# Ali Qureshi

Head of Public Cloud Nordics

NetNordic

netnordic
THE BEST COMPANION

Ali Qureshi

# NetNordic
# Secure Journey to Cloud

netnordic
THE BEST COMPANION

# Our broad cloud offering accelerate digital transformation with focus on business value

**Cloud strategy & advisory**

We **tailor a cloud strategy around your business** needs using key principles for device and software mgmt., user access mgmt., security & compliance and advising best-in-class cloud-first approach

**Cloud migration and adoption**

Our team delivers projects efficiently with focus on intergrating both people and technology. This ensures a **successful adoption considering the organizations cloud readiness and ambitions**

**Cloud optimization**

NetNordic ensures you **get maximum value out of your cloud journey** by conducting optimization services, diving deep into the data, using right sizing, and advising you on choosing the right services for the job.

**Cloud security**

Ready-made integrations on network, security, IAM enable NetNordic's partners to take full advantage of our integrated Azure cloud platform while **maintaining a seamless, secure and unified IT environment.**

**Cloud operations & monitoring**

Offering a broad portfolio in Azure, NetNordic manage services with focus on monitoring and providing valuable insights about the clients' environment to **support customers cloud projects**

**Hybrid & private cloud**

The hybrid and private cloud services allow clients to keep workloads not ready for public cloud easily available with a **comprehensive, fully managed setup with dual-site hosting, disaster recovery and more**

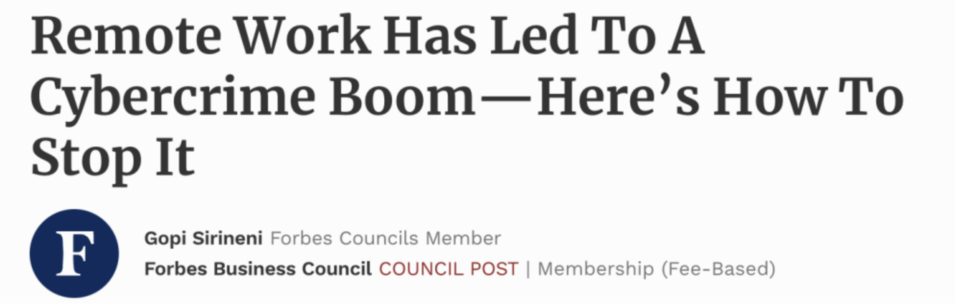
Source: NetNordic

# Cyber Crime development and AI

AI methods, such as deepfakes and voice cloning, are maximizing the success rates of social engineering by the minute. Many experts worry that the accessibility of generative AI solutions like ChatGPT will further democratize cybercrime and erode trust or even worsen political instability.

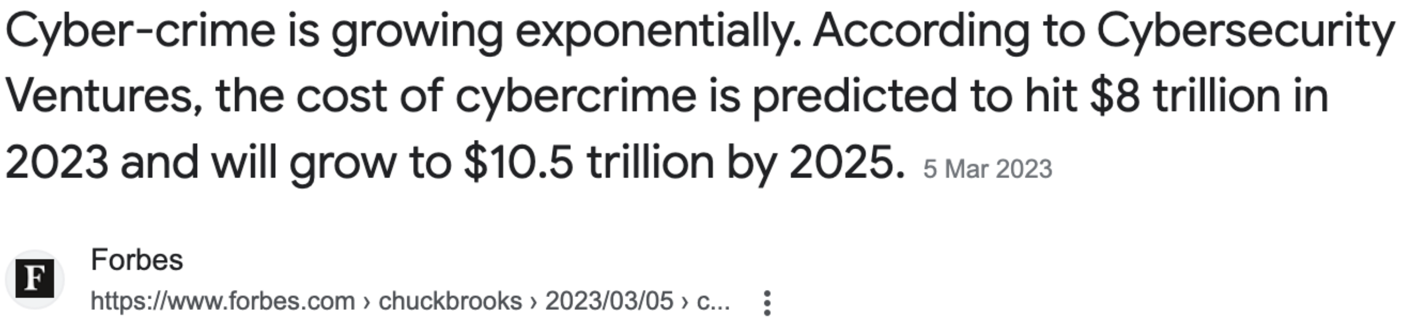
It's now on organizations to keep up with criminals' pace of innovation to protect themselves.

› Find out how to stay ahead



## Remote Work Has Led To A Cybercrime Boom—Here's How To Stop It

**Gopi Sirineni** Forbes Councils Member
**Forbes Business Council** COUNCIL POST | Membership (Fee-Based)



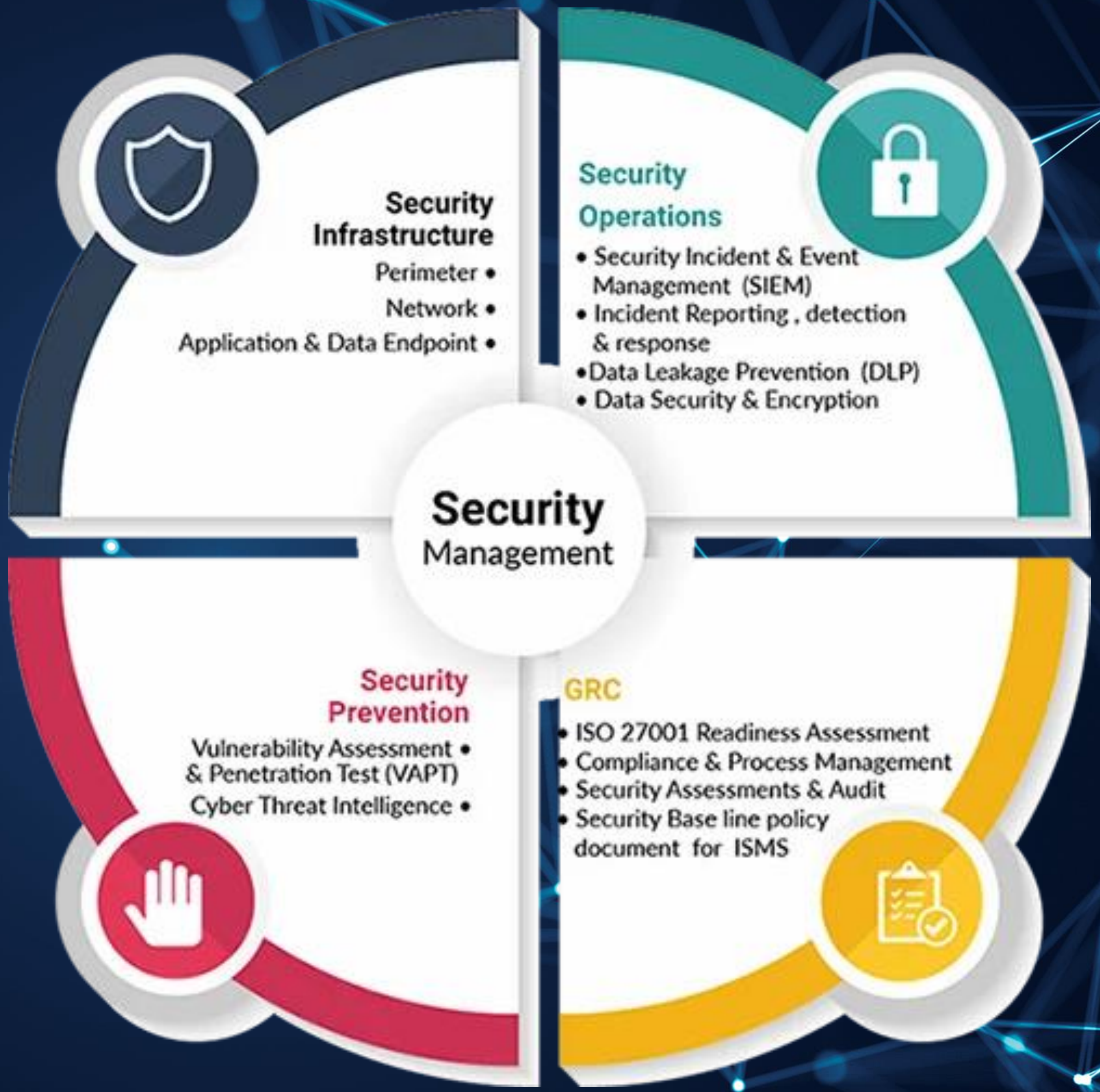
Cyber-crime is growing exponentially. According to Cybersecurity Ventures, the cost of cybercrime is predicted to hit $8 trillion in 2023 and will grow to $10.5 trillion by 2025. 5 Mar 2023

Forbes
https://www.forbes.com › chuckbrooks › 2023/03/05 › c...

# Key Strategic Objectives

## Office IT

| Principles | Objectives | Business Value | Financial Impact |
|---|---|---|---|
| Device and software standardization | • We issue a standard set of devices to our employees (PCs supplied in S-XL packages)<br>• Standard certified OS and software is used across all business units and countries<br>• Solutions are based on standard technology and software with minimal level of customization | • Increased efficiency in IT support through less time spent on troubleshooting problems caused by custom installations<br>• Employees work more efficient with devices not causing problem | ↓ OPEX ↑ EBITDA |
| Centralized and standardized user access management | • One identity for all applications using AAD O365<br>• One place to enable and disable user access to software and devices<br>• On board and offboard users in one place | • Good user experience<br>• Less license cost<br>• Less governance cost and high security<br>• Fast integration to external cloud applications | ↓ OPEX ↑ EBITDA |
| Security and compliance | • Installed software is monitored on all devices using Intune O365<br>• Multifactor Authentication and conditional access<br>• Audit trail across all platforms and monitor Monitor 24/7/365<br>• Central patch management for all software | • Software compliant and high security<br>• Cost reduction through optimizing software usage<br>• Less administration through streamlined software versions | ↓ OPEX ↑ EBITDA |
| Cloud First Approach | • Optimize costs by shifting to OpEx and reducing CapEx<br>• Strengthen security and compliance with cloud-native controls<br>• Improve agility and innovation through rapid service deployment<br>• Enable data-driven decisions with real-time analytics and AI<br>• Ensure business continuity with cloud-based disaster recovery | • Decreased operational and maintenance costs<br>• Scalability<br>• Secure<br>• Less business interruption<br>• Flexible and fast time to market | ↓ OPEX ↑ EBITDA |



## Security Management

### Security Infrastructure

- Perimeter
- Network
- Application & Data Endpoint

### Security Operations

- Security Incident & Event Management (SIEM)
- Incident Reporting , detection & response
- Data Leakage Prevention (DLP)
- Data Security & Encryption

### Security Prevention

- Vulnerability Assessment & Penetration Test (VAPT)
- Cyber Threat Intelligence

### GRC

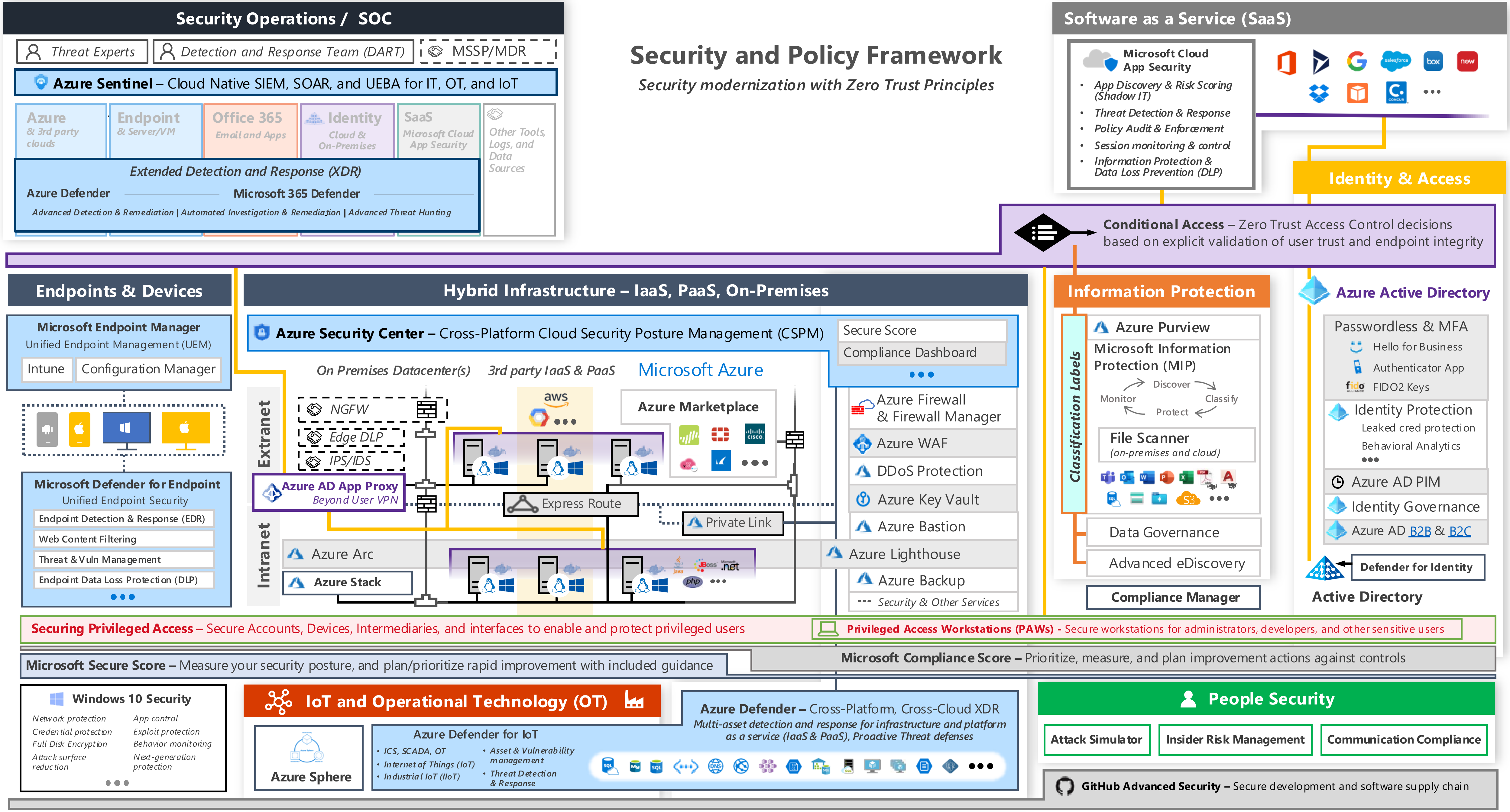
- ISO 27001 Readiness Assessment
- Compliance & Process Management
- Security Assessments & Audit
- Security Base line policy document for ISMS

netnordic

THE BEST COMPANION

# Security and Policy Framework

*Security modernization with Zero Trust Principles*



## Security Operations / SOC

Threat Experts | Detection and Response Team (DART) | MSSP/MDR

**Azure Sentinel** – Cloud Native SIEM, SOAR, and UEBA for IT, OT, and IoT

Azure *& 3rd party clouds* | Endpoint *& Server/VM* | Office 365 *Email and Apps* | Identity *Cloud & On-Premises* | SaaS *Microsoft Cloud App Security* | *Other Tools, Logs, and Data Sources*

*Extended Detection and Response (XDR)*

Azure Defender | Microsoft 365 Defender

*Advanced Detection & Remediation | Automated Investigation & Remediation | Advanced Threat Hunting*

## Software as a Service (SaaS)

Microsoft Cloud App Security

- *App Discovery & Risk Scoring (Shadow IT)*
- *Threat Detection & Response*
- *Policy Audit & Enforcement*
- *Session monitoring & control*
- *Information Protection & Data Loss Prevention (DLP)*

## Identity & Access

**Conditional Access** – Zero Trust Access Control decisions based on explicit validation of user trust and endpoint integrity

## Endpoints & Devices

**Microsoft Endpoint Manager**
Unified Endpoint Management (UEM)
Intune | Configuration Manager

**Microsoft Defender for Endpoint**
Unified Endpoint Security
- Endpoint Detection & Response (EDR)
- Web Content Filtering
- Threat & Vuln Management
- Endpoint Data Loss Protection (DLP)
- •••

## Hybrid Infrastructure – IaaS, PaaS, On-Premises

**Azure Security Center –** Cross-Platform Cloud Security Posture Management (CSPM)

Secure Score
Compliance Dashboard
•••

*On Premises Datacenter(s)* | *3rd party IaaS & PaaS* | Microsoft Azure

Extranet: NGFW, Edge DLP, IPS/IDS

**Azure AD App Proxy** *Beyond User VPN*

aws •••

Azure Marketplace •••

Express Route

Private Link

Intranet: Azure Arc, Azure Stack

java, JBoss, .net, php •••

Azure Firewall & Firewall Manager
Azure WAF
DDoS Protection
Azure Key Vault
Azure Bastion
Azure Lighthouse
Azure Backup
••• *Security & Other Services*

## Information Protection

*Classification Labels*

Azure Purview

Microsoft Information Protection (MIP)
Discover → Classify → Protect → Monitor

File Scanner *(on-premises and cloud)*

•••

Data Governance

Advanced eDiscovery

Compliance Manager

## Azure Active Directory

Passwordless & MFA
- Hello for Business
- Authenticator App
- FIDO2 Keys

Identity Protection
Leaked cred protection
Behavioral Analytics
•••

Azure AD PIM

Identity Governance

Azure AD B2B & B2C

Defender for Identity

Active Directory

**Securing Privileged Access –** Secure Accounts, Devices, Intermediaries, and interfaces to enable and protect privileged users

**Privileged Access Workstations (PAWs) -** Secure workstations for administrators, developers, and other sensitive users

**Microsoft Secure Score –** Measure your security posture, and plan/prioritize rapid improvement with included guidance

**Microsoft Compliance Score –** Prioritize, measure, and plan improvement actions against controls

**Windows 10 Security**

| | |
|---|---|
| *Network protection* | *App control* |
| *Credential protection* | *Exploit protection* |
| *Full Disk Encryption* | *Behavior monitoring* |
| *Attack surface reduction* | *Next-generation protection* |

•••

## IoT and Operational Technology (OT)

Azure Sphere

Azure Defender for IoT
- *ICS, SCADA, OT*
- *Internet of Things (IoT)*
- *Industrial IoT (IIoT)*
- *Asset & Vulnerability management*
- *Threat Detection & Response*

**Azure Defender –** Cross-Platform, Cross-Cloud XDR
*Multi-asset detection and response for infrastructure and platform as a service (IaaS & PaaS), Proactive Threat defenses*

•••

## People Security

Attack Simulator | Insider Risk Management | Communication Compliance

**GitHub Advanced Security –** Secure development and software supply chain

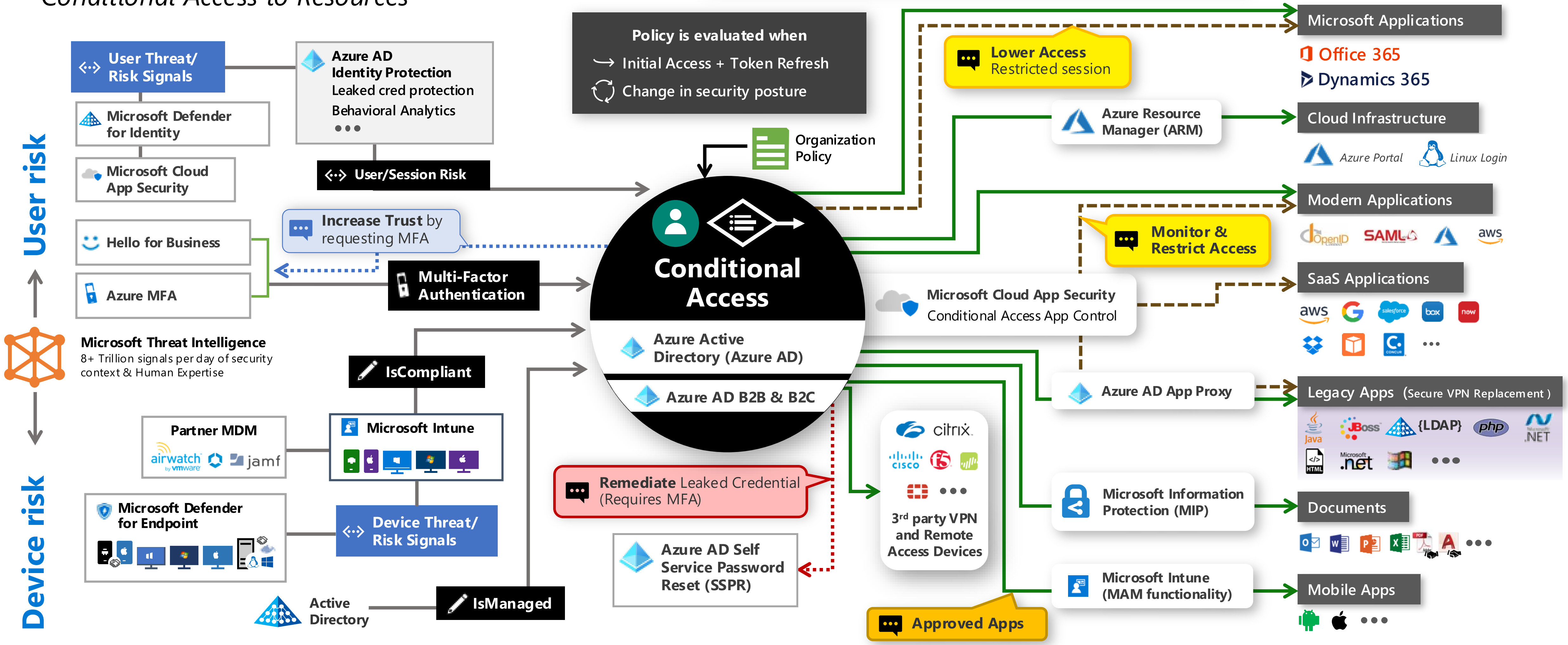
# Zero Trust User Access

*Conditional Access to Resources*

**Legend**

Full access — Limited access

Risk Mitigation — Remediation Path


User risk
User Threat/ Risk Signals
Microsoft Defender for Identity
Microsoft Cloud App Security
Azure AD Identity Protection
Leaked cred protection
Behavioral Analytics
•••
User/Session Risk
Hello for Business
Azure MFA
Increase Trust by requesting MFA
Multi-Factor Authentication
Microsoft Threat Intelligence
8+ Trillion signals per day of security context & Human Expertise
Device risk
IsCompliant
Partner MDM
airwatch by vmware
jamf
Microsoft Intune
Microsoft Defender for Endpoint
Device Threat/ Risk Signals
Active Directory
IsManaged
Policy is evaluated when
Initial Access + Token Refresh
Change in security posture
Organization Policy
Conditional Access
Azure Active Directory (Azure AD)
Azure AD B2B & B2C
Remediate Leaked Credential (Requires MFA)
Azure AD Self Service Password Reset (SSPR)
citrix
cisco
•••
3rd party VPN and Remote Access Devices
Approved Apps
Lower Access Restricted session
Azure Resource Manager (ARM)
Monitor & Restrict Access
Microsoft Cloud App Security Conditional Access App Control
Azure AD App Proxy
Microsoft Information Protection (MIP)
Microsoft Intune (MAM functionality)
Microsoft Applications
Office 365
Dynamics 365
Cloud Infrastructure
Azure Portal
Linux Login
Modern Applications
OpenID
SAML
aws
SaaS Applications
aws
salesforce
box
now
•••
Legacy Apps (Secure VPN Replacement )
Java
JBoss
{LDAP}
php
.NET
HTML
.net
•••
Documents
•••
Mobile Apps
•••

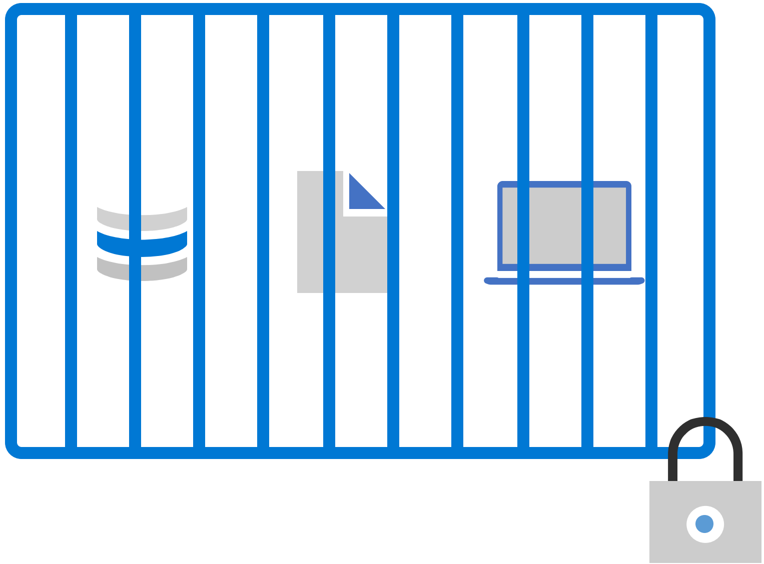
**Signal**
to make an informed decision

**Decision**
based on organizational policy

**Enforcement**
of policy across resources

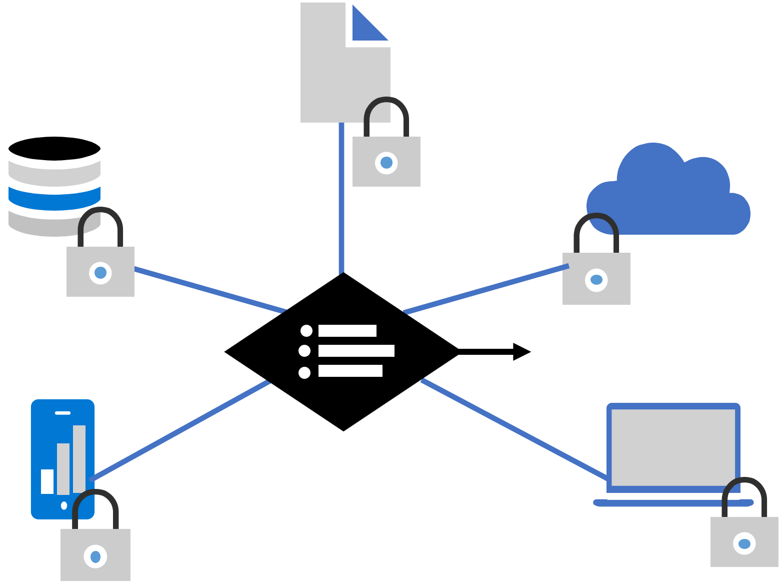
# Secure assets where they are with Zero Trust

Simplify security and make it more effective



**Classic Approach**

Restrict everything to a 'secure' network



**Zero Trust**

Protect assets anywhere with central policy

netnordic
THE BEST COMPANION

# END POINT SECURITY – ZERO TRUST

Zero trust Policy
ISO27001 Policy's
Data classification

## End Point Security

Patching of software, Local Admin lock, Defender for endpoint, MDM

## Password Protection

Forcing password penetration test, Password policy, fraud detection

## Email Protection

Attachments, Spoof, links

## Authentication

Multi Factor Authentication, Single sign on (SSO)

## Automated Provisioning

Provisioning users to applications, access rights and dynamic Groups

## Network and Traffic analytics

Monitoring of Firewalls, network traffic and AI on user behaviour

## Security awareness

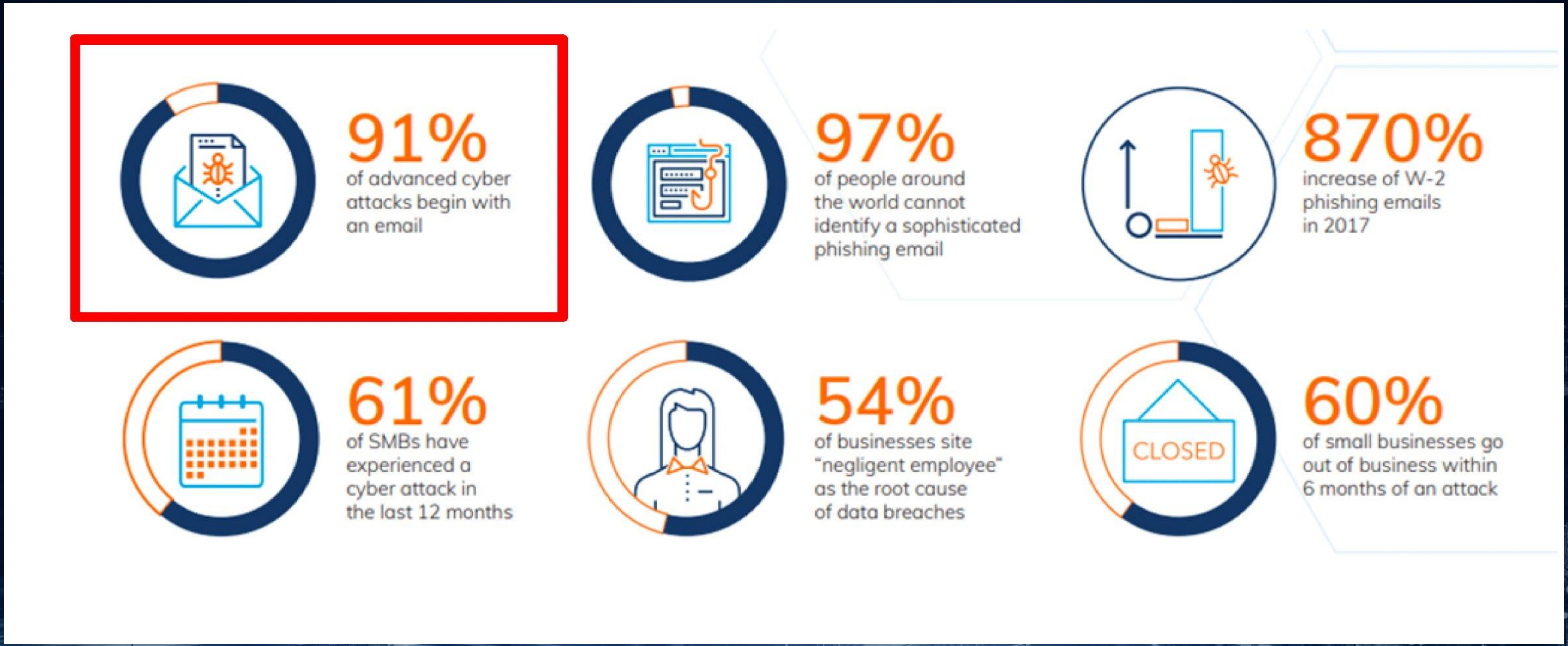
Education, fraud simulations and Security Awareness Monitoring

SOC

netnordic
THE BEST COMPANION

## Email is the #1 attack vector

Over 90& of cyber-attacks begin with an email



91% of advanced cyber attacks begin with an email

97% of people around the world cannot identify a sophisticated phishing email

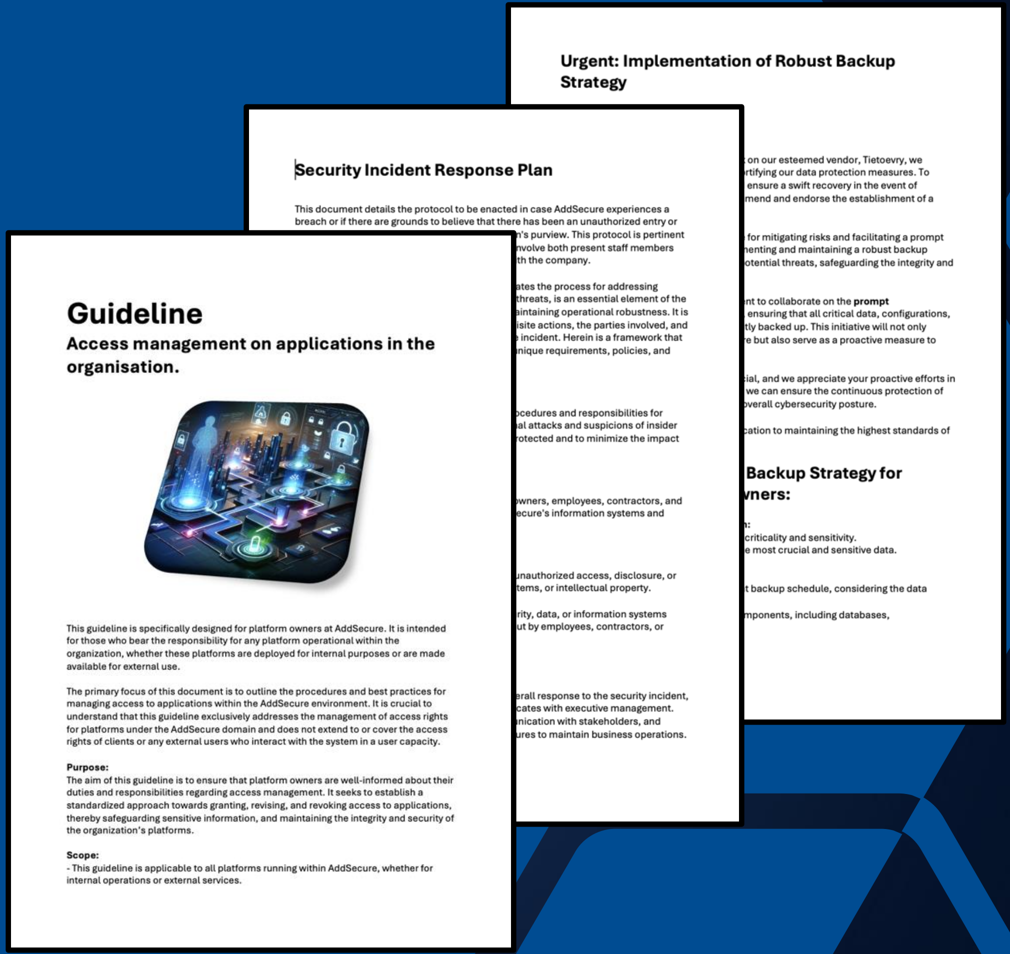
870% increase of W-2 phishing emails in 2017

61% of SMBs have experienced a cyber attack in the last 12 months

54% of businesses site "negligent employee" as the root cause of data breaches

60% of small businesses go out of business within 6 months of an attack

# Security Guides



## Guideline

### Access management on applications in the organisation.

This guideline is specifically designed for platform owners at AddSecure. It is intended for those who bear the responsibility for any platform operational within the organization, whether these platforms are deployed for internal purposes or are made available for external use.

The primary focus of this document is to outline the procedures and best practices for managing access to applications within the AddSecure environment. It is crucial to understand that this guideline exclusively addresses the management of access rights for platforms under the AddSecure domain and does not extend to or cover the access rights of clients or any external users who interact with the system in a user capacity.

**Purpose:**
The aim of this guideline is to ensure that platform owners are well-informed about their duties and responsibilities regarding access management. It seeks to establish a standardized approach towards granting, revising, and revoking access to applications, thereby safeguarding sensitive information, and maintaining the integrity and security of the organization's platforms.

**Scope:**
- This guideline is applicable to all platforms running within AddSecure, whether for internal operations or external services.

## Security Incident Response Plan

This document details the protocol to be enacted in case AddSecure experiences a
breach or if there are grounds to believe that there has been an unauthorized entry or
n's purview. This protocol is pertinent
nvolve both present staff members
th the company.

ates the process for addressing
threats, is an essential element of the
aintaining operational robustness. It is
isite actions, the parties involved, and
incident. Herein is a framework that
nique requirements, policies, and

ocedures and responsibilities for
al attacks and suspicions of insider
rotected and to minimize the impact

wners, employees, contractors, and
ecure's information systems and

unauthorized access, disclosure, or
tems, or intellectual property.

rity, data, or information systems
ut by employees, contractors, or

erall response to the security incident,
cates with executive management.
nication with stakeholders, and
ures to maintain business operations.

## Urgent: Implementation of Robust Backup Strategy

on our esteemed vendor, Tietoevry, we
rtifying our data protection measures. To
ensure a swift recovery in the event of
mend and endorse the establishment of a

for mitigating risks and facilitating a prompt
nenting and maintaining a robust backup
otential threats, safeguarding the integrity and

nt to collaborate on the **prompt**
ensuring that all critical data, configurations,
tly backed up. This initiative will not only
e but also serve as a proactive measure to

ial, and we appreciate your proactive efforts in
we can ensure the continuous protection of
overall cybersecurity posture.

cation to maintaining the highest standards of

### Backup Strategy for
### wners:

**n:**
criticality and sensitivity.
e most crucial and sensitive data.

t backup schedule, considering the data

mponents, including databases,

We make sure you

# WORK SMARTER

netnordic
THE BEST COMPANION