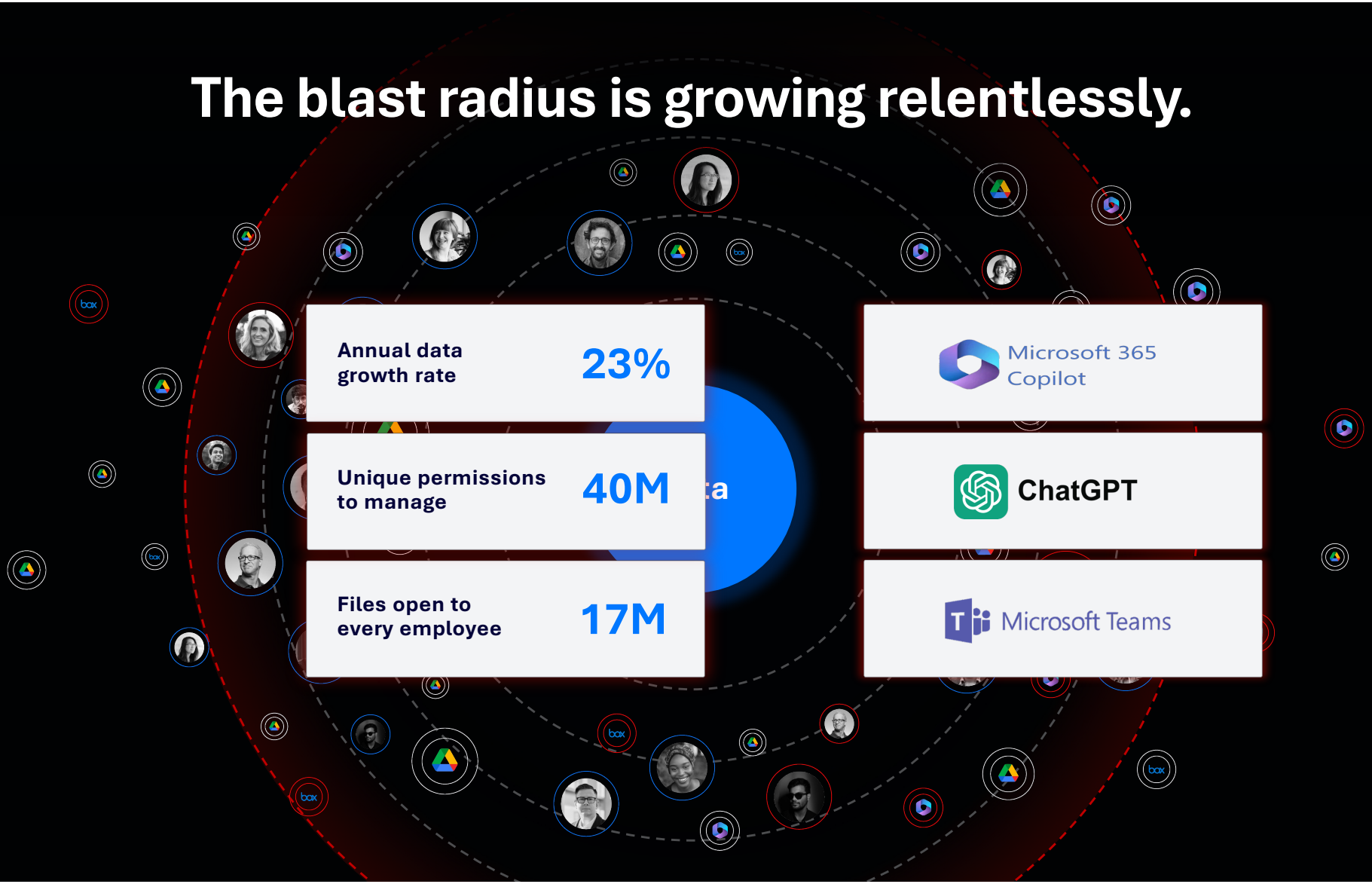
WATCH LIVE

KEY POINTS

- A leak of highly classified Pentagon documents has undermined trust among U.S. allies, former U.S. officials and intelligence experts tell CNBC.
- U.S. authorities on Thursday arrested 21-year-old Jack Teixeira, a low-ranking member of the Massachusetts Air National Guard, in connection with the investigation into the leak.
- America's control over its most valuable secrets has been thrust into question by the fallout from the most damaging intelligence leak since Edward Snowden's breach more than a decade ago,

VARONIS

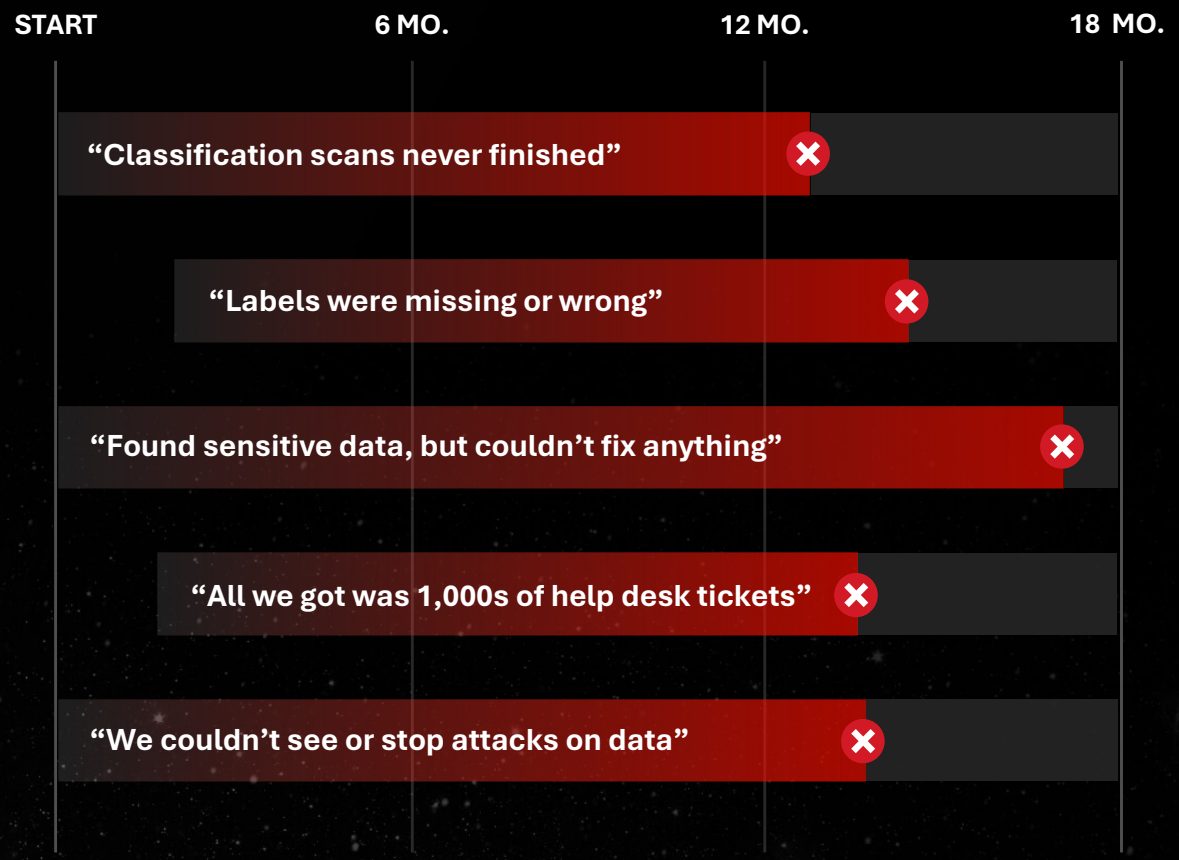
The blast radius is growing relentlessly.



Most approaches result in busywork followed by a breach.

“We spent 18 months struggling just to classify and label data with **no measurable outcome.**”

CISO, Large Federal Agency



VARONIS

Traditional ways to secure data

Native controls

Microsoft Purview
Built-in auditing
Built-in access controls

Point solutions

Classification tools
Privacy tools
Auditing tools

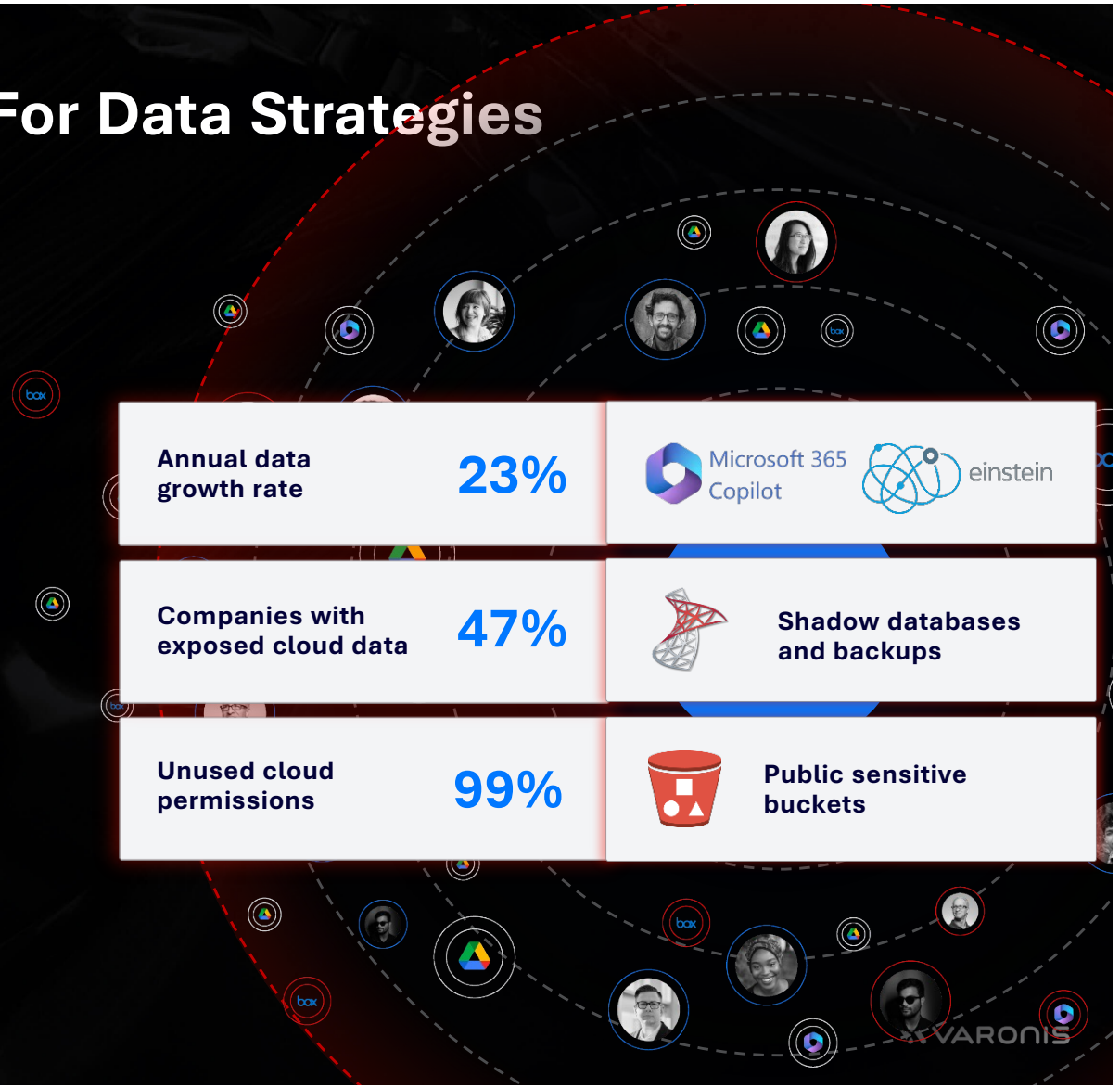
Legacy DLP

Manual labeling
Inline blocking
File-by-file remediation

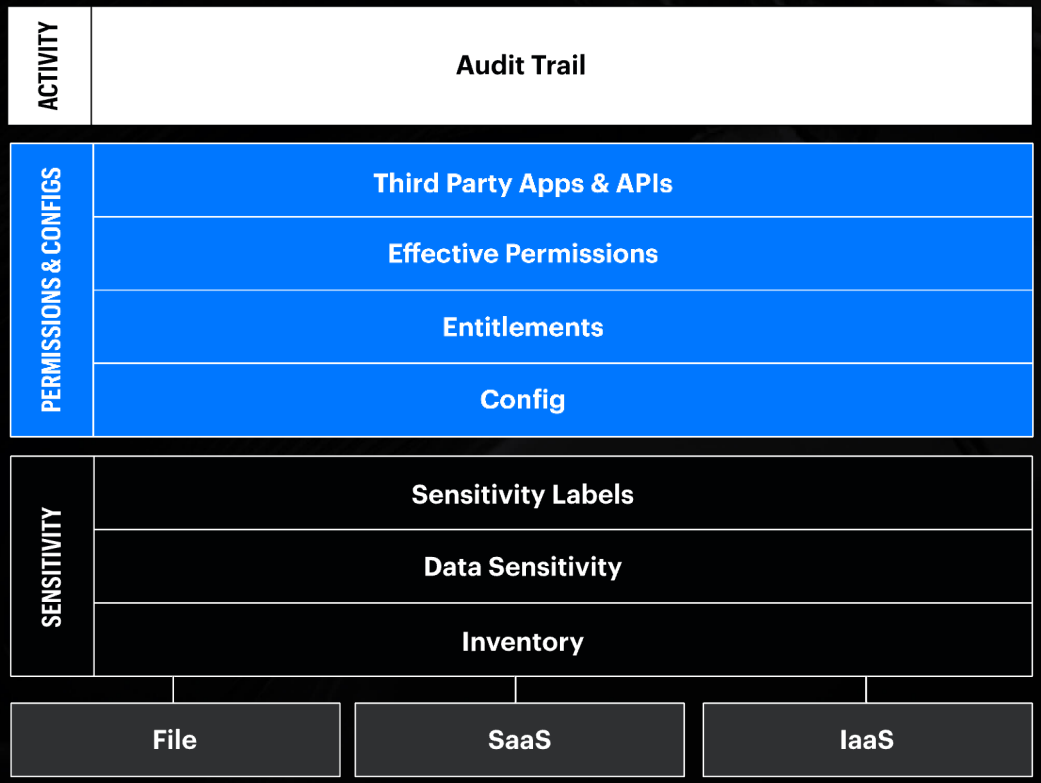
Fundamental Questions For Data Strategies

(And how long would it take?)

+ Can you define the data?
+ Can you secure the data?
+ Can you manage the data?
+ Do your Zero Trust policies extend to the data?
+ Can you detect and stop a data breach?
+ Can you automate the Find, Fix, Alert processes?



Do you have the telemetry to enforce your data strategy and policies?

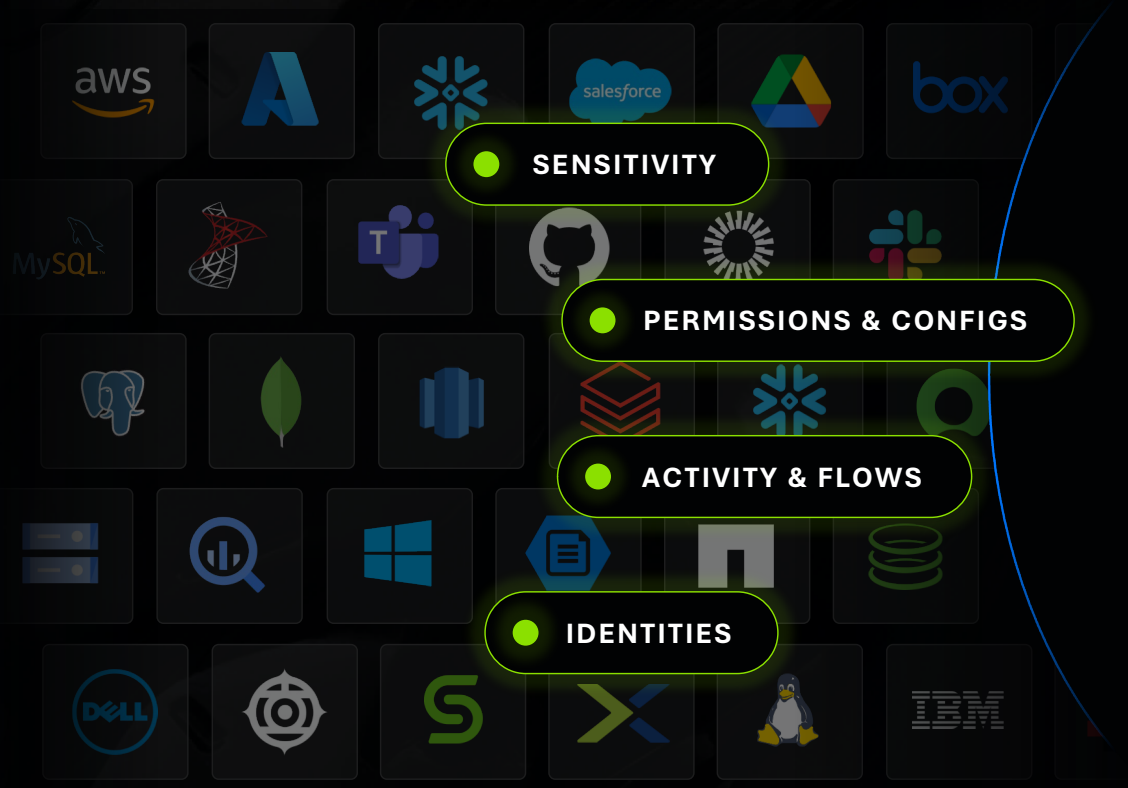


VARONIS

FIND

Real-time visibility

Understand your data security posture and activity in real-time.



Contextual

Understand exposure, usage, lineage, and business context.

Current

Know what's changed and created, so visibility is always up-to-date.

Complete

Full scans on huge data stores.
No blind spots.

VARONIS

FIX

Automated prevention

Continuously reduce your blast radius and auto-enforce policies.

Auto-enforce policies:

- Revoke excessive access
- Fix misconfigurations
- Apply labels
- Remove third-party apps
- Disable stale users
- Delete ROT data

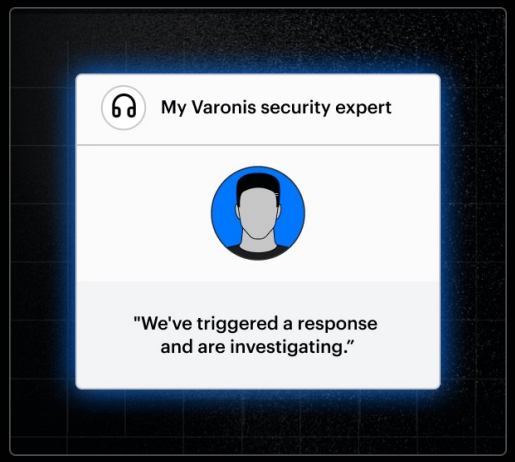
ALERT

Proactive detection

Always-on, data-centric UEBA for automated threat detection

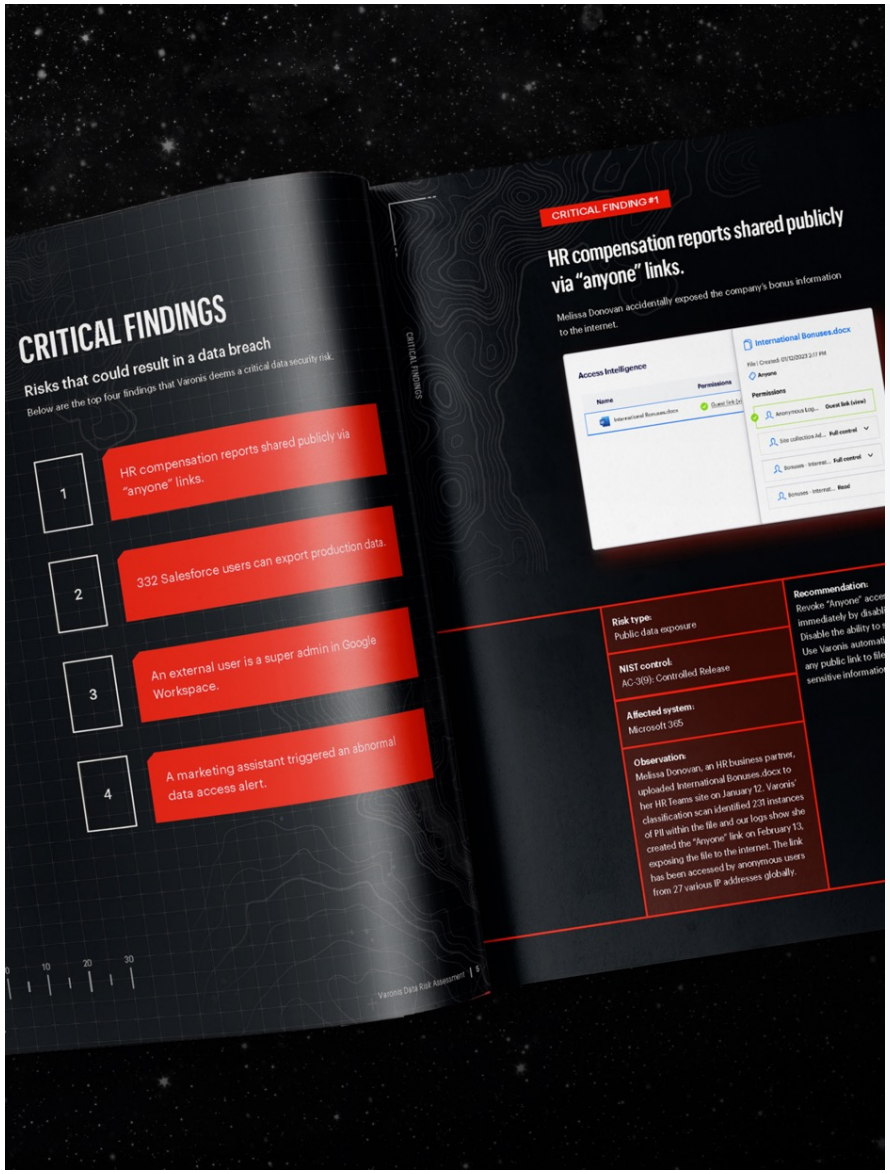
Monitor everything

Alerts generated in realtime



Fully integrated with your stack

VARONIS



Data Risk Assessment

- **Fast setup**
- **SaaS deployment**
- **Custom deliverable**

Find

+ Sensitive data across all data stores
+ Exposure levels and data usage
+ Potential impact of an attack

Fix

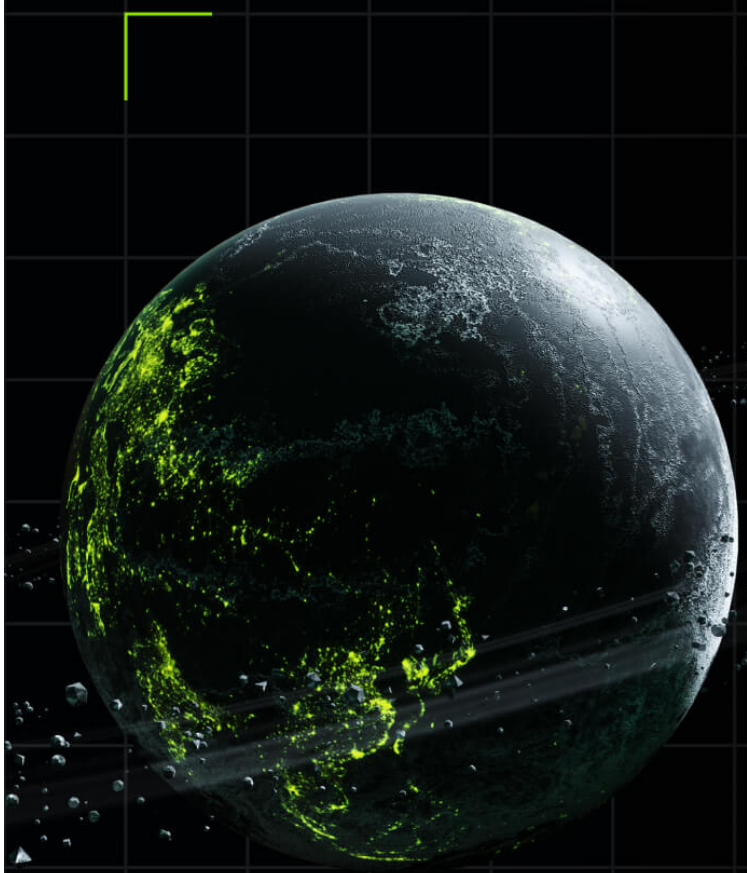
+ Public and org-wide data exposure
+ Risky identities and rogue third-party apps
+ Misconfigurations and compliance gaps

Alert

+ Real-time monitoring of data and identities
+ Unified and searchable forensics audit trail
+ Advanced UEBA + dedicated IR analyst

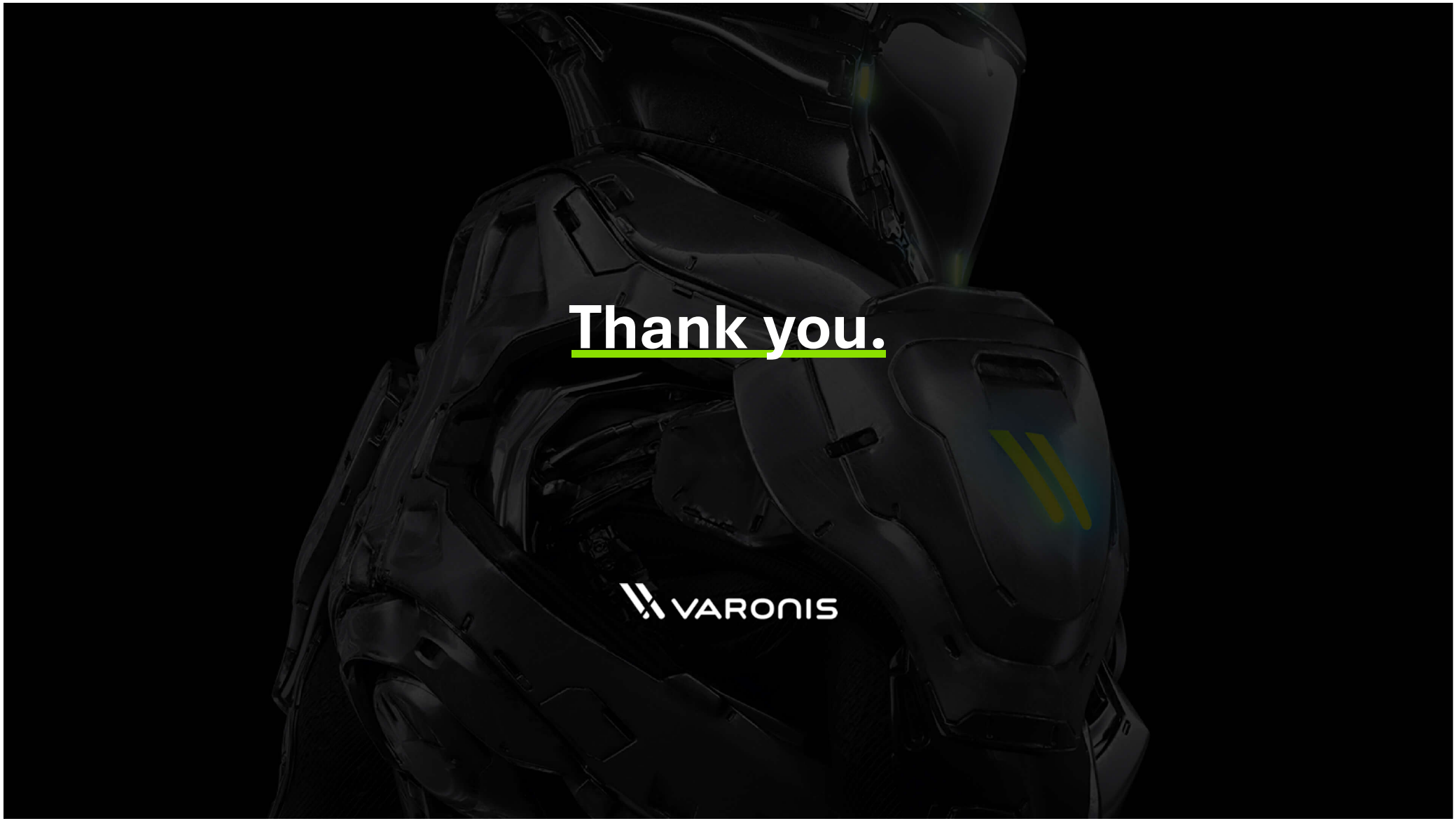
VARONIS

Optimized Data Strategy For Mission Partner Environments Summary



1. Discover sensitive data, categorize, label and map the data flows
2. Discover who has access to sensitive data
3. Identify user peacetime profiles and activity patterns to sensitive data – alert on deviations
4. Automate the Find, Fix, Alert and get to Outcomes
5. Operationalize data security outcomes into workflows

Automated Data Centric Approach


Thank you.
VARONIS