rubrik | Zero Trust Data Security™

save the data™

How to Prepare for a Ransomware Attack on Microsoft 365

Kim Lambert - Principal Product Marketing Manager, Rubrik
Drew Russell - Technical Go-To-Market Lead, Microsoft Security Practices, Rubrik

Agenda

- The human toll of cyberattacks
- A new way of looking at data security
- How to ensure you’re ready - a demo of Microsoft 365 protection

rubrik™

PAYETTE

"My first thought was a simple power outage. It was not uncommon to have power fluctuations with heating and cooling.

But once I got to the office and started to bring the system back up, I realized this wasn't just a standard power outage.

We were under attack."

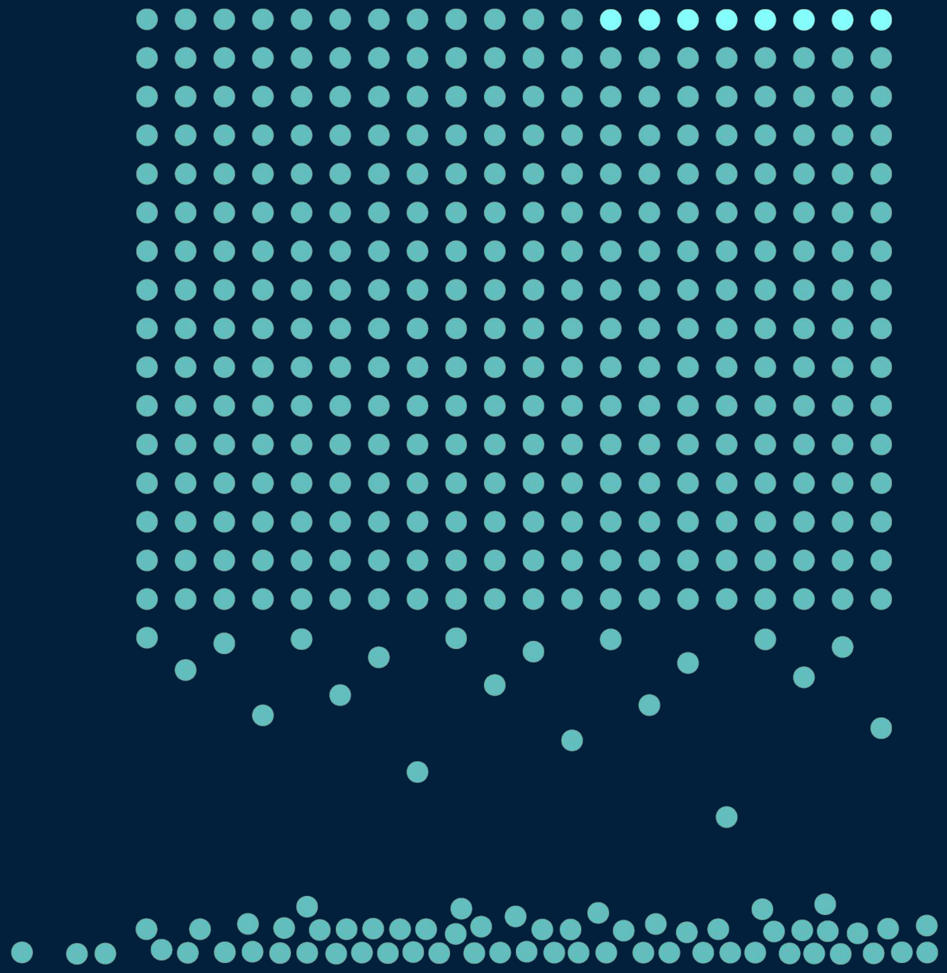
Introducing Rubrik Zero Labs

"Comprehensive threat intelligence from Rubrik Zero Labs will help enable organizations to prepare for a full swath of cyber threats."

Steve Stone
Head of Rubrik Zero Labs
Former Mandiant Vice President

98%

of organizations reported at least one cyberattack reaching their senior leader level of awareness



Organizations Struggle with Confidence

33%

of organizations believe their board / executives have little to no confidence in their organization’s ability to recover critical data

76%

of respondents would consider paying a ransom demand

52%

“extremely” or “very likely” to pay the ransom

The Weight of Cybercrime is Taking its Toll

96%

of IT and security leaders reported a significant emotional or psychological impact from cyberattacks in the last year:

50% Increased anxiety in daily role

43% Worry over job security

37% Loss of trust among colleagues

33% Loss of sleep/trouble sleeping

External Microsoft 365 Threats

Massive Solar Winds Hack - Microsoft 365

Microsoft 365 customers are at the center of a massive, persistent Russian cyberattack breaching US government and large commercial environments.

Microsoft Exchange credential stealing malware

The malicious module represents an effective option for attackers to gain a strong foothold in targeted networks by persisting inside an Exchange server

Proofpoint Discovers Potentially Dangerous Microsoft 365 Functionality

Functionality can ransom SharePoint and OneDrive files

71%

of organizations have experienced a Microsoft 365 account takeover.

32%

of companies experienced SaaS data loss in some form

71%

of organizations experienced suspicious behaviors from native automation

85%

of organizations using Microsoft 365 have suffered email data breaches

Securing Microsoft Office 365 in the New Normal,Vectra AI, 2021
The Evolution of Data Protection Cloud Strategies, ESG, 2021
The 2020 Spotlight Report on Office 365, Vectra AI, 2020
Preventing Email Data Loss in Microsoft 365, Egress Software, 2021

External and Internal Microsoft 365 Threats

Massive Solar Winds Hack - Microsoft 365

Microsoft 365 customers are at the center of a massive, persistent Russian cyberattack breaching US government and large commercial environments

Microsoft Exchange credential stealing malware

The malicious module represents an effective option for attackers to gain a strong foothold in targeted networks by persisting inside an Exchange server

Proofpoint Discovers Potentially Dangerous Microsoft 365 Functionality

Functionality can ransom SharePoint and OneDrive files

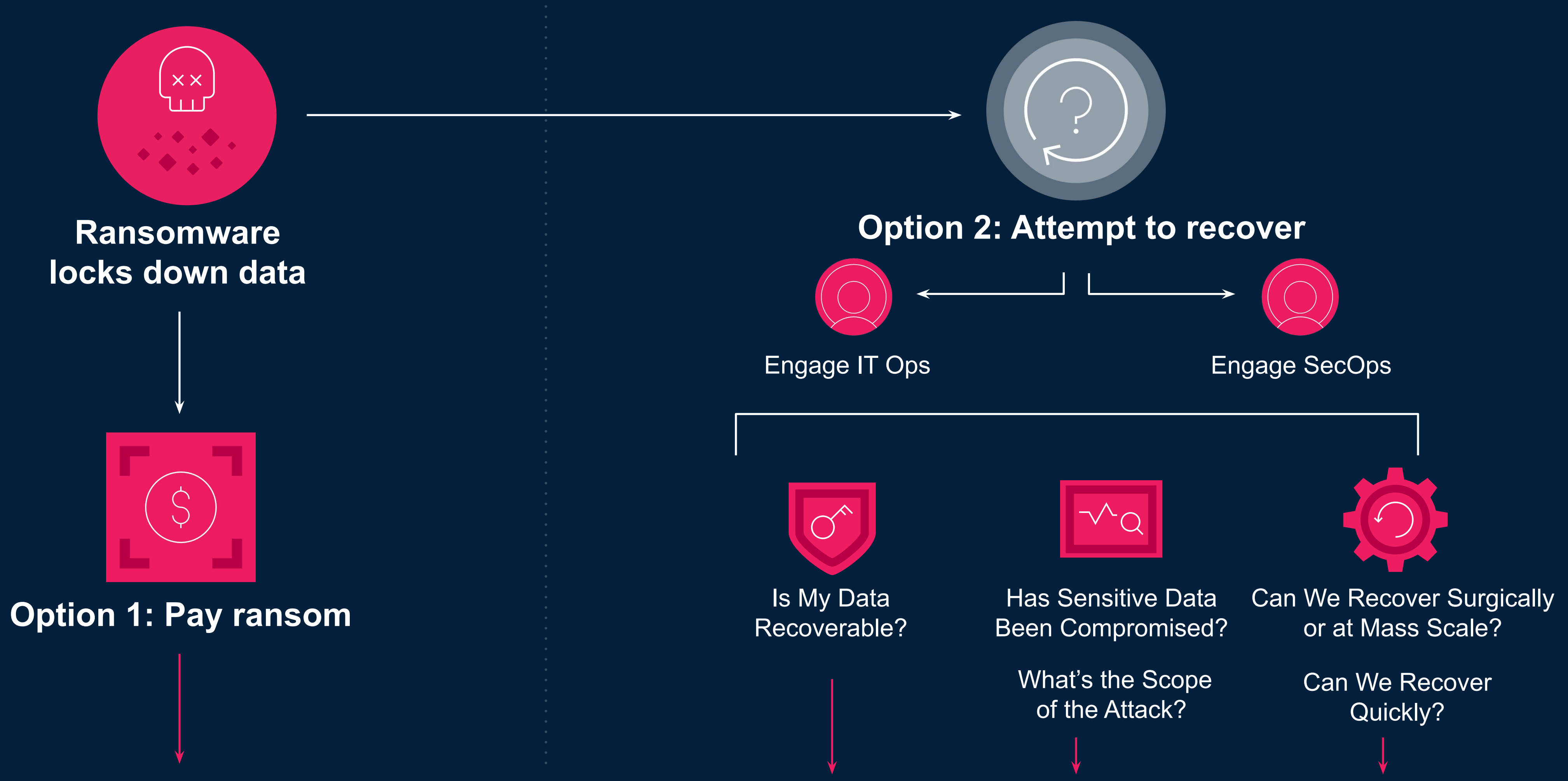
IT blunder permanently erases 145,000 user's personal chats in Microsoft Teams deployment

'Microsoft has confirmed the Teams chat data is not recoverable'

Creation of New Mailboxes and Assigning of Permissions to Access Other Mailboxes

Mandiant's Incident Response team has continued to respond to compromises originating from exploitation of these vulnerabilities

Why Are Organizations Stuck Paying Ransoms?



Ransomware locks down data

Option 1: Pay ransom

Option 2: Attempt to recover

Engage IT Ops

Engage SecOps

Is My Data Recoverable?

Has Sensitive Data Been Compromised?

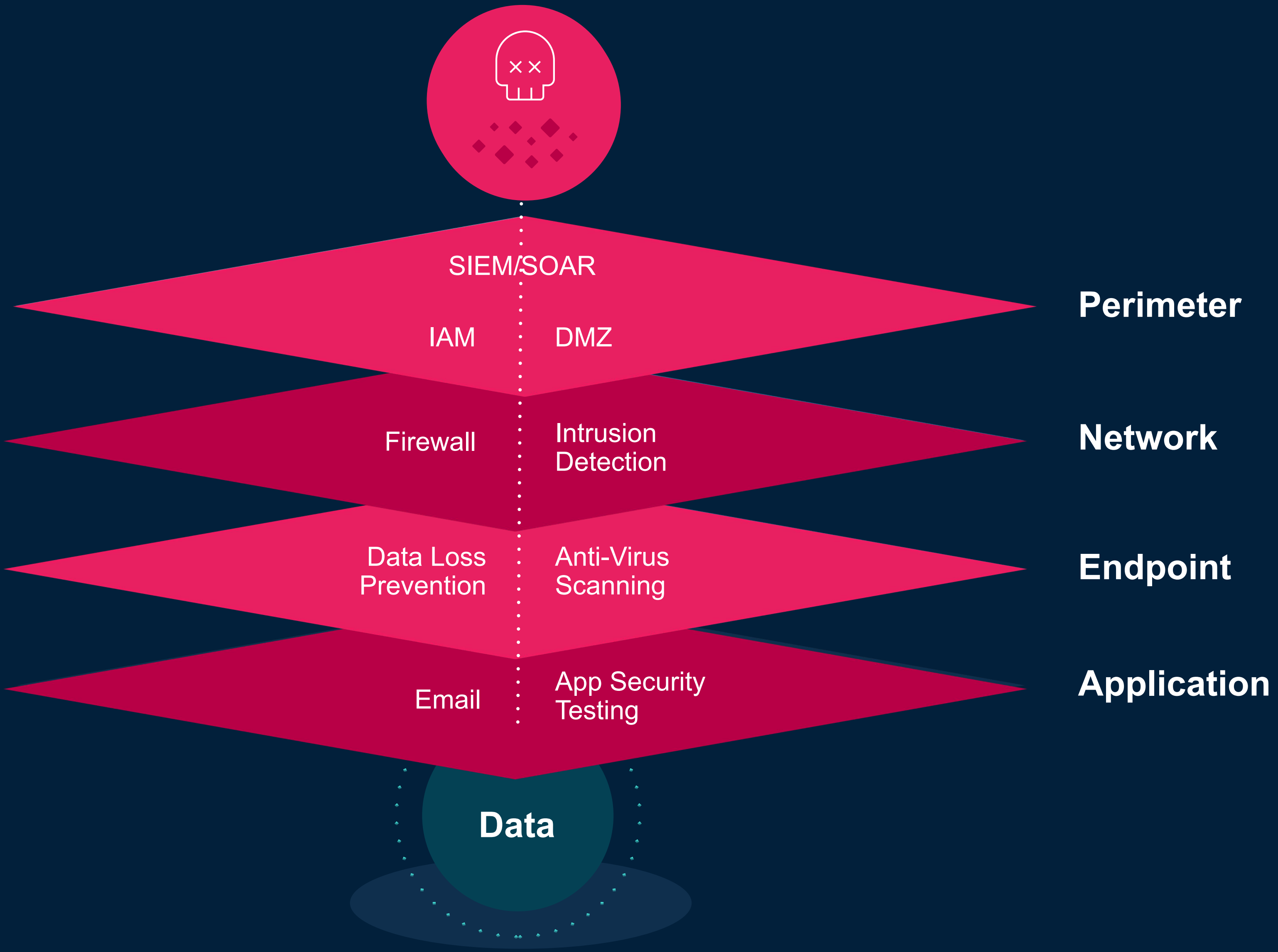
What's the Scope of the Attack?

Can We Recover Surgically or at Mass Scale?

Can We Recover Quickly?

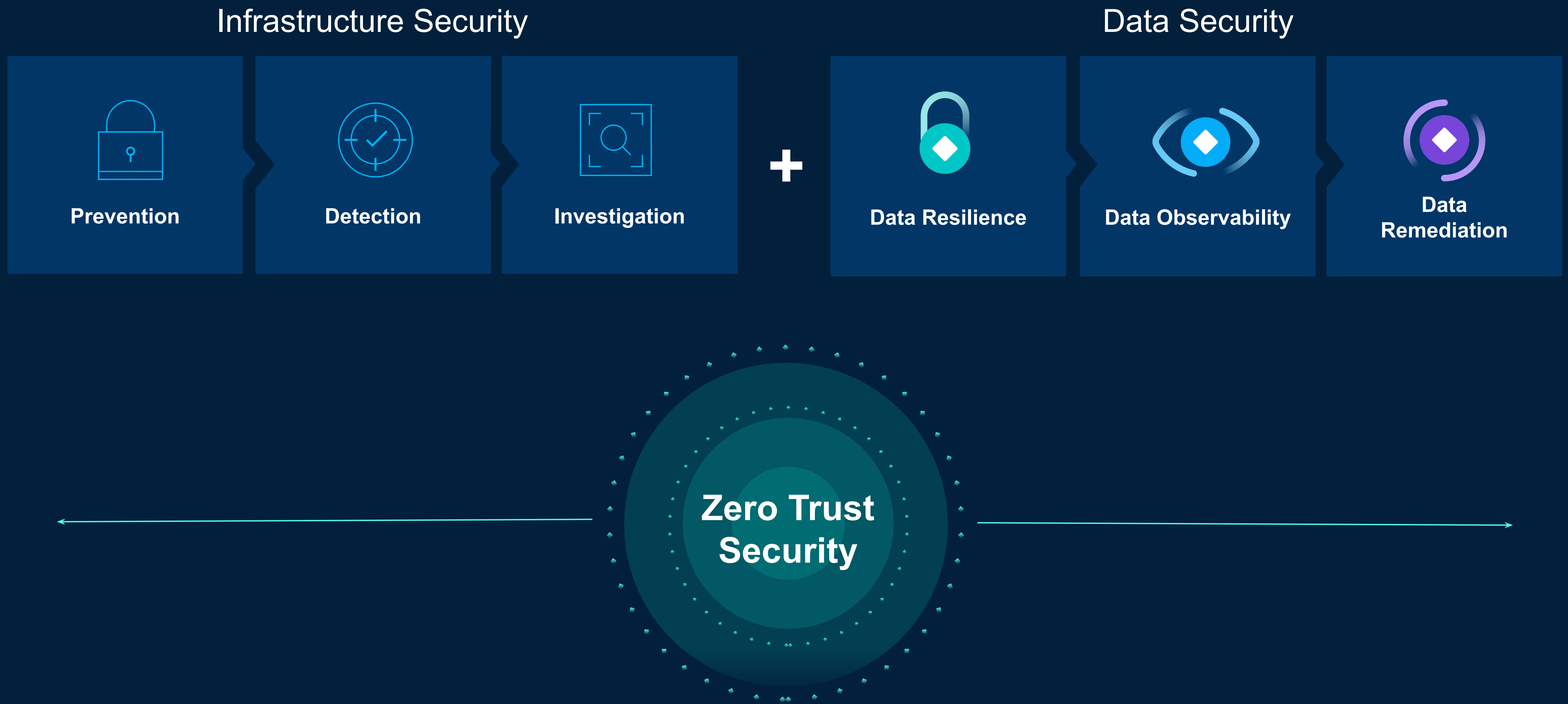
PAY RANSOM / HOPE FOR BUSINESS RECOVERY OF MICROSOFT 365

Infrastructure Security is Not Enough



The Next Frontier in Cybersecurity

Infrastructure Security And Data Security Together Provide Zero Trust Security



Infrastructure Security

Prevention

Detection

Investigation

+

Data Security

Data Resilience

Data Observability

Data Remediation

Zero Trust Security

The Pillars of Data Security

Data Resilience

What if you could by cyber-proof your backup data?

Data Observability

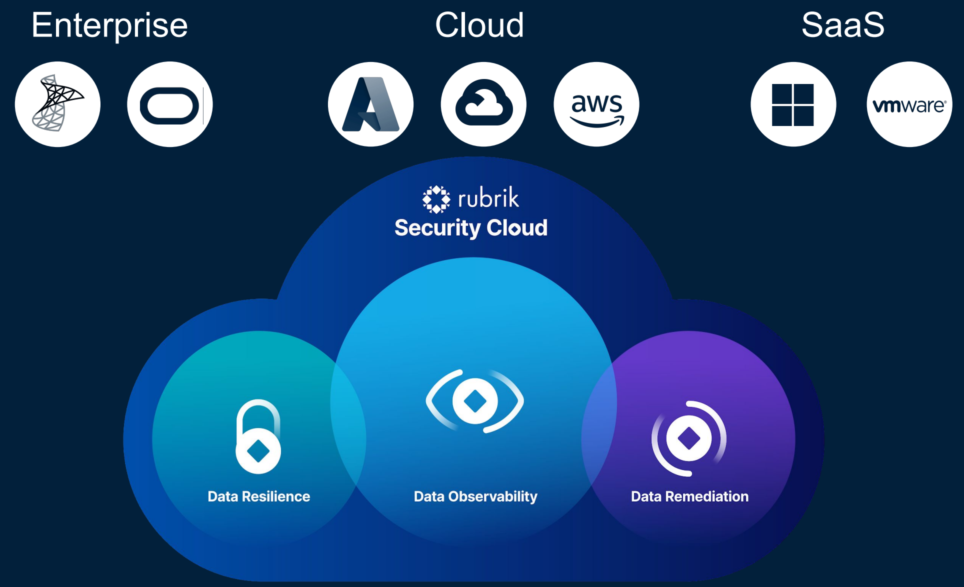
What if you could monitor risks and investigate threats quickly?

Data Remediation

What if you could rapidly recover just the data you need?

Rubrik Security Cloud

Secure data, wherever it lives, across enterprise, cloud, and SaaS. Make your business unstoppable.



Enterprise Data Protection

Cloud Data Protection

Microsoft 365 Protection

Ransomware Monitoring & Investigation

Sensitive Data Monitoring & Management

Threat Monitoring & Hunting

Data Security Command Center

Threat Containment

Mass Recovery

Orchestrated App Recovery

Microsoft 365

Data Resilience - What Your Teams Are Asking

Do we have any fail-safes if everything is compromised?

Can my Microsoft 365 retention rules
be tampered with?

Can my admins be compromised?

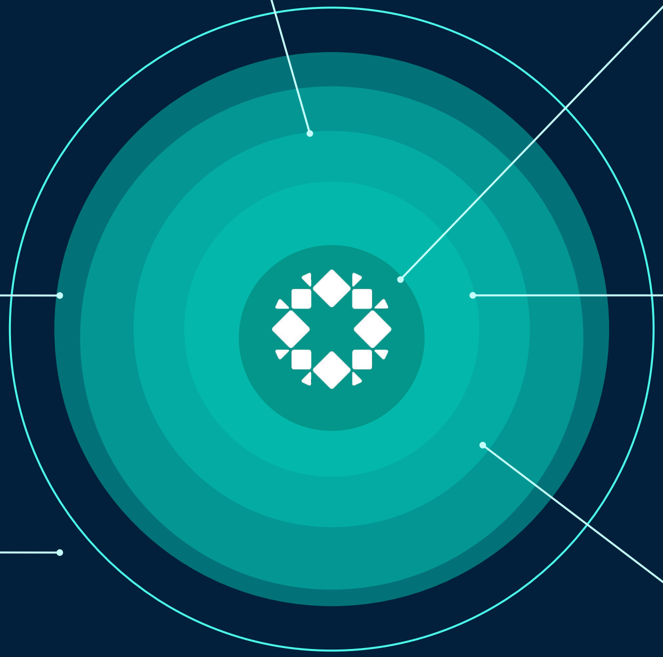
Can my backups be discovered by bad actors?

Can my backup data be seen by bad actors?

Can my backups be modified?

Rubrik Data Resilience for Microsoft 365

Secure your data from insider threats or ransomware with air-gapped, immutable, access-controlled backups



Immutability
so they can't change it

WORM storage to prevent data modification / deletion

Retention Lock
so they can't disrupt backups

Two-person approval needed to change retention policies

Intelligent Data Lock
so they can't delete data

Holds all data for 30 days beyond last admin action

Logical Air Gap – so they can't find it

Undiscoverable with NFS/SMB Network Protocols

Bring Your Own Key

Ability to revoke access from Rubrik

Enforced Control – so they can't access it

Natively enforced
MFA and TOTPs, granular RBAC, and delegated privileges / multi-geo support

Microsoft 365

Data Observability - What Your Teams Are Asking

When did malware first enter our Microsoft 365 backups?

Has there been any unusual deletions or modifications of my Microsoft 365 data?

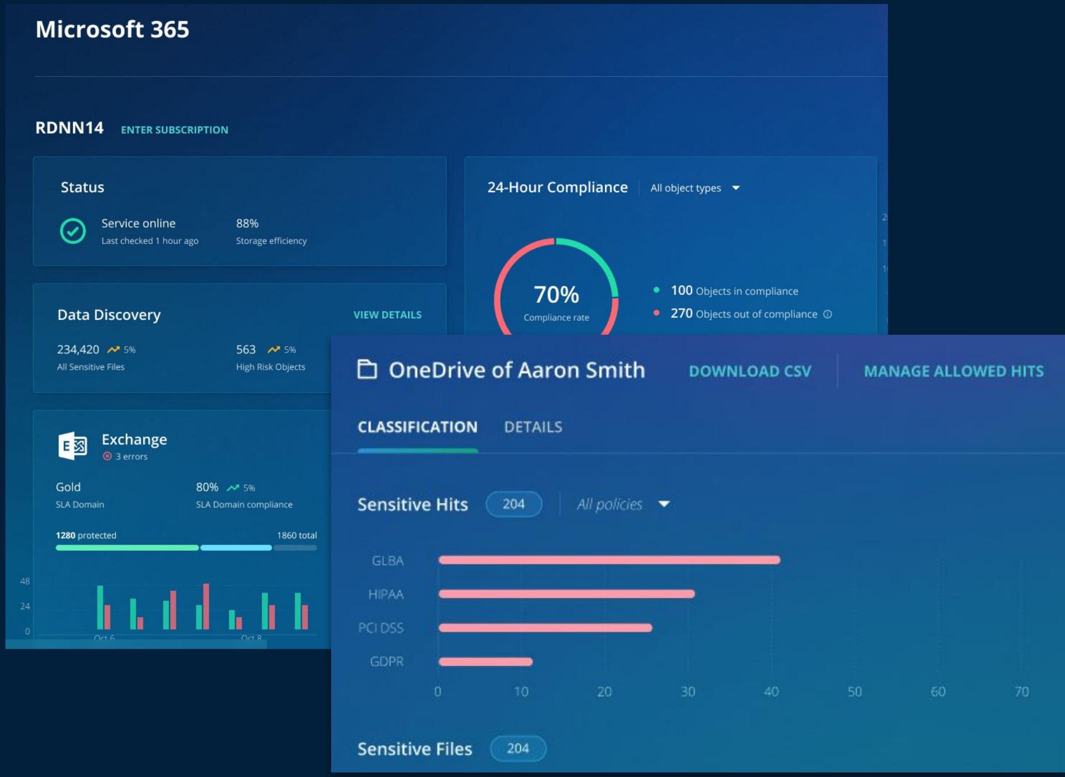
Was sensitive data affected by an attack?

Rubrik Data Observability for Microsoft 365

Continuously monitor your data for ransomware and manage potential sensitive data exposure risk in an attack

- **Ransomware Monitoring and Investigation:** Determine the scope of ransomware attacks, using machine learning to detect deletion, modifications, and encryptions

- **Sensitive Data Monitoring and Management:** Reduce sensitive data exposure by discovering what types of sensitive data you have and where it lives



Microsoft 365

RDNN14 ENTER SUBSCRIPTION

Status

Service online
Last checked 1 hour ago

88%
Storage efficiency

24-Hour Compliance All object types

70% Compliance rate

100 Objects in compliance

270 Objects out of compliance

Data Discovery VIEW DETAILS

234,420 5%
All Sensitive Files

563 5%
High Risk Objects

Exchange
3 errors

Gold
SLA Domain

80% 5%
SLA Domain compliance

1280 protected 1860 total

OneDrive of Aaron Smith DOWNLOAD CSV MANAGE ALLOWED HITS

CLASSIFICATION DETAILS

Sensitive Hits 204 All policies

Sensitive Files 204

Microsoft 365

Data Remediation - What Your Teams Are Asking

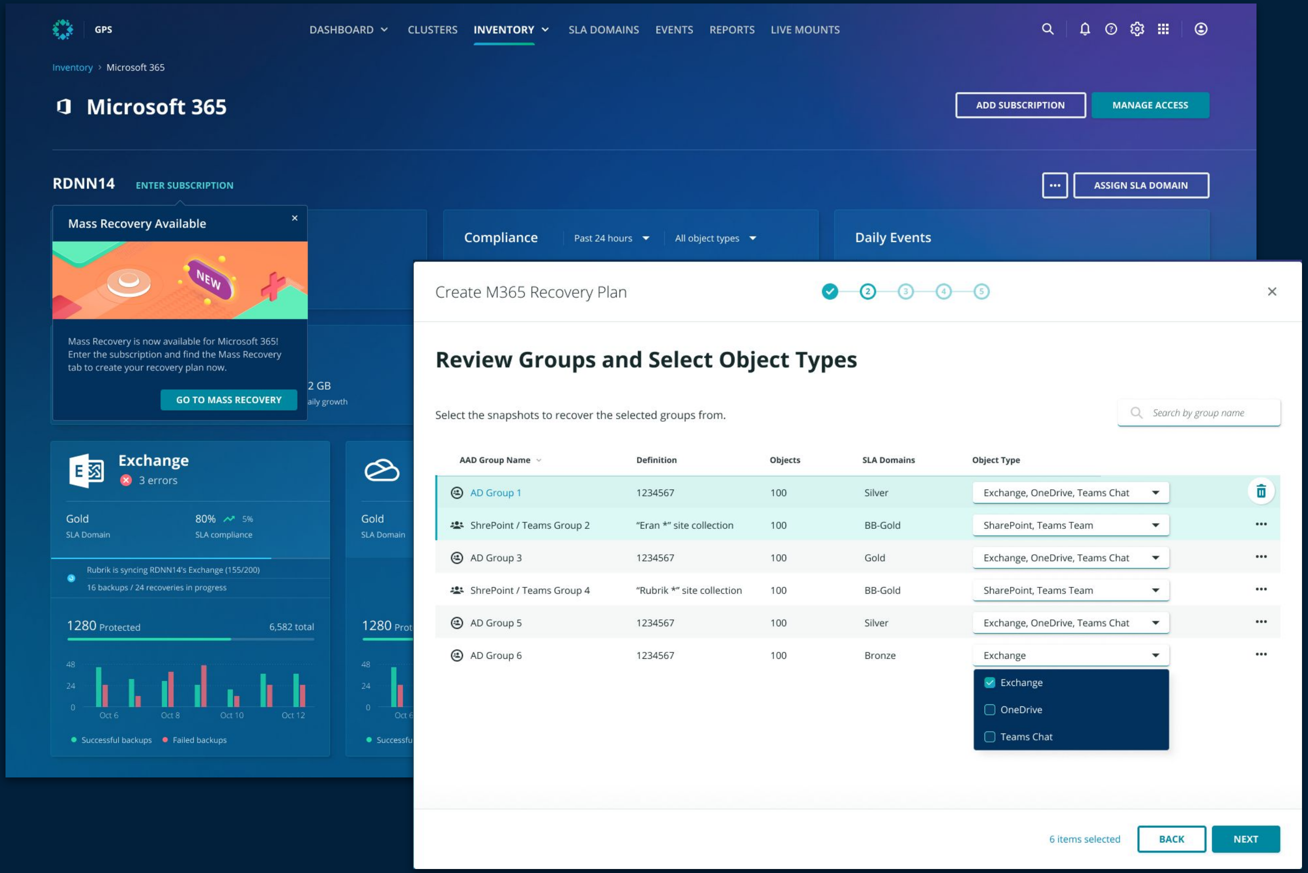
How do I automate the recovery of my most critical Microsoft 365 apps?

How can I surgically recover just what I need?

Rubrik Data Remediation for Microsoft 365

Rapidly recover your apps, files or users across Exchange, SharePoint, OneDrive, and Teams, surgically or at-scale

- **Mass Recovery:** Recover thousands of users quickly
- Restore business operations quickly by surgically recovering apps, files, or users



Microsoft 365

RDNN14 ENTER SUBSCRIPTION

Mass Recovery Available

Mass Recovery is now available for Microsoft 365! Enter the subscription and find the Mass Recovery tab to create your recovery plan now.

GO TO MASS RECOVERY

Exchange

3 errors

Gold SLA Domain

80% 5% SLA compliance

Rubrik is syncing RDNN14's Exchange (155/200)

16 backups / 24 recoveries in progress

1280 Protected 6,582 total

Create M365 Recovery Plan

Review Groups and Select Object Types

Select the snapshots to recover the selected groups from.

Search by group name

AAD Group Name	Definition	Objects	SLA Domains	Object Type
AD Group 1	1234567	100	Silver	Exchange, OneDrive, Teams Chat
ShrePoint / Teams Group 2	“Eran *” site collection	100	BB-Gold	SharePoint, Teams Team
AD Group 3	1234567	100	Gold	Exchange, OneDrive, Teams Chat
ShrePoint / Teams Group 4	“Rubrik *” site collection	100	BB-Gold	SharePoint, Teams Team
AD Group 5	1234567	100	Silver	Exchange, OneDrive, Teams Chat
AD Group 6	1234567	100	Bronze	Exchange

☑ Exchange
☐ OneDrive
☐ Teams Chat

6 items selected BACK NEXT

PAYETTE

Payette Fends off Cyber Breach with Rubrik Security Cloud!

rubrik | Microsoft

> “Rubrik seamlessly integrates with Microsoft to protect M365 data, arming it with immutability and resiliency against cyber threats.
> It is a game changer.

Dan Gallivan,
Director of IT
PAYETTE

Rubrik delivered:

<24 hrs

critical systems back online

100%

recovery within 1 week

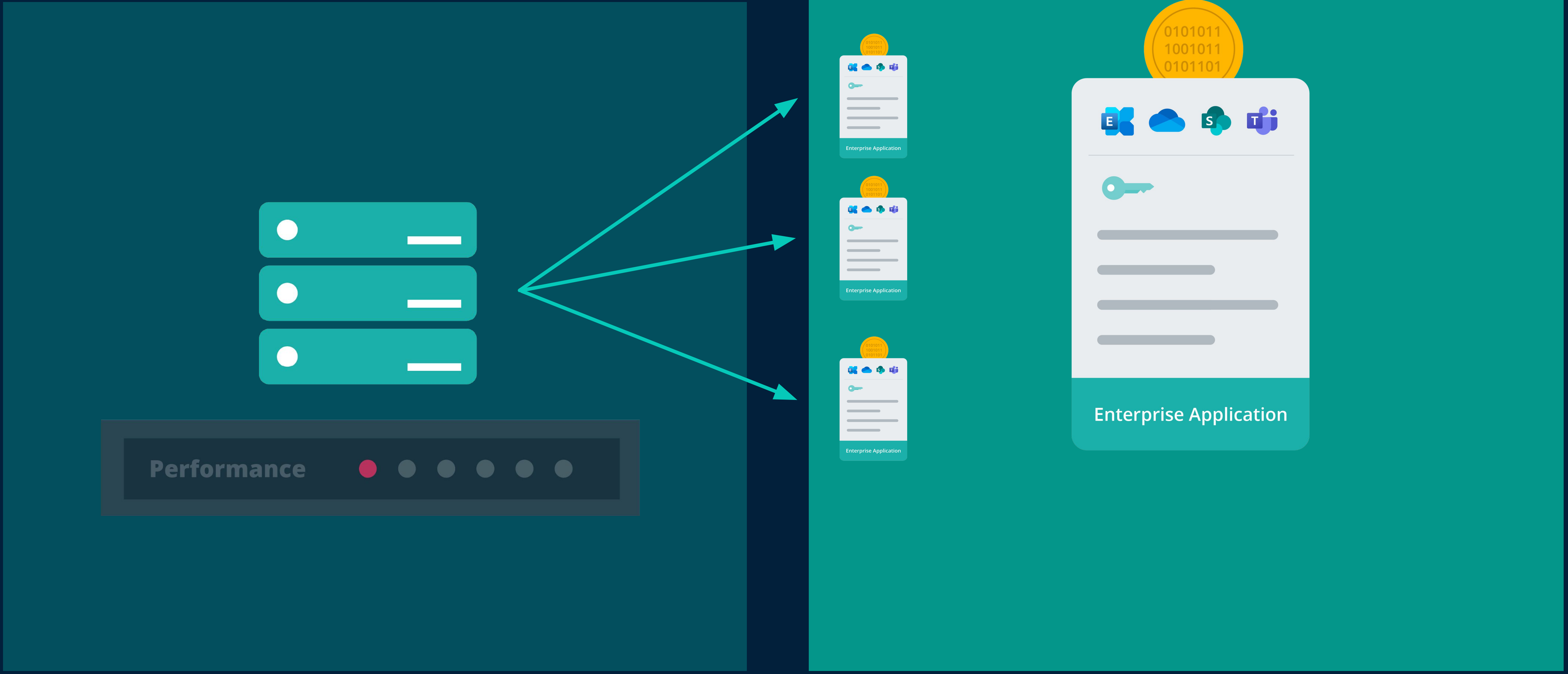
Microsoft 365

and Azure data resilient against cyber threats

How Does It Work?

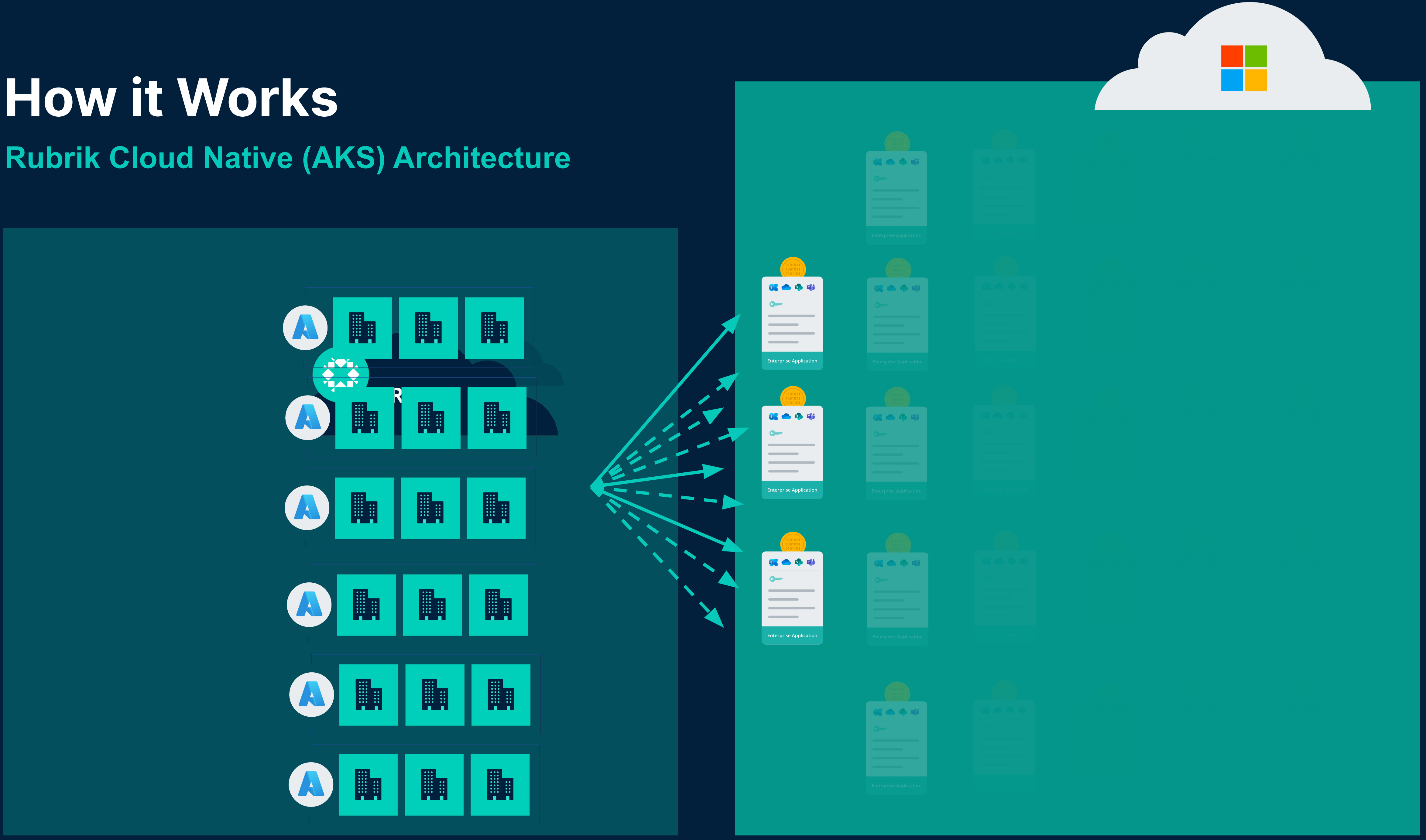
How it Works

On-prem architecture limitations



How it Works

Rubrik Cloud Native (AKS) Architecture



rubrik | Zero Trust Data Security™

Demo

rubrik | Zero Trust Data Security™

Thank you

Wrap-Up

- Microsoft 365 is a critical, Tier-1 SaaS app and is targeted by attackers
- Rubrik can secure your data from cyber attack or even human error
- Your Microsoft 365 and other organizational data can be resilient, observable, and recoverable

rubrik | Zero Trust Data Security™

Q&A