Notfallwiederherstellung & Security Operations

Erfolgreiche auf Vorfälle reagieren und Notfälle meistern

Kenneth Döhmen
Lead Security Engineer DKV Mobility

Fabian Weber
Managing Partner water IT Security & Defense

Ransomware attacks continue to rise

In 2021, every

11 SECONDS

A company was hit by ransomware[1]

Average cost of

$1.4M

To recover from ransomware attacks[1]

$590M

Reported ransom paid in 2021[2]

Of all victims

46%

Paid a ransom demand[1]

But got only

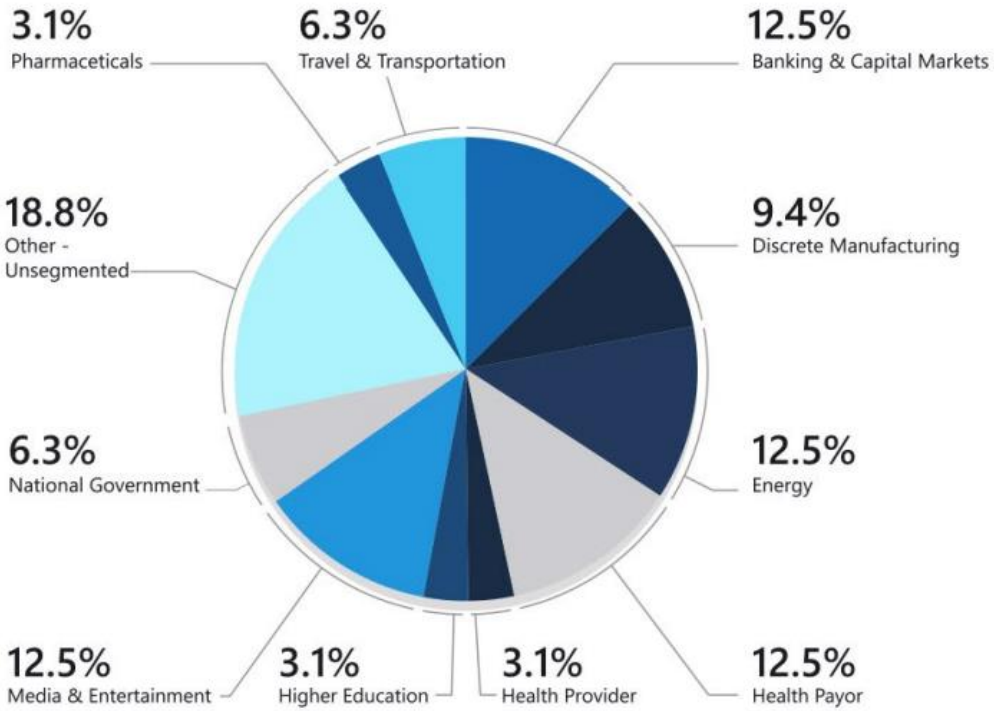
61%

Of their data back[1]

Only

57%

Recovered data successfully[1]



Healthcare (Providers plus Payors) 15.6%,
Energy 12.5%,
Financial 12.5%,
Media & Entertainment 12.5%

Figure 1: Percentage Distribution of Key Sectors Targeted in Recent Ransomware Attacks

[1]Source: Sophos – State of Ransomware 2021, 2022

[2]FinCen Ransomware Advisory – Nov 2021

Why do bad things happen?

Hardware will fail

So we incorporate physical redundancies wherever possible

Software will have bugs

So we deploy code changes cautiously to reduce the impact

People will make mistakes

So we automate people out of the equation where it makes sense

Business Continuity is Everyone's Business…

Ransomware

Data corruption and deletion

Outages and natural disasters

Compliance

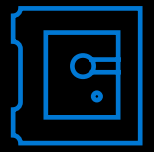
Protect your organization from ransomware

Create a response plan and adopt the right tools

Adopt an internal culture of Zero Trust, assumed breach, and good security hygiene and posture. Implement a system of data recovery/backup and secure access.

Related capabilities

- Remote access
- Zero Trust
- Security posture
- Data backup



Prevent attackers from getting in

Harden the security perimeter by leveraging best-in-class security workloads.

Deploy comprehensive prevention, detection, and response capabilities.

Related capabilities

- SIEM + XDR for prevention, detection, and response
- Cross-workload security

Protect critical data from compromise

Minimize the potential for lateral movement and privilege escalation should an attacker gain an entry point.

Related capabilities

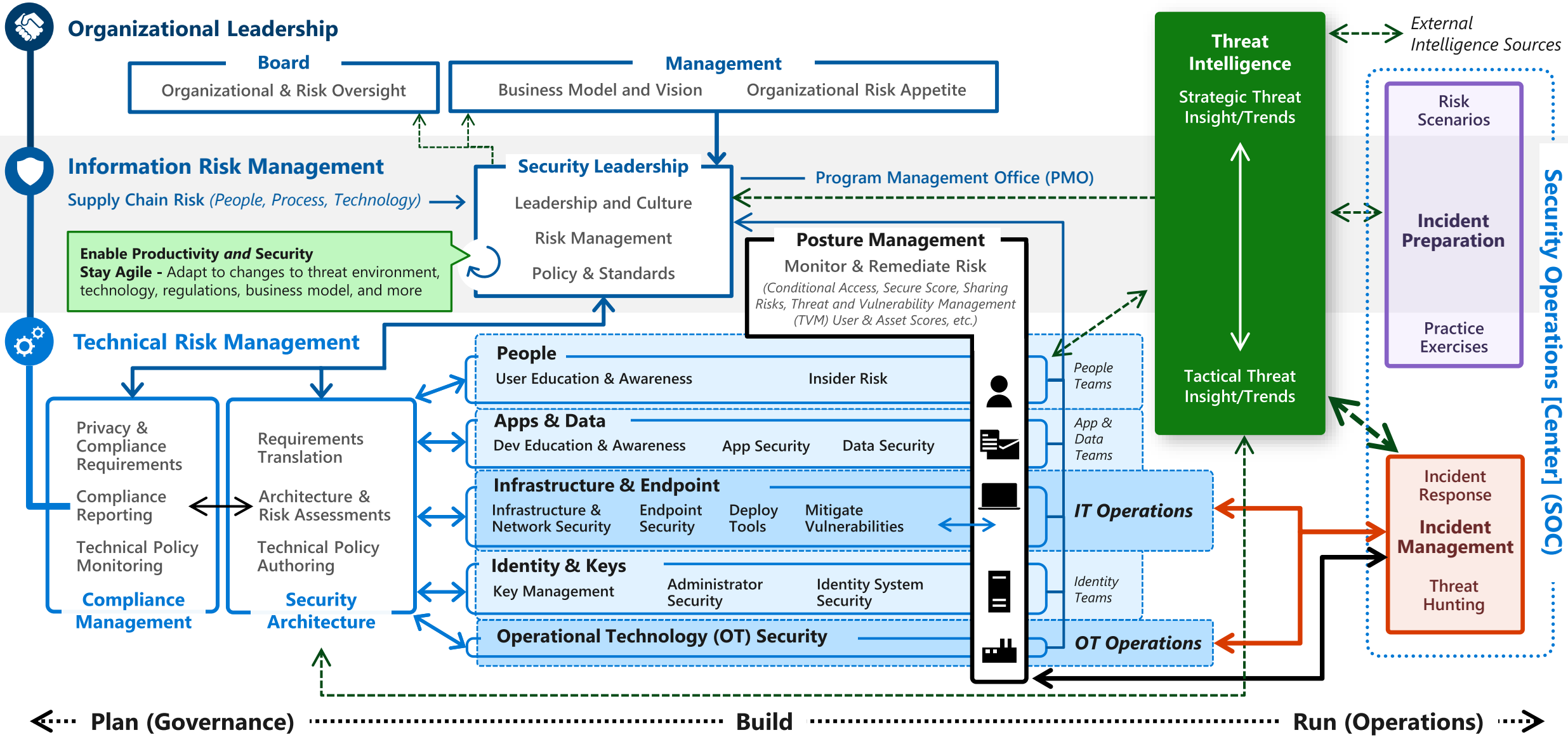
- Internal process/access management
- Data backup and business continuity

Managing Information\Cyber Risk

Security responsibilities or "jobs to be done"

December 2022 - https://aka.ms/SecurityRoles

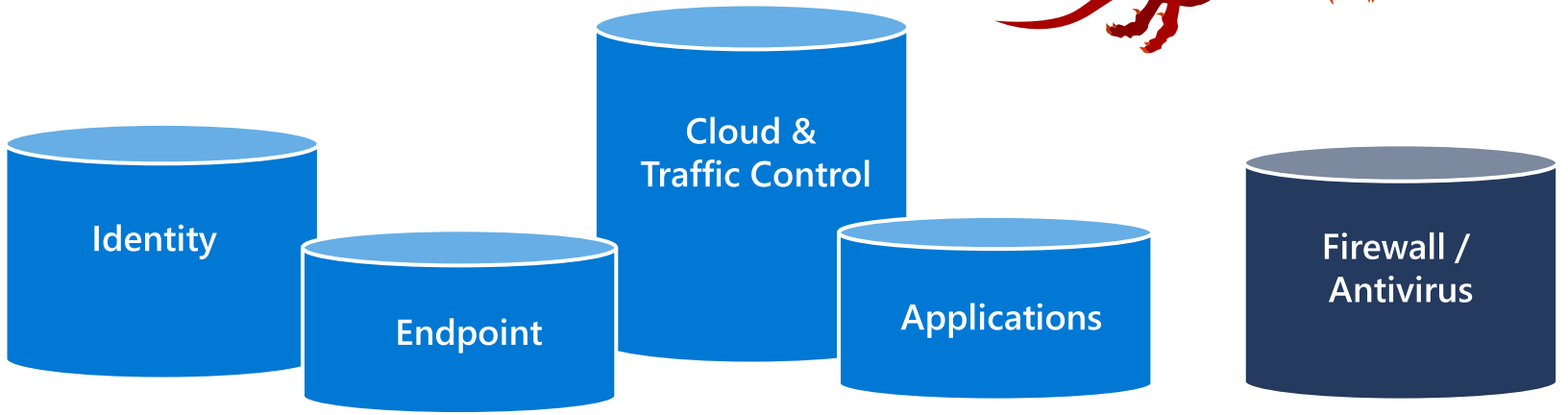
Microsoft



Silos are the Bane of Security Operations

Defender Silos make chasing them difficult

Attackers traverse rapidly across the enterprise



Integrating Silos is Challenging

MAPPING CHALLENGES
Bringing it all together

- Proof of concept
- Provider choice
- Gap Assessment
- Business Continuity
- Etc.

STRONG BIASES/TENDENCIES

Identity ⟷ **Endpoint**

Reports only high-quality alerts because
- Analysts have alert fatigue, resist new tools
- Analysts have network background and value of Identity isn't self evident

Verbose alert reporting
- AV testing focuses on "not missing" malware
- Reporting more improves showing in AV Testing reports

• • •

Security today with Microsoft365

Microsoft Defender for Endpoint

Network Identity Services Engine
802.1x

Microsoft BitLocker
incl. Bitlocker to Go

Microsoft Entera (Azure AD) Passwort Protection

Microsof 365
Vulnerability Management

Microsoft Exchange Online Protection
incl. Safe Links, Safe Attechments,Attack Simulation

Microsoft Defender for Cloud

Zscaler Internet Access &
Zscaler Private Access

Microsoft Conditional Access

Microsoft Defender for Identity

Microsoft Cloud App Security

Microsoft Information Protection

Microsoft Hello for Business

Microsoft Intune

Microsoft Sentinel

Firewalls

Identities

Endpoints

Apps

E-mail

Cloud Apps

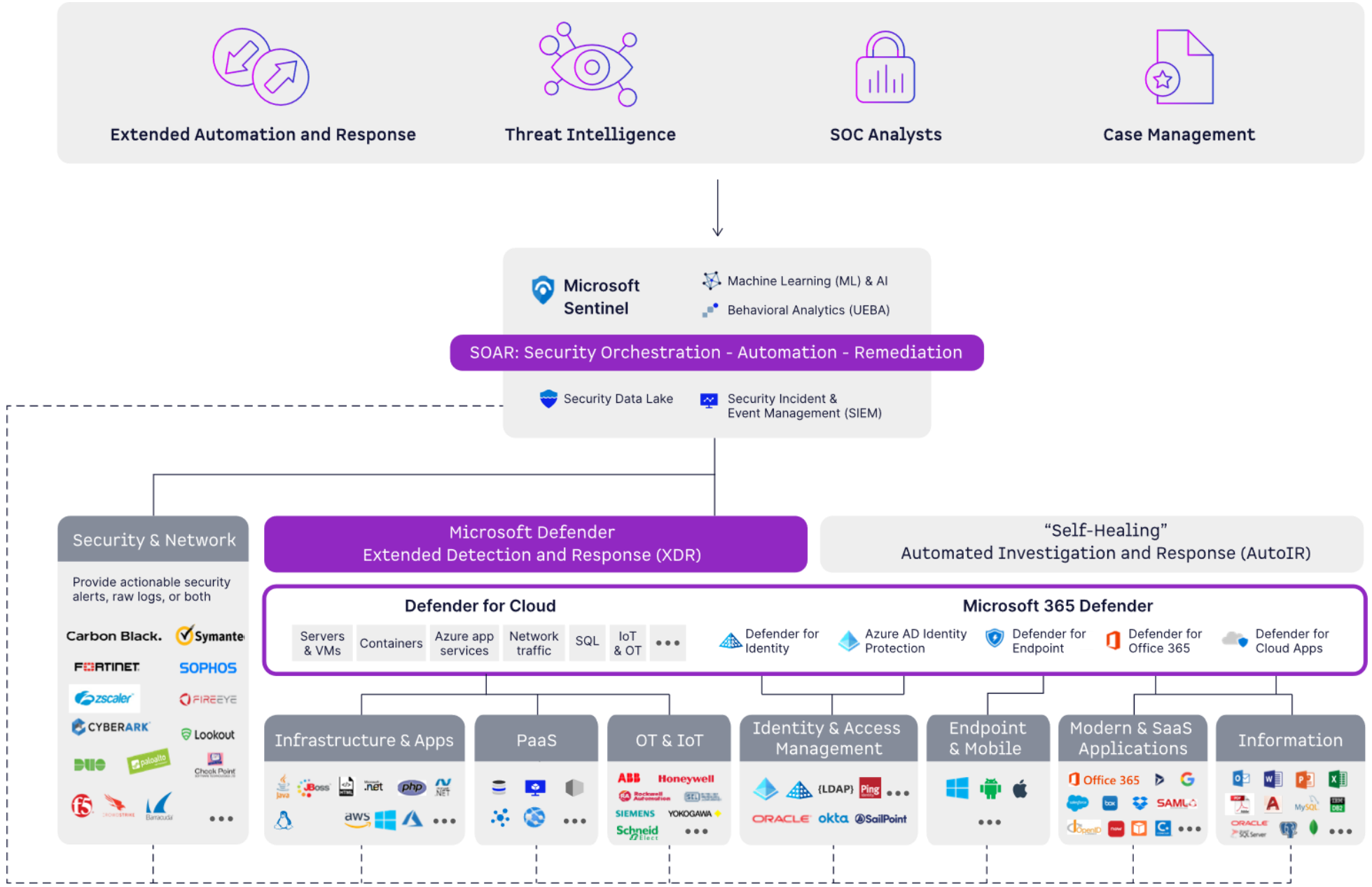
Docs

Network

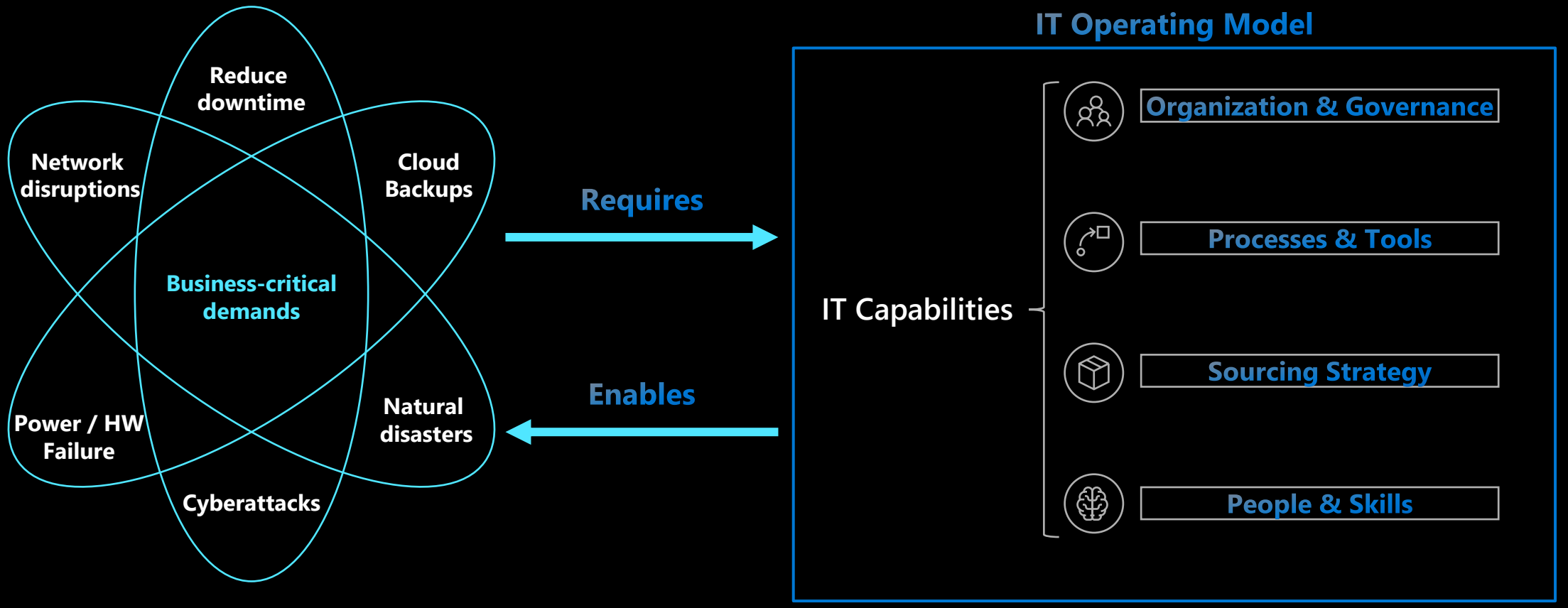
IoT

Azure App Services

Service Architecture



Business critical demands



Customer need

Infrastructure (applications and data)

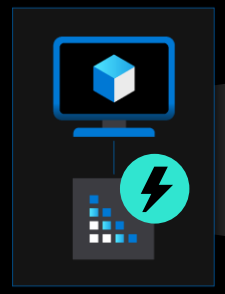
Data (stateful)

Improved availability

Build and run highly-available applications with near-zero RPO/RTO

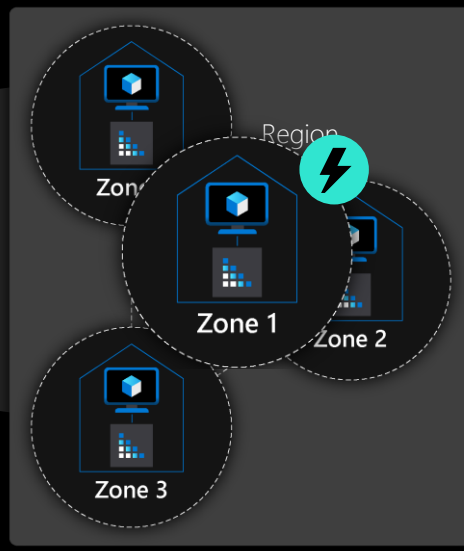
Implement disaster recovery plans with data residency and minimal RPO/RTO

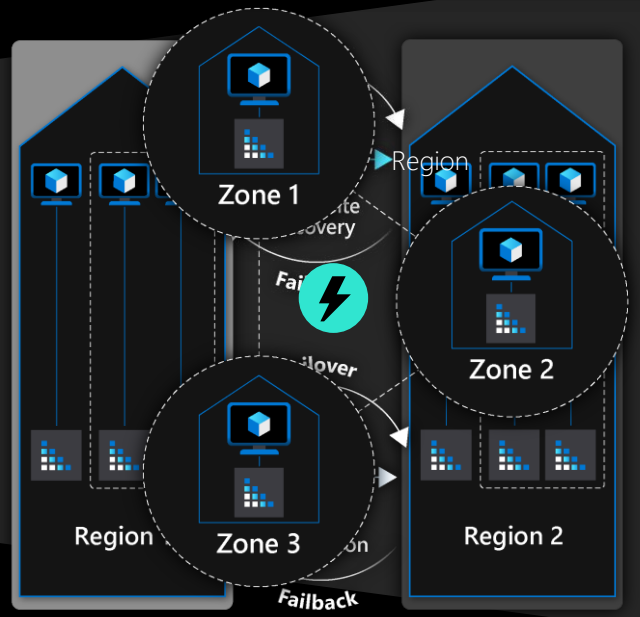
Premium Storage | Availability Sets | Availability Zones | Azure Site Recovery/Region Pairs



Single VM

Datacenter





SLA 99.9%

Isolated VM failure

e.g., OS disk HDD issue

SLA 99.95%

Hardware failure

e.g., server rack issue

SLA 99.99%

Entire datacenter failure

e.g., power/network issue

Industry-leading RPO/RTO

Entire region failure

e.g., natural disaster

Scope of Impact...

Accidental data loss | Data corruption | Ransomware | Rogue administrator

Azure Backup

Go back to restore a healthy version of the data

Managed SOC Implementation

Phase 1 — 4 weeks

Signoff

Phase 2 — 4-12 weeks

Signoff

Phase 3 — Ongoing

Review & Assessment

- Contractual agreement
- Assessment of the SOC, Technology and process landscape

Onboarding

- Deployment of open Defenders and platform optimization for SOC operations.
- Communication channels
- Incident processes

Incident Handling

- Alignment of Escalation procedures
- Creation of a RACI matrix
- 1st check in on interfaces and performance indicator

Monitoring

- Monitoring alignment based regular meetings
- Incident documentation for and improvement

Regular Operation

- Finalization of a results paper with all findings from the PoC
- Preparation for regular SOC operation

SOC Team

Transition Team

SDM Team

Today's choices echo in tomorrows resilience

Do's	Dont's
- Top down approach - Open communication	- Operating in silos
- Outsource if bottlenecks exist	- Ignoring risks due to lacking knowledge and resources
- Keep your playbooks, guidance and plans up-to-date and accessible	- Underestimate the importance of centralized documentation and planning
- Conduct tests and table top exercises	- Unclarified roles
- Define the bigger picture and go for it	- Working on small details without an overall goal

Session Feedback

Session Title: Notfallwiederherstellung & Security Operations - Erfolgreich auf Vorfälle reagieren und den Notfall meistern

https://aka.ms/AzSum-S013