VARONIS

Is your data safe?

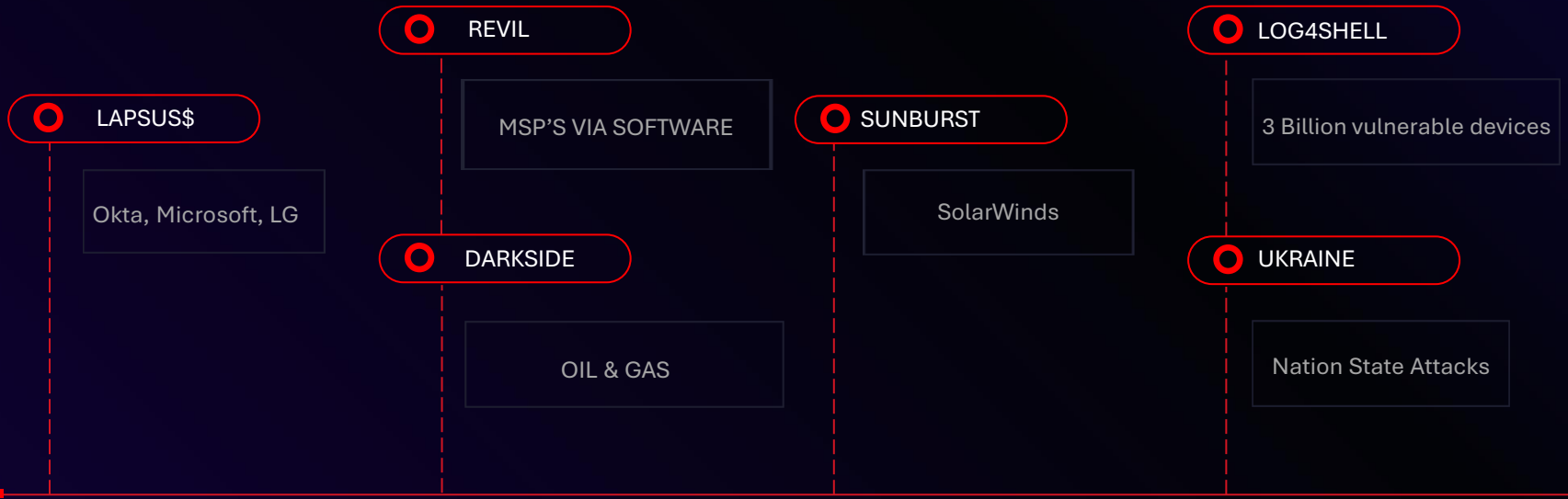
The why & how of building a data-first security program

October 2022


INCREASING
REGULATIONS
DATA
GROWTH
SOPHISTICATED
ATTACKERS
We've been watching the
SECULAR TRENDS for a
long time...

Technical
Scarcity

CYBERCRIME keeps getting worse



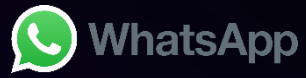
The threat landscape is ever changing...

VARONIS

REGULATIONS sharpened their teeth

FINE

€ 225,000,000



Country: Ireland
Authority: Data Protection Authority of Ireland
Date: 09/02/2021
Fine: €225,000,000
Organization Fined: WhatsApp
Article Violated: Art. 5 (1) a)
Type: Non-compliance with lawful basis for data processing

Summary: Facebook owned messaging app WhatsApp has been fined by the Data Protection Authority of Ireland with a huge sum of €225 million. This concludes an investigation spanning from 2018. The Data Protection Authority of Ireland commented that WhatsApp discharged its GDPR transparency obligations with regard to the provision of information and the transparency of that information to both users and non-users of WhatsApp's service. This includes information provided to data subjects about the processing of information between WhatsApp and other Facebook companies.

FINE

€ 746, 000, 000

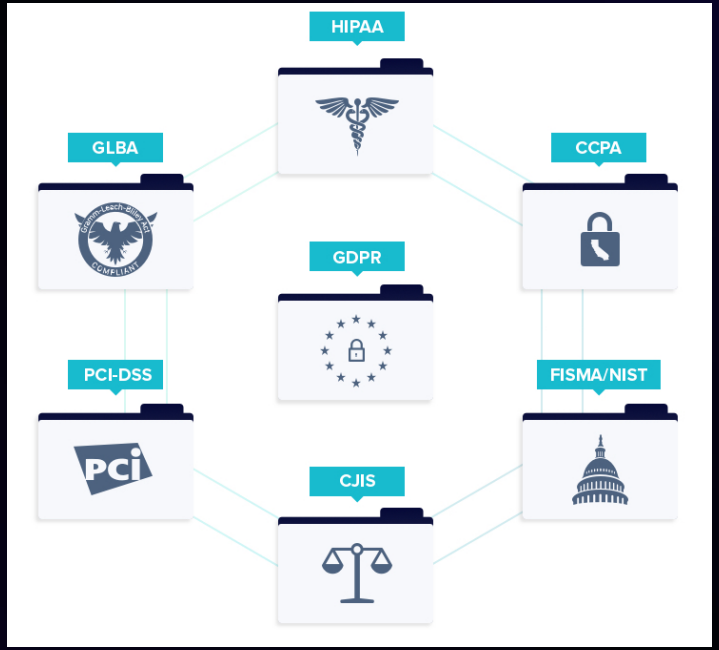
Country: Luxembourg
Authority: National Commission for Data Protection (CNPD)
Date: 07/22/2021
Fine: €746,000,000
Organization Fined: Amazon Europe Core S.a.r.l.
Article Violated: Several
Type: Failure to comply with data processing principles, and others

Summary: The DPA authority in Luxembourg fined Amazon Europe Core S.a.r.l. with EUR 746,000,000 ($887,000,000) because the US subsidiary did not process personal data according to the GDPR regulations. Apparently, Amazon Europe Core had misused its customer data for targeted advertising. But the company defends itself, saying that there was no data breach and at not time was customer data exposed to other unauthorized third parties. The fine enforced by the Luxembourg DPA came as a result of a 2018 complaint by French privacy rights group, La Quadrature du Net. They argued that Amazon, among other big companies, manipulate customers through targeted content and advertising. They further argued that this was against the principles or privacy and information freedoms of all Europeans. Whether Amazon's defense wins the case remains to be seen.

VARONIS

Modern regulations are data-centric

- Where is your regulated data located?
- Is any of that data exposed and at-risk?
- Do only the right people have access?
- How is regulated data being processed?
- Can you find and delete personal data?



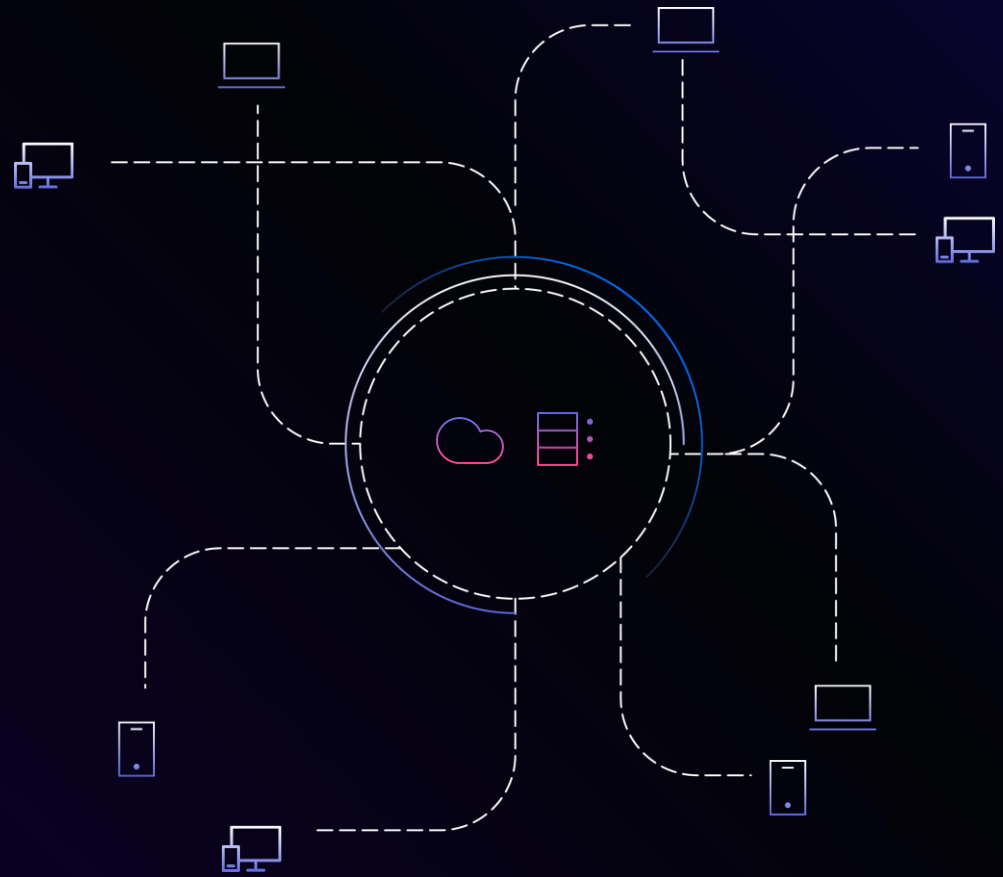
The Data-First Approach

VARONIS

Our world is more
RELIANT on data
than ever...

The security
PERIMETER is
harder to define

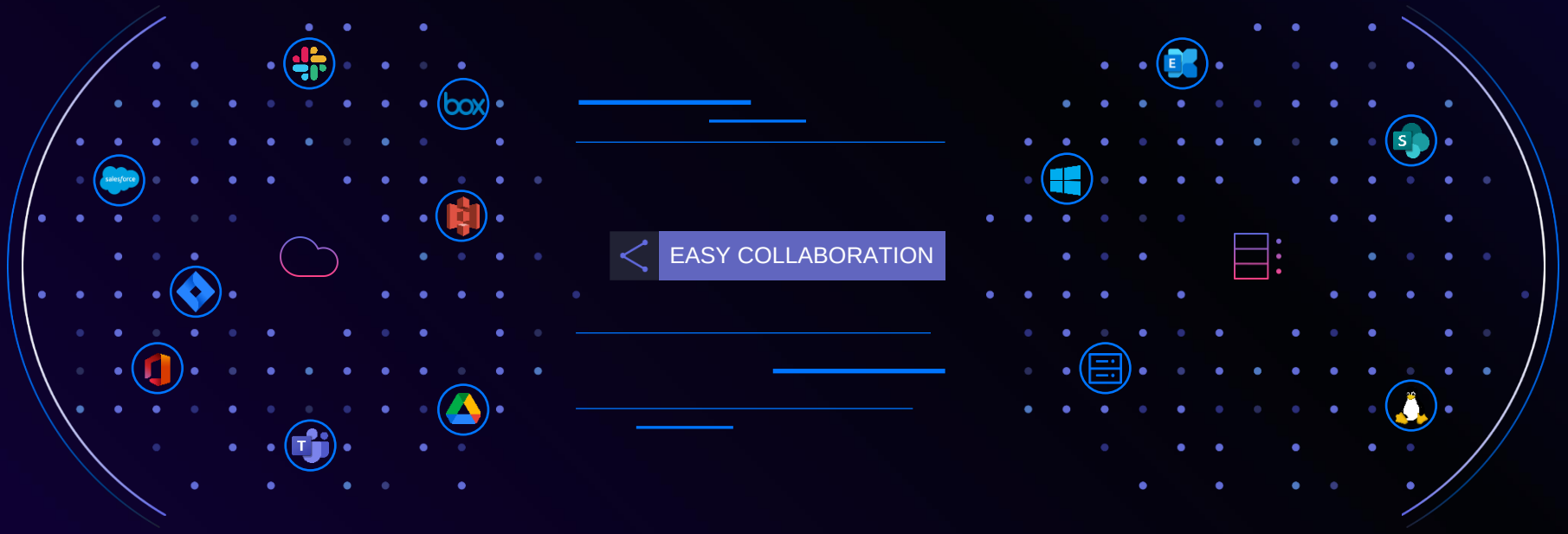
Endpoints are more like ACCESS points



Data GROWS in “sanctioned” data stores

VARONIS

They make
COLLABORATION EASY



VARONIS

And make
SECURITY HARD

17 MILLION

AVERAGE # OF FILES ACCESSIBLE
BY EVERY EMPLOYEE

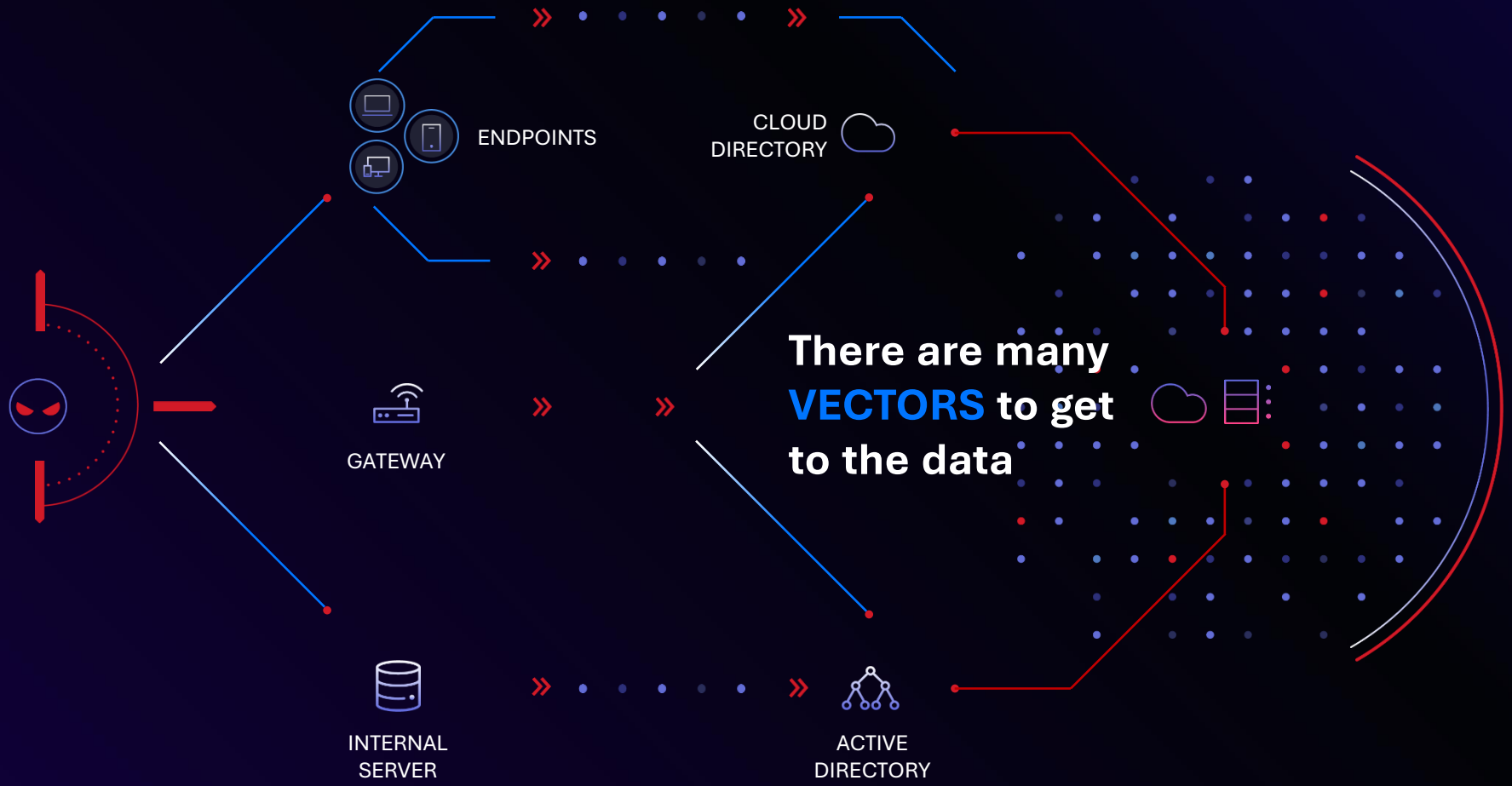
VARONIS

Where is the Team's data stored?

SharePoint Online

OneDrive

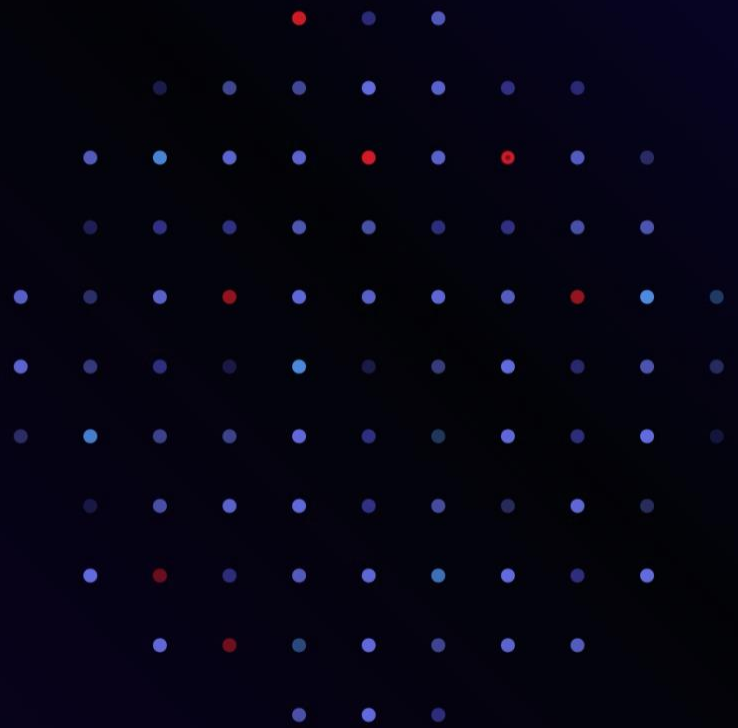
VARONIS


ENDPOINTS
CLOUD DIRECTORY
GATEWAY
There are many VECTORS to get to the data
INTERNAL SERVER
ACTIVE DIRECTORY

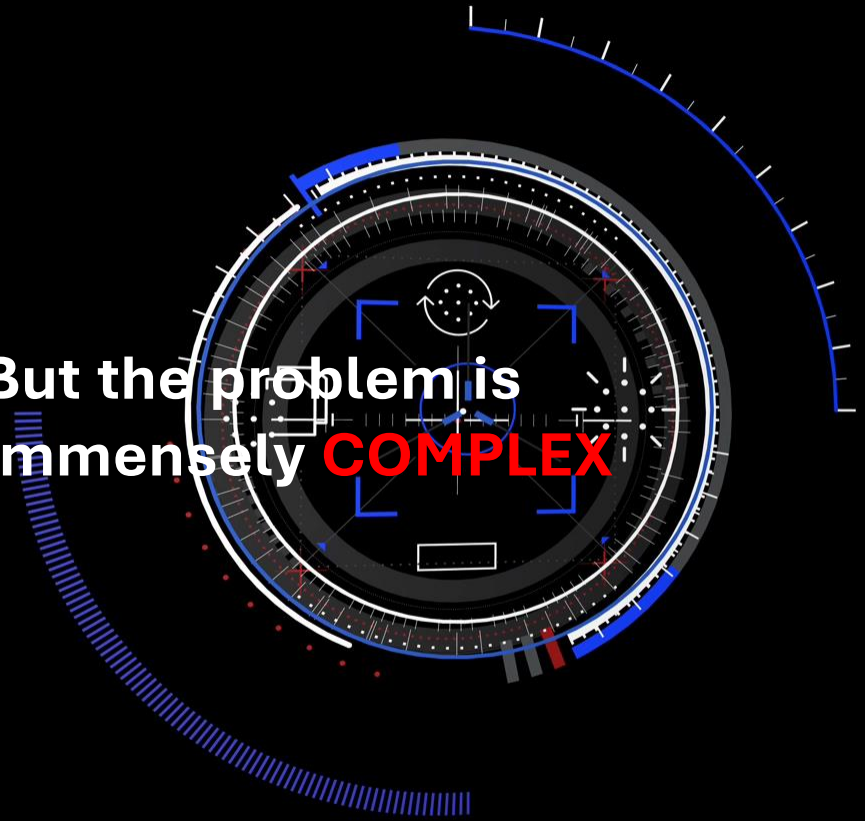
All it takes is ONE

VARONIS

But what happens
when security
STARTS WITH DATA?



It’s intuitively SIMPLE



But the problem is immensely COMPLEX

And the SCALE of the problem is hard for people to imagine

Consider a single Terabyte of data

- 1 million files, 50k folders
- 5% of folders with unique permissions
- Each unique folder with 3-5 groups


The CONTROLS are
closer to the asset

Reduce the BLAST RADIUS

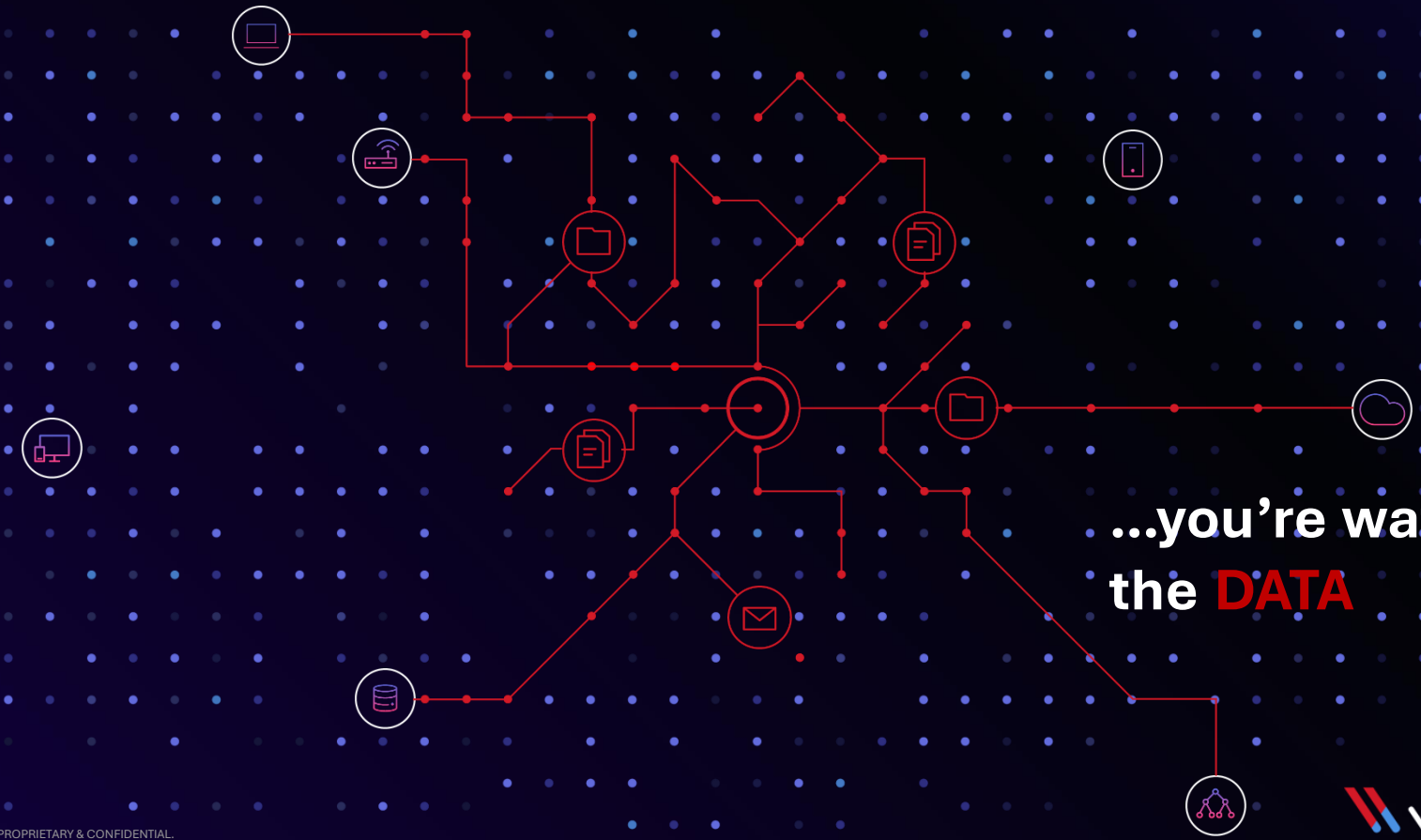
LESS ACCESS

REDUCE DAMAGE

SLOW ATTACKERS

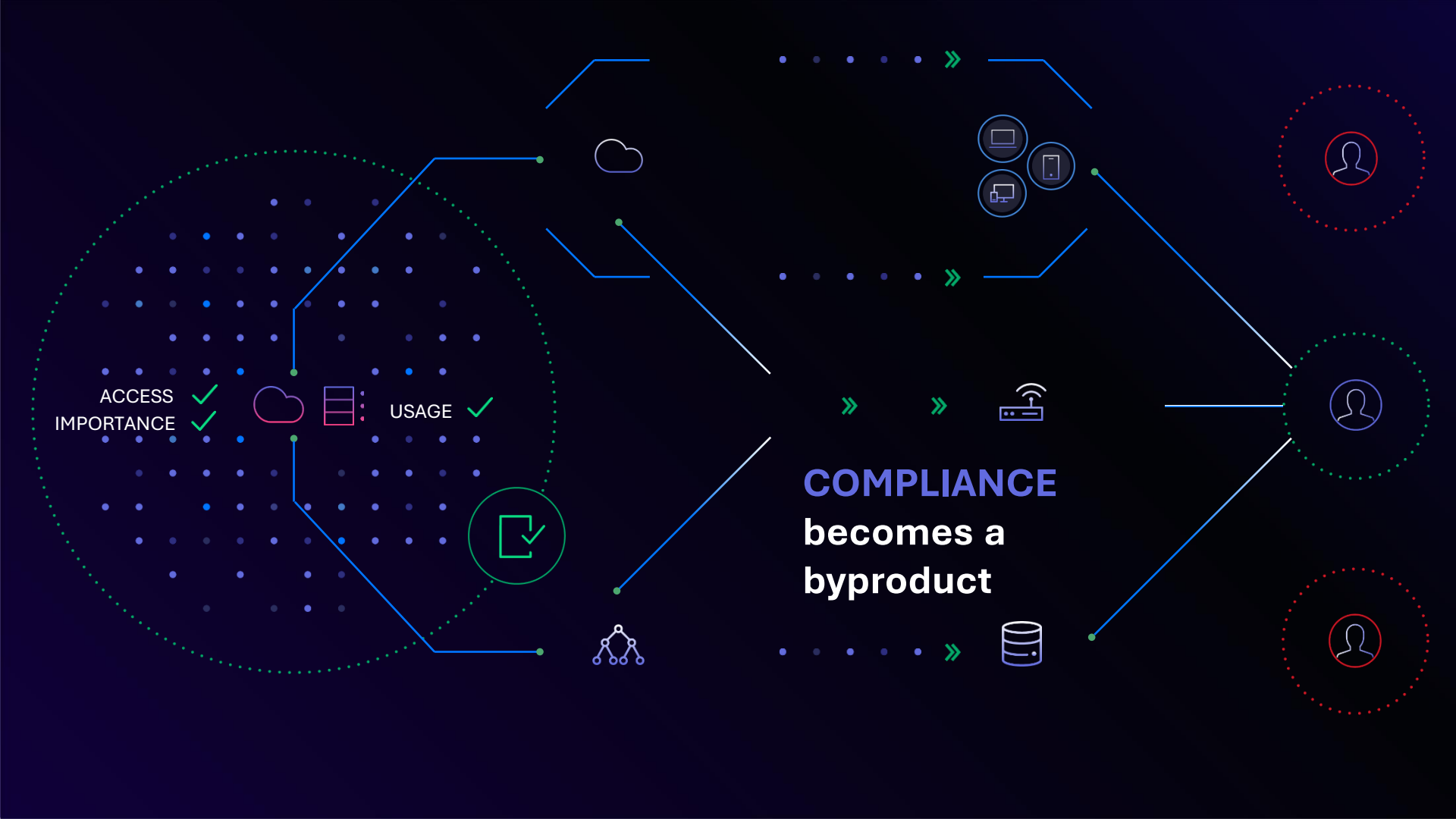
VARONIS

You CATCH what others miss because...



...you're watching the DATA

VARONIS


ACCESS
IMPORTANCE
USAGE
COMPLIANCE
becomes a
byproduct

Real life examples...

VARONIS


LAPSUS$

LAPSUS$ Reply

We recruit employees/insider at the following!!!!

- Any company providing Telecommunications (Claro, Telefonica, ATT, and other similar)
- Large software/gaming corporations (Microsoft, Apple, EA, IBM, and other similar)
- Callcenter/BPM (Atento, Teleperformance, and other similar)
- Server hosts (OVH, Locaweb, and other similar)

TO NOTE: WE ARE NOT LOOKING FOR DATA, WE ARE LOOKING FOR THE EMPLOYEE TO PROVIDE US A VPN OR CITRIX TO THE NETWORK, or some anydesk

If you are not sure if you are needed then send a DM and we will respond!!!!
If you are not a employee here but have access such as VPN or VDI then we are still interested!!

You will be paid if you would like. Contact us to discuss that

@lapsusjobs 837 37.2K 2:37 PM

NVIDIA, Samsung, LG, Ubisoft, EA

LAPSUS$

We hacked NVIDIA,

The hack is kinda public atm, and here's our announcement,

We were into nvidia systems for about a week, we fastly escalated to admin of a lot of systems.

We grabbed 1TB of data,
We grabbed the most important stuff, schematics, driver, firmware, etc...

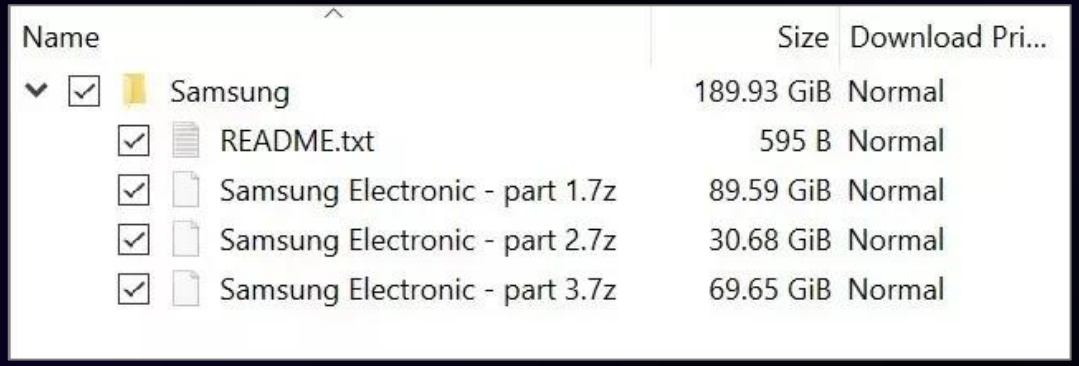
We are still waiting for nvidia to contact us.
We are also selling a full LHR V2 (GA102–GA104) –> we hope it will soon be removed by nvidia

If NVIDIA doesn't contact us, we will take actions.

Please note: We are not state sponsored and we are not in politics AT ALL.

Btw NVIDIA tried but failed, we have all the data.

614 edited 11:08 AM

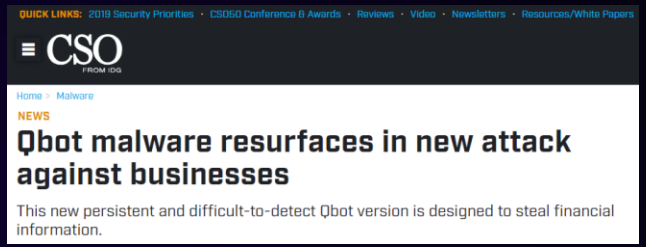


Russian APT Encounter

- Varonis alerted on malicious activity
- Well-known IR firm told customer there was no sign of compromise
- Customer called the Varonis IR team to be sure
- IR team
  - Discovered and contained infection in 13 minutes
  - IR began remediation, recovery, and forensics
- Research team
  - Reversed Qbot malware and exposed C2 server
  - Extracted victim list and found future variants

VARONIS

At Least 2,726 Victims Worldwide



VARONIS

How do you protect data from LAPSUS$ style threats?

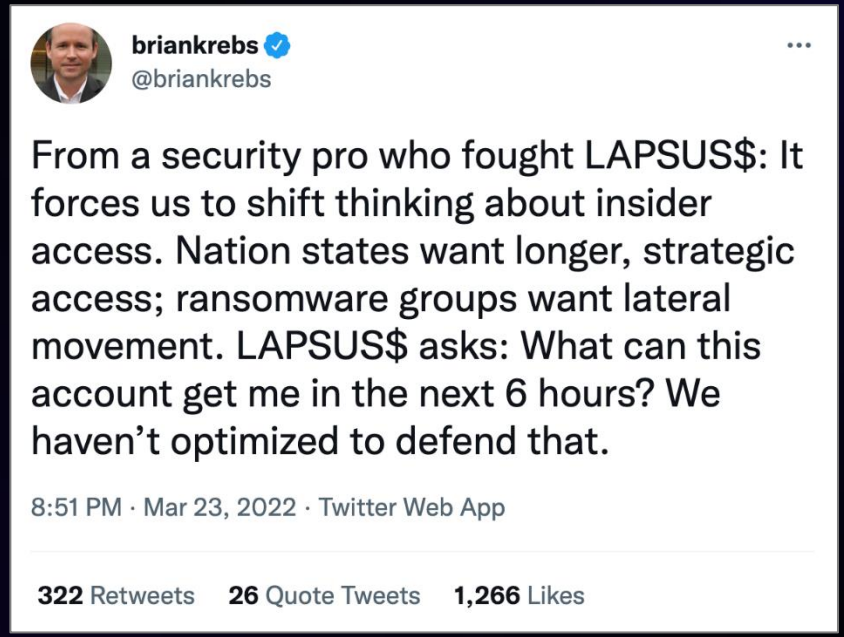
VARONIS

Know where your sensitive data is overexposed

VARONIS

Focus on global access first, then right-size

- Force attackers to gain privileged access in order to do meaningful damage
- Many attackers we see are looking for soft targets
  - “What can this account get me in the next 6 hours?”
- Hunt and eliminate “Everyone” group access on file shares and “Anyone” links in M365

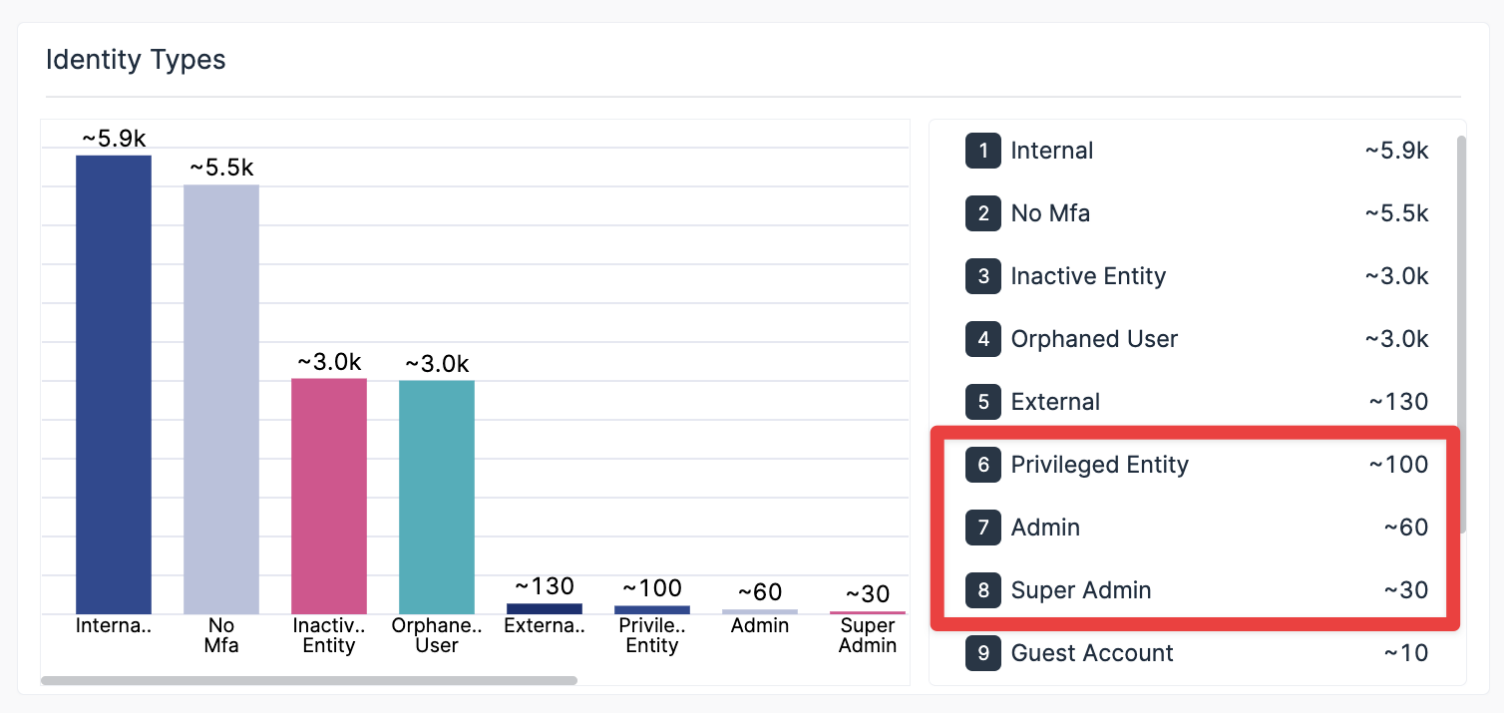


VARONIS

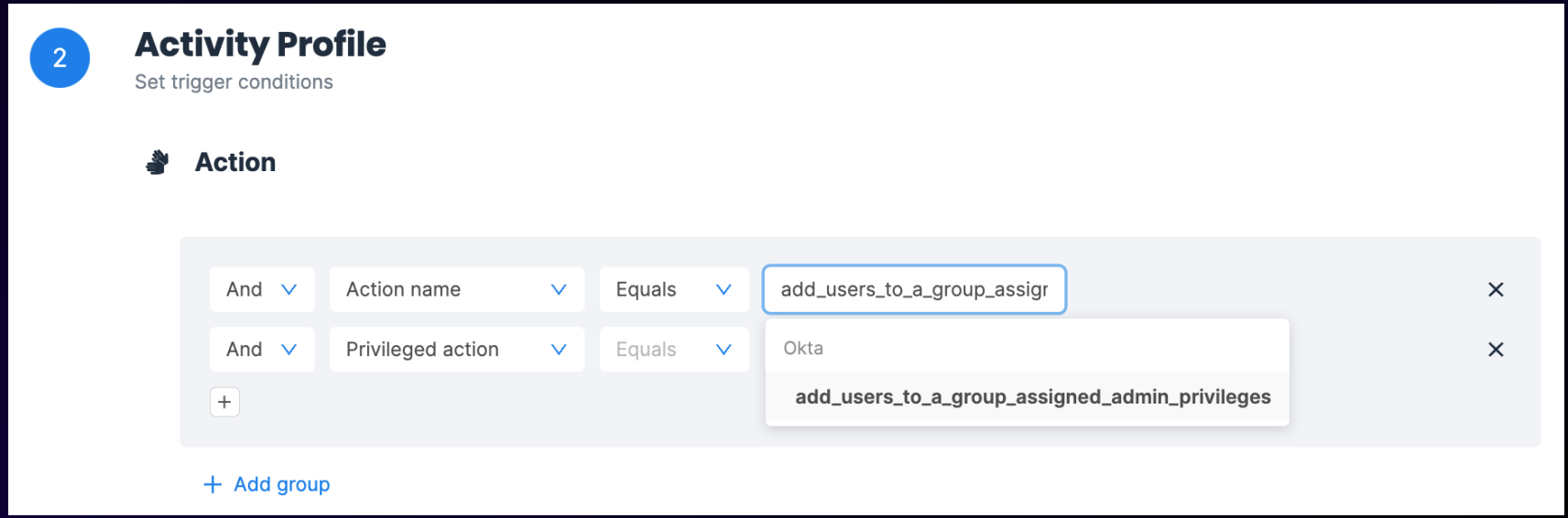
Classification helps you prioritize

2022-01-20 19:57:07	Mimikatz downloaded from hxxps://github.com by [SYSTEM NAME REDACTED]\[ACCOUNT NAME REDACTED]	Escalate Privileges
2022-01-20 20:58:31	RDP disconnect from [SYSTEM NAME REDACTED] by [SYSTEM NAME REDACTED]\[ACCOUNT NAME REDACTED]	Move Laterally
2022-01-20 23:02:41	First malicious logon by [ACCOUNT NAME REDACTED]@sykes[.]com to O365	Initial Compromise
2022-01-21 00:05:15	[ACCOUNT NAME REDACTED]@sykes[.]com accessed hxxps://[INTERNAL URL REDACTED]/personal/[INTERNAL USER NAME REDACTED]/Documents/Projects/ryk/DomAdmins-LastPass.xlsx via SecureLink	Internal Recon

Quick win: start with super admins and privileged accounts

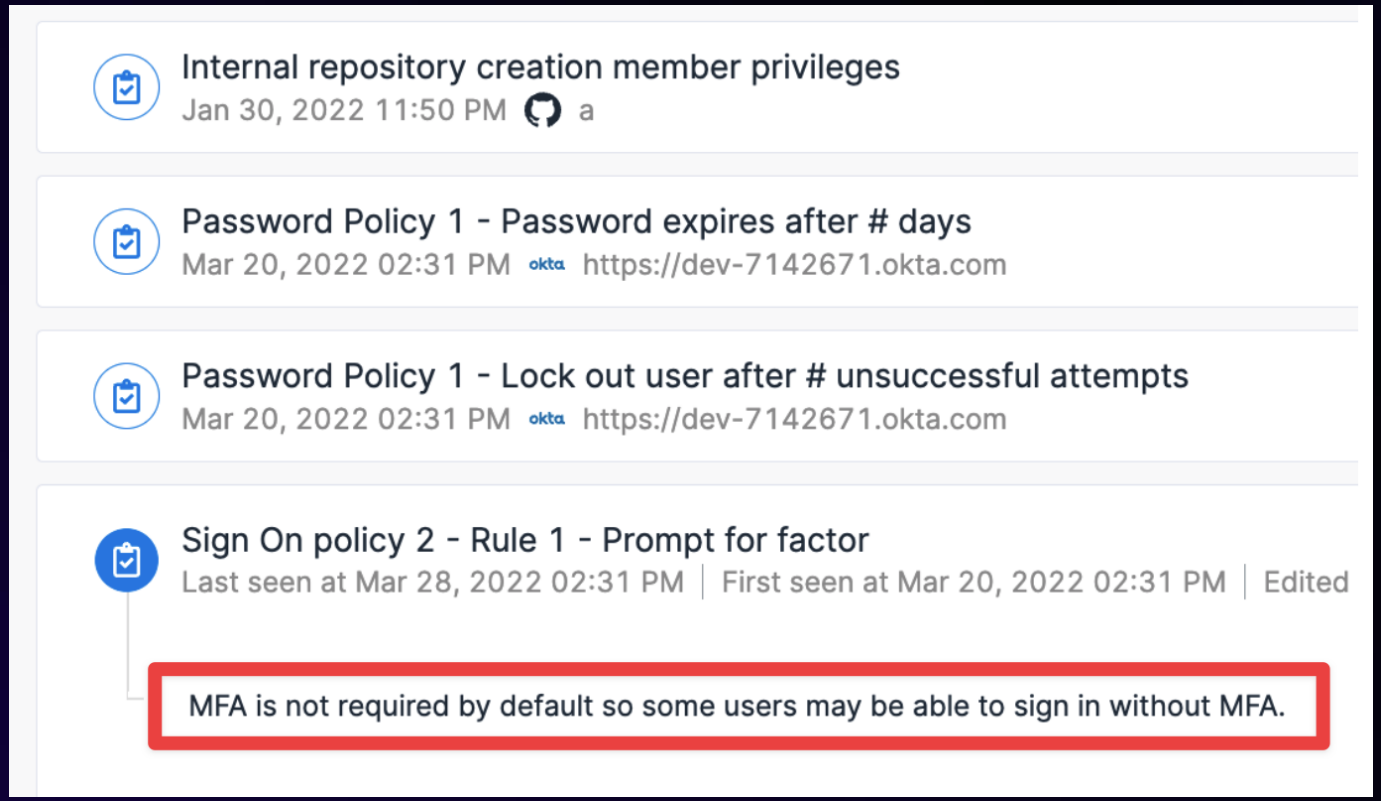


50% of security leaders said they don’t get an alert when someone is given super admin privileges



VARONIS

Identify org-wide misconfigurations and exposures



VARONIS

Focus on user behavior, not just static IOCs

- When a user accesses or downloads an abnormal amount of sensitive data
- When sensitive data is shared publicly
- If a user logs in from an unusual or blacklisted country.
- If MFA has been disabled
- Excessive password/MFA reset requests
- If a contractor or stale account becomes active after a long period of inactivity

VARONIS

Key Takeaways

- Data growth, increased regulation
- If you assume compromise, protecting data should be a priority
- Sophisticated insiders and external attackers can evade detection
- Defenders should seek to reduce uncertainty with visibility and context
- Combining the right ingredients can reduce Time To Detection / Time To Response and help you answer: “Is our data safe?”
- Risk assessments are a great first step in reducing uncertainty

VARONIS

Thank you

Bradley Bosher

Senior Systems Engineer

bbosher@varonis.com