Harnessing AI For Data Security

A Guide To Proactive Risk Management

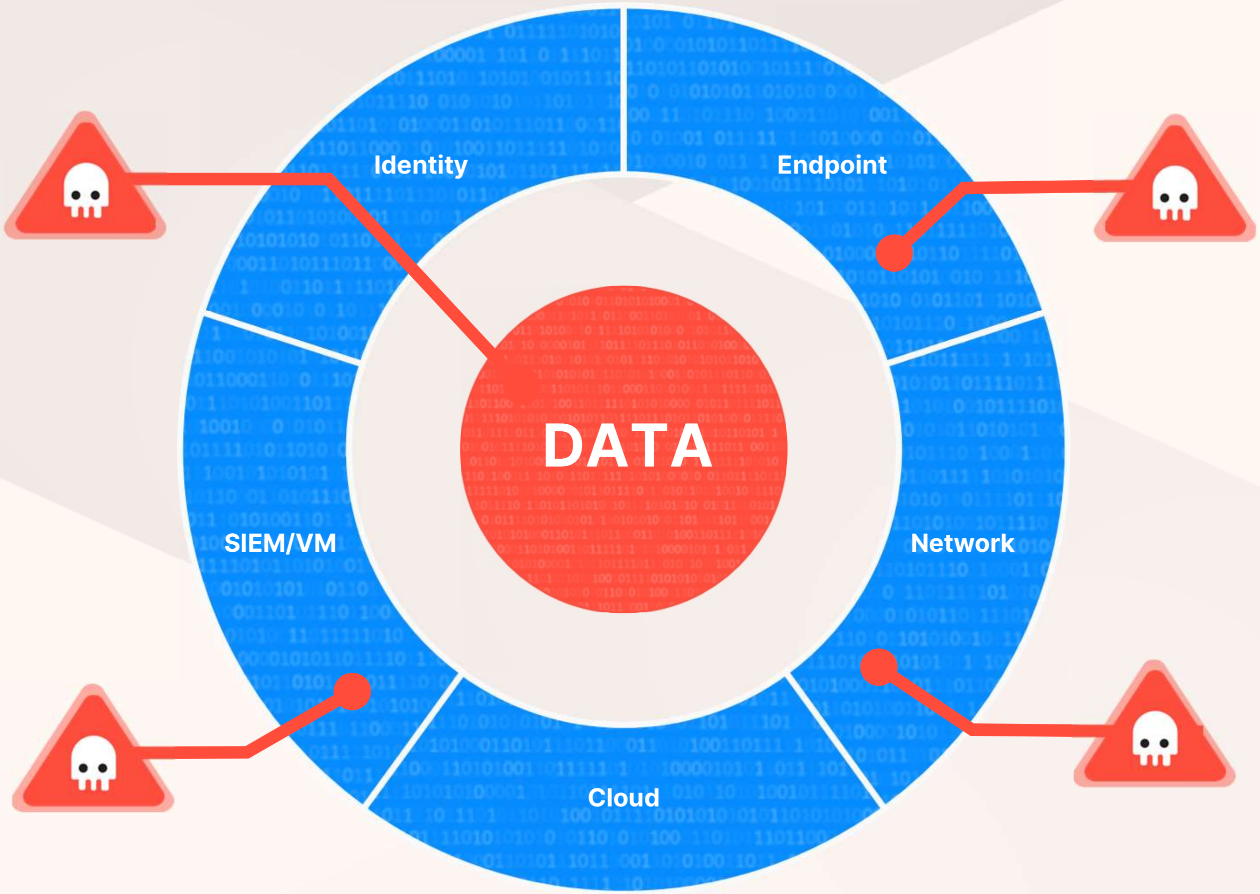
Frank Schwaak

Field CTO EMEA @Rubrik

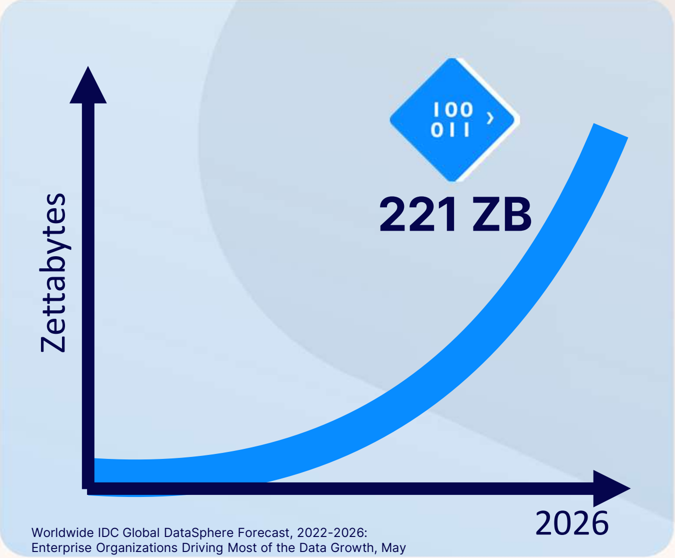
April 2024

The Situation

DATA REMAINS AT RISK

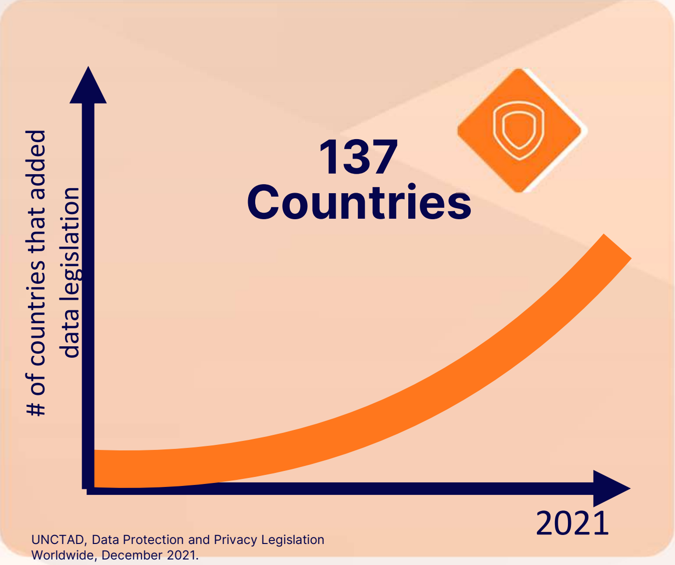


WHILE…



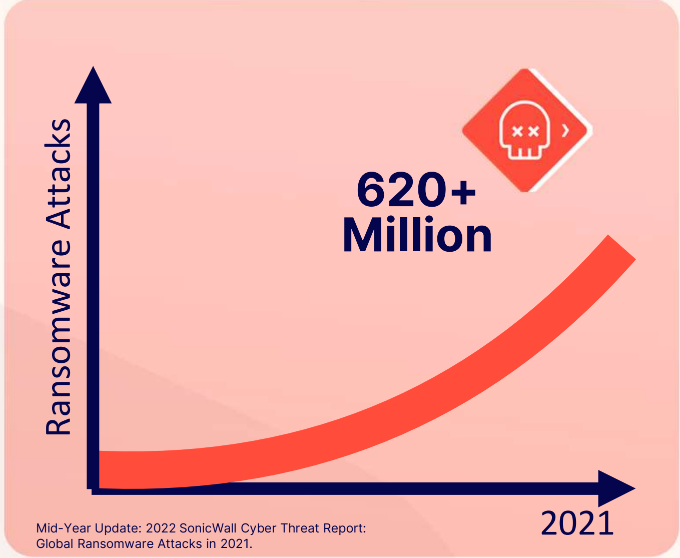
Worldwide IDC Global DataSphere Forecast, 2022-2026: Enterprise Organizations Driving Most of the Data Growth, May 2022.

DATA IS EXPLODING



UNCTAD, Data Protection and Privacy Legislation Worldwide, December 2021.

DATA REGULATIONS ARE EXPLODING



Mid-Year Update: 2022 SonicWall Cyber Threat Report: Global Ransomware Attacks in 2021.

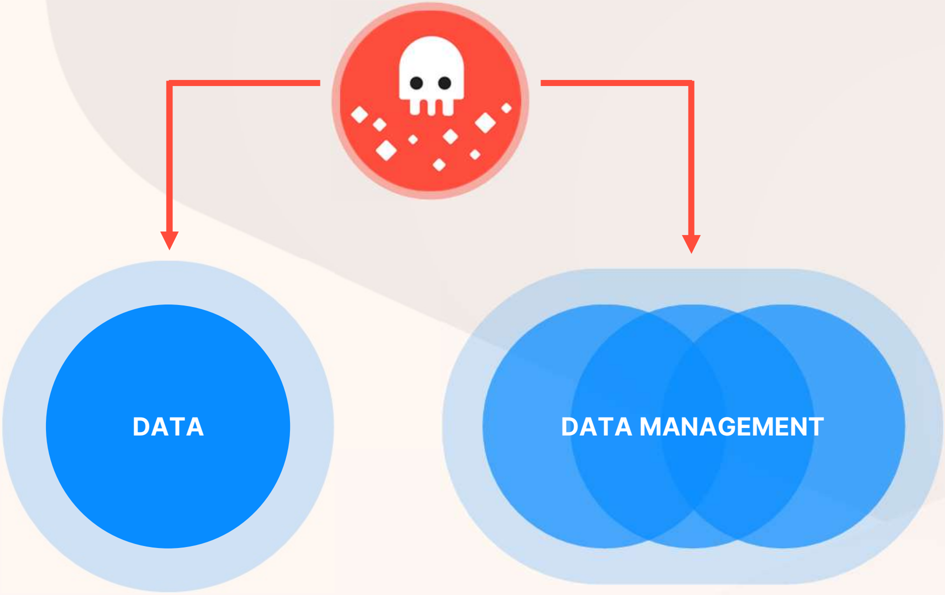
DATA ATTACKS ARE EXPLODING

RANSOMWARE ATTACKS WILL STRIKE EVERY 2 SECONDS WITHIN THE NEXT 10 YEARS

Cybersecurity Ventures, Ransomware Will Strike Every 2 Seconds by 2031 (September 2022).

DATA SECURITY IS SLIPPING THROUGH THE CRACKS

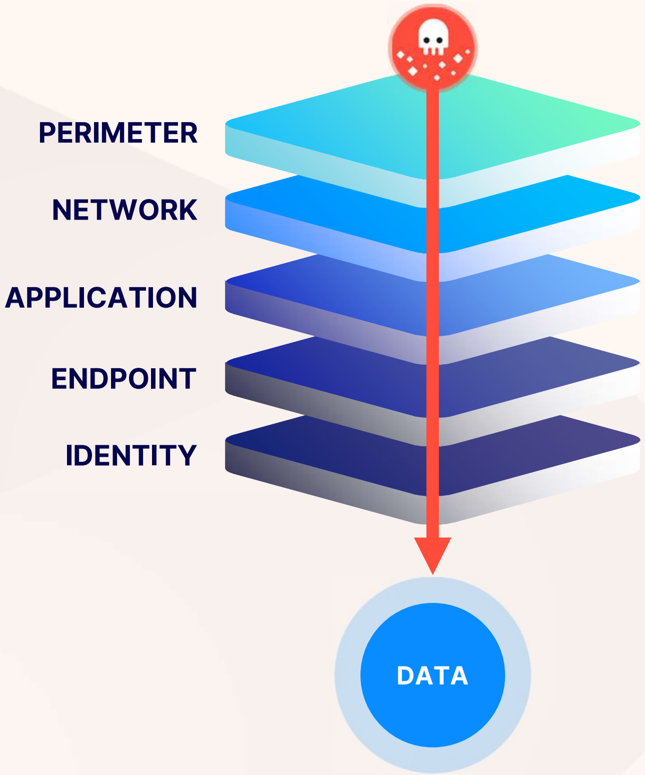
LEGACY BACKUP & RECOVERY APPROACH



DATA

DATA MANAGEMENT

TRADITIONAL CYBERSECURITY APPROACH



PERIMETER

NETWORK

APPLICATION

ENDPOINT

IDENTITY

DATA

BSI Lagebericht - November 2023

“Einen vollständigen Schutz vor Ransomware-Angriffen gibt es nicht, …“

Die Lage der IT-Sicherheit in Deutschland 2023

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•

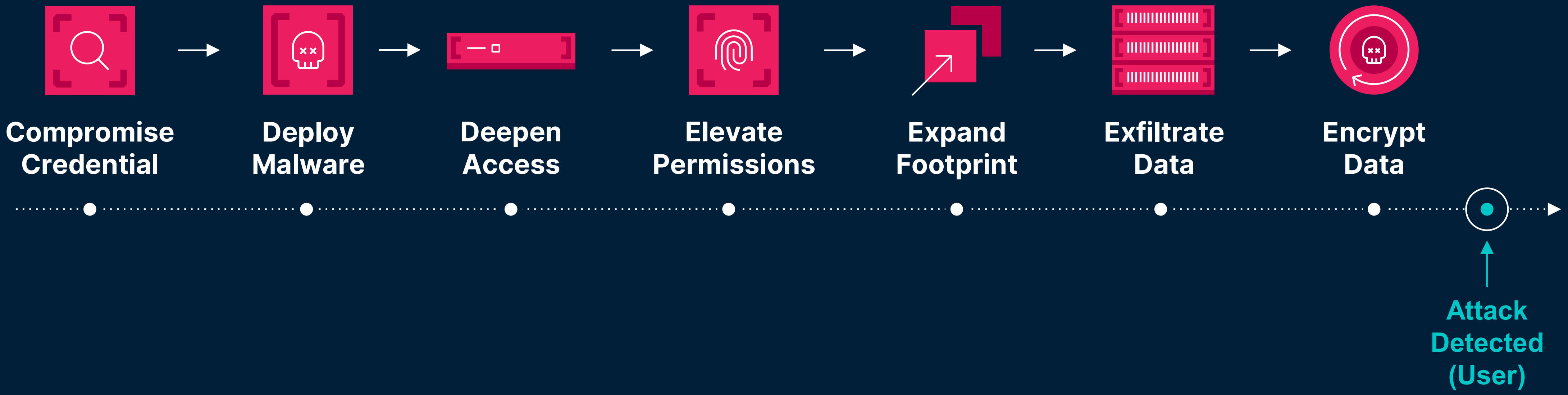
… denn Angreifer können auch neue Angriffswege nutzen, für die noch **keine Detektions- und Abwehrmethoden entwickelt wurden**. Bestimmte Angriffe zum Beispiel auf Unternehmen, Behörden und IT-Dienstleister können aber durchaus auch verhindert werden. **Backups und Notfallpläne unterstützen dabei, die Auswirkungen im Ernstfall zu begrenzen oder sogar vollständig zu kompensieren**.

https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

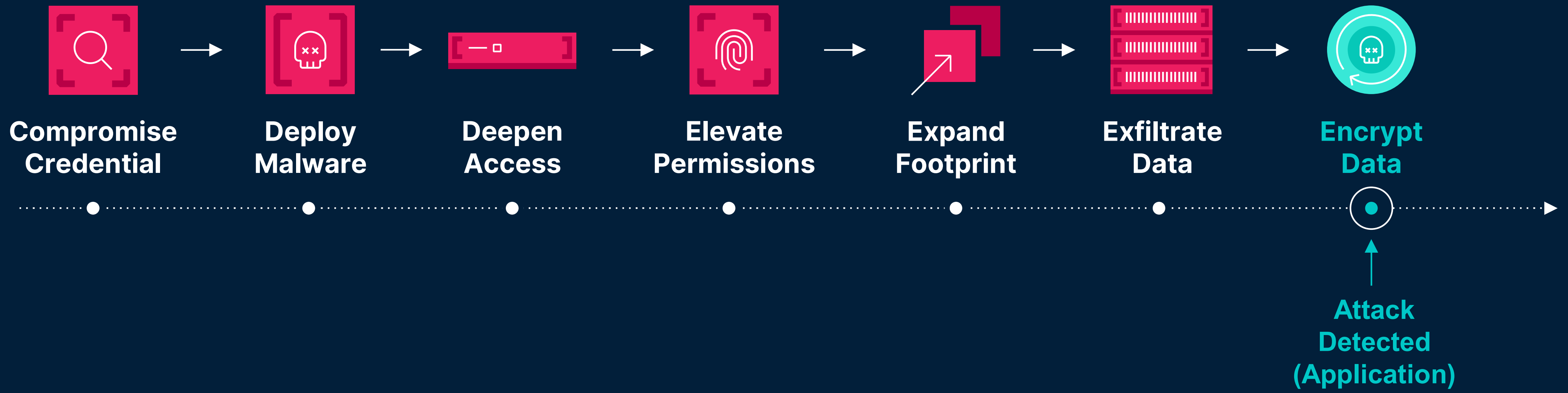
Hackers aren’t breaking in…

They’re logging in.

Anatomy of a Zero Day Cyber Attack



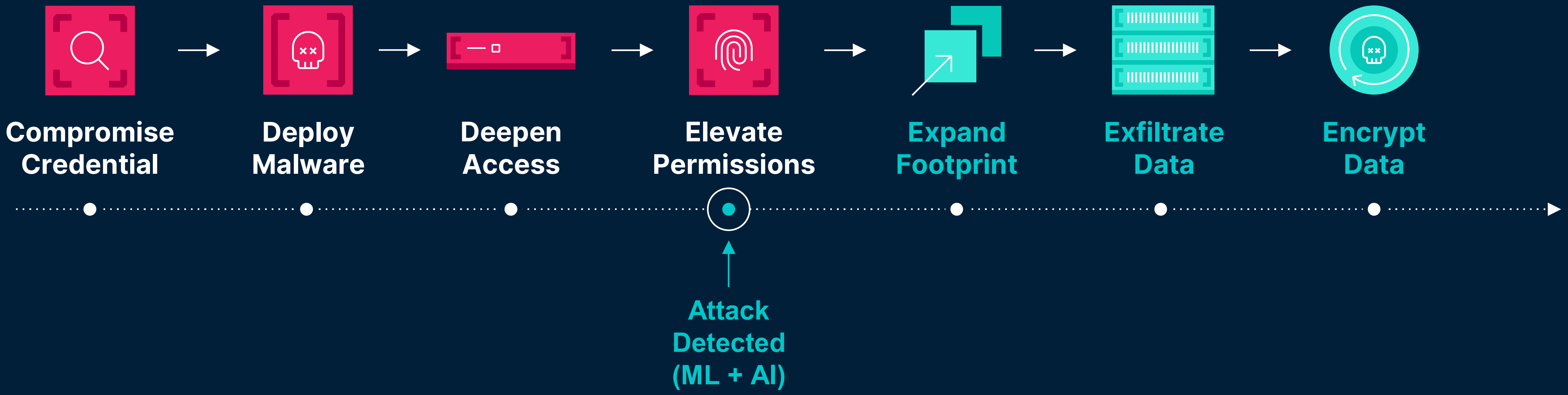
Anatomy of a Zero Day Cyber Attack



Compromise Credential → Deploy Malware → Deepen Access → Elevate Permissions → Expand Footprint → Exfiltrate Data → Encrypt Data

Attack Detected (Application)

Imagine you could detect it sooner



Compromise Credential → Deploy Malware → Deepen Access → Elevate Permissions → Expand Footprint → Exfiltrate Data → Encrypt Data

Attack Detected (ML + AI)

True Cyber Resilience

Cyber Resilience

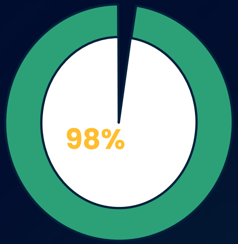
Users

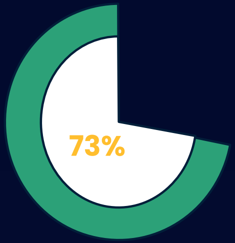
Data

Zero Labs Results

The future of data security

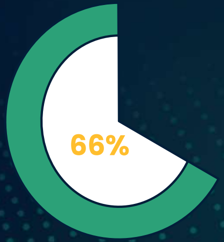
- 98% of external organizations believe they currently have significant data visibility challenges

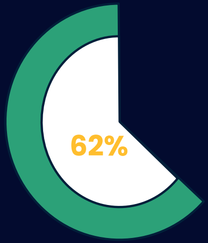




- A typical global organization's data is growing by 73% in the cloud over the last 18 months

- 66% of Security leaders believe their data growth has already outpaced their ability to secure data and manage risk





- 62% of external organizations believe employees are accessing data in violation of established data policies rubrik | Zero Trust Data Security™

AI & The Threat Landscape

Understanding the risks

The Threat Landscape

Generative AI Based Threats

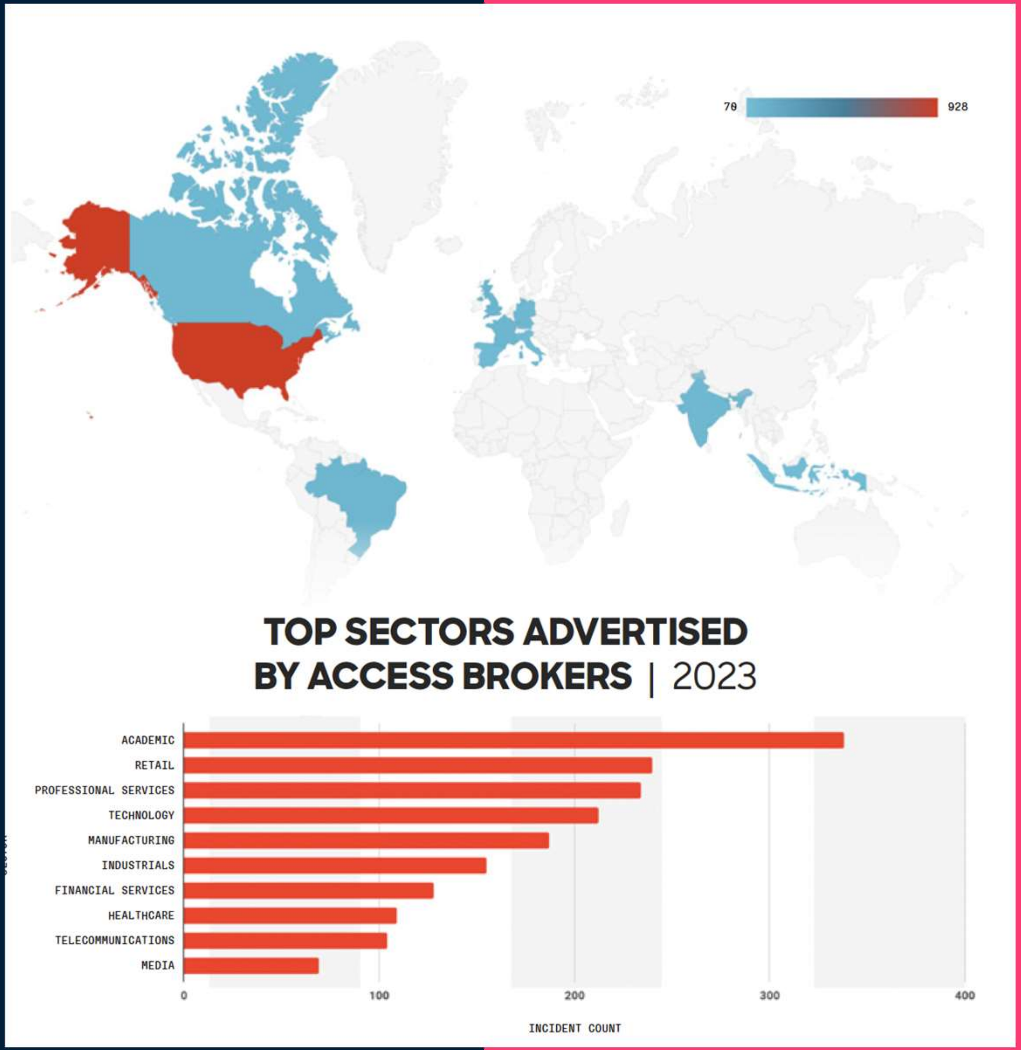
- GenAI now actively used in malware production
  - FraudGPT, WormGPT & OPWNAI

App, Credentials & Zero Day Attacks

- A **Cyberattack** occurred every **29seconds in 2023**(1)
- **Exploited vulnerabilities** led to 36% ransomware attacks in 2023 with **28778 CVEs in 2023** (2)

Data Breach Statistics

- **Average** Data Breach cost @ $4.45m (3)
- Average cost of a ransomware attack 2023 **USD $1.85 million**(4)



TOP SECTORS ADVERTISED BY ACCESS BROKERS | 2023

Cybersecurity Skills Shortage Increases Downtime

71%

of organizations have a cyber security skills shortage[1]

60%

of attacks occur at the hypervisor rendering recovery plans & tooling obsolete[2]

22

days is the average time it takes to recover from ransomware[3]

[1] Enterprise Strategy Group: The Life and Times of Cybersecurity Professionals, Volume VI, 2023

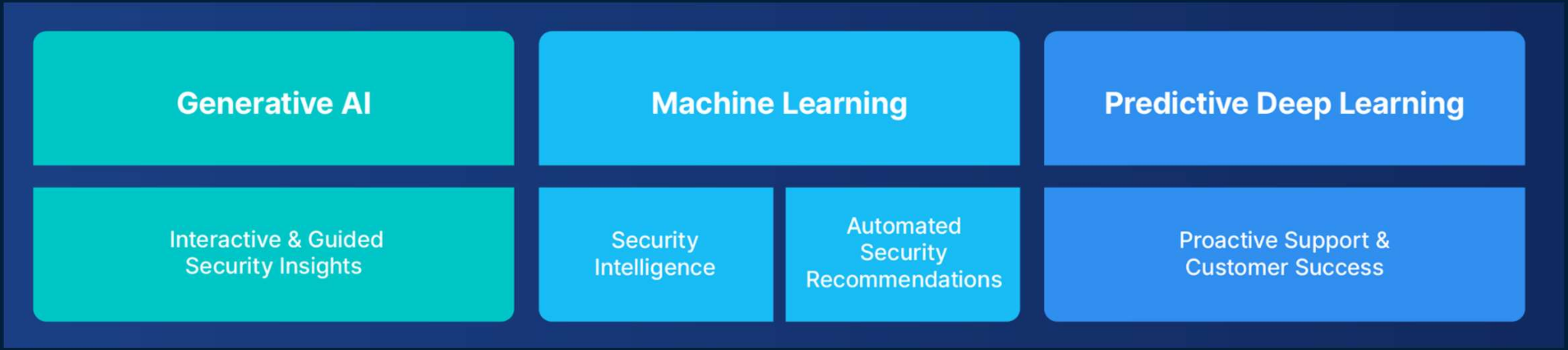
[2] Rubrik Ransomware Response Team, Nov 2023

[3] Statista: Length of impact after a ransomware attack worldwide, Q2 2022

Maturing Cyber Security & Resilience

Leveraging AI effectively to manage risk

AI used for Data Security & Cyber Resilience



Generative AI

Interactive & Guided Security Insights

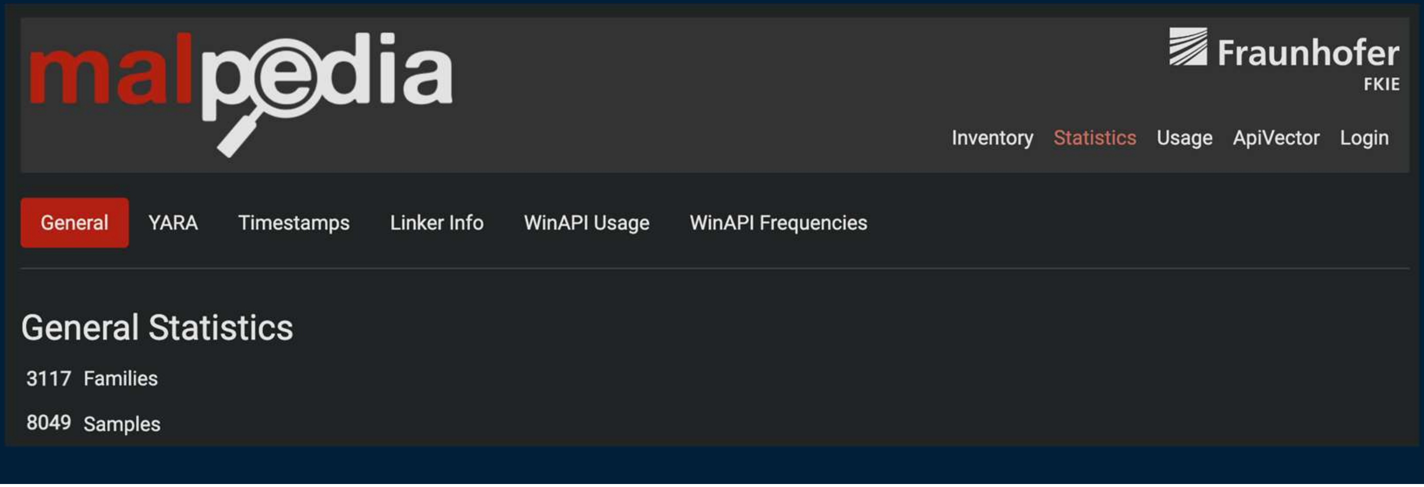
Machine Learning

Security Intelligence

Automated Security Recommendations

Predictive Deep Learning

Proactive Support & Customer Success



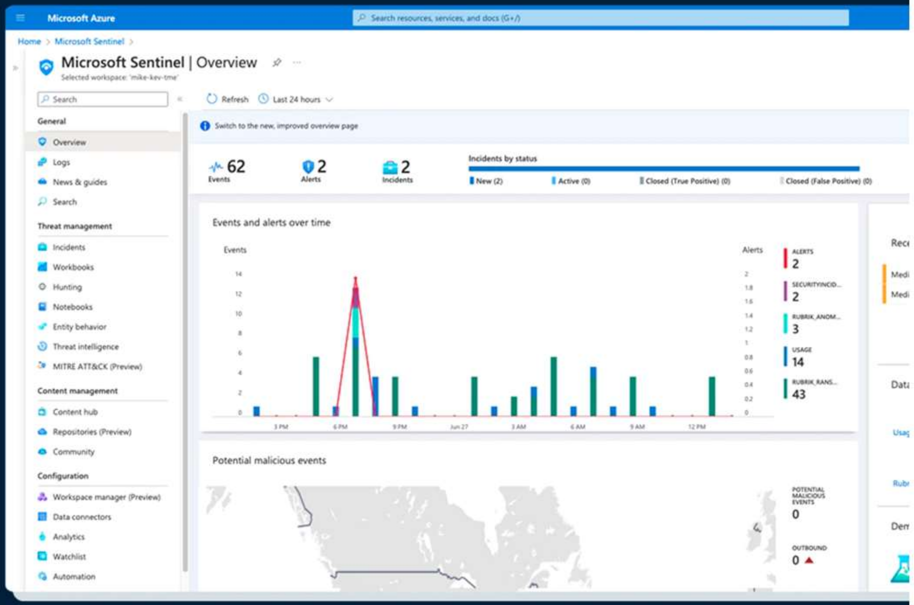
General Statistics

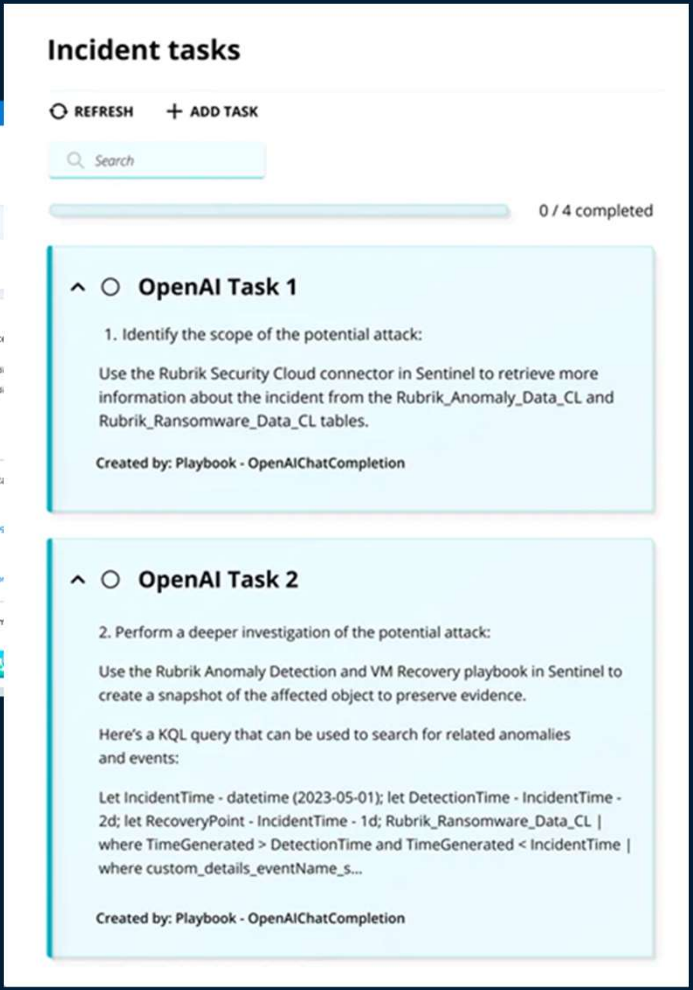
3117 Families

8049 Samples

Azure OpenAI

Respond to Incidents Faster with Generative AI-driven Recommendations





Incident tasks

REFRESH + ADD TASK

Search

0 / 4 completed

^ ○ OpenAI Task 1

1. Identify the scope of the potential attack:

Use the Rubrik Security Cloud connector in Sentinel to retrieve more information about the incident from the Rubrik_Anomaly_Data_CL and Rubrik_Ransomware_Data_CL tables.

Created by: Playbook - OpenAIChatCompletion

^ ○ OpenAI Task 2

2. Perform a deeper investigation of the potential attack:

Use the Rubrik Anomaly Detection and VM Recovery playbook in Sentinel to create a snapshot of the affected object to preserve evidence.

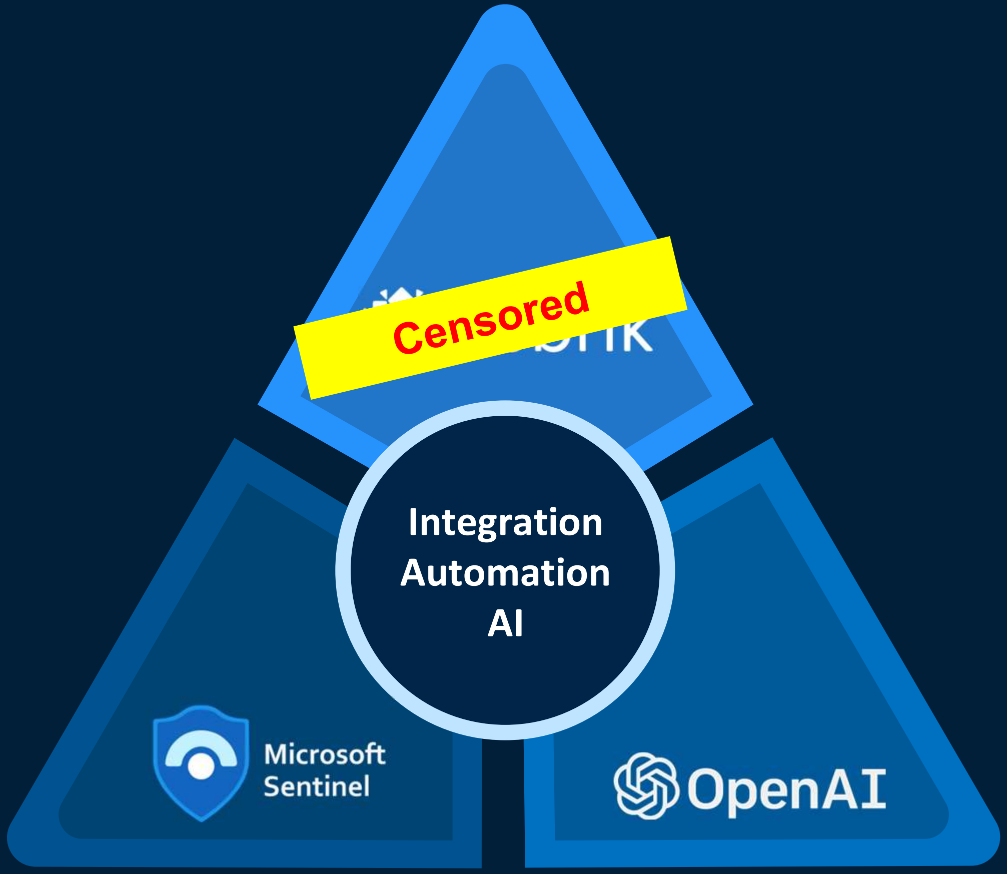
Here's a KQL query that can be used to search for related anomalies and events:

Let IncidentTime - datetime (2023-05-01); let DetectionTime - IncidentTime - 2d; let RecoveryPoint - IncidentTime - 1d; Rubrik_Ransomware_Data_CL | where TimeGenerated > DetectionTime and TimeGenerated < IncidentTime | where custom_details_eventName_s...

Created by: Playbook - OpenAIChatCompletion

Censored + Microsoft Sentinel + Azure OpenAI

Respond to Threats Faster with Generative AI-driven Cyber Recovery



- **Streamline Incident Creation**
  Automatically create incidents in Sentinel based on Backup/Snapshot intelligence
- **Automate Task Workstreams**
  Azure OpenAI suggests incident response tasks, speeding investigation
- **Accelerate Cyber Recovery**
  Enabling IT and security teams to react swiftly to maintain business resiliency

Final Thoughts

Call to Action

The only important slide in this deck

- Make sure you are covered in regards to all 6 pillars of the NIST CSF v2
- Check if your last line defence is truly resilient
- Check of your backups are air-gapped and 100% immutable (not just „marketing immutable“)
- Implement tools that have been created with Zero Trust First & in mind (no 3rd party apps!)
- Make use of ML and AI as part of your cyber recovery strategy…
- … but don’t let AI automatically initiate the responses
- Be prepared for the day and test recoveries to an IRE on a regular basis (ideally automated)
- Live and breathe Zero Trust and most importantly use Common Sense
- See new Regulations not as a Pain but as a Chance to improve the overall Cyber Resiliency

- Come and see me here today and tomorrow for additional thoughts

Want to learn more?

https://events.rubrik.com/data-security-talks

rubrik DATA SECURITY TALKS

rubrik Security Cloud™

Thank you!

frank.schwaak@rubrik.com
linkedin.com/in/frankschwaak/
@FrankSchwaak