Security in Microsoft Cloud

Ole Tom Seierstad & Henrik Linnestad
Cloud services offer significant value to the public sector

Improved cost efficiency
Near limitless scaling
Improved security
Reduced energy consumption and carbon footprint
Higher flexibility and adaptability of solutions
Higher rate of innovation
Hva skal til for at norske byer og kommuner skal lykkes i å bli smarte?

Salangen-ordfører Sigrun Wiggen
Prestbakmos 7 tips til kommuner som vil i gang med en digital transformasjon

1. Stikk fingeren i jorda og gjør en grundig vurdering av teknologisk kapital.

2. Gå sammen med nabokommuner for å dele kompetanse og investeringer.

3. Be om å få besøke bedrifter og andre kommuner og høst inspirasjon fra hvordan de har digitalisert.


5. Invester i ny teknologi fremfor å reparere på gammel, for å møte kravene til digitalisering og utnytte mulighetene det gir.


7. Vær sprekk, romslig og fremtidsretta. Utforski hva teknologien kan gi organisasjon og innbyggere, bruk fagenhetenes kompetanse til å definere behov, og tenk "utafor boksen".

Norske kommuner som tar steget helt ut i nettskyen!

Samarbeidskommunene Salangen, Lavangen og Gratangen (K4) er de første kommunene i Norge som tar steget helt ut i Microsofts offentlige nettsky (Office 365 og Azure). Med sine tilsammen ca. 4.500 innbyggere og en IKT-avdeling med 2 ansatte, anser de dette som sin beste mulighet til å kunne innfri kravene i KS sin digitaliseringsstrategi, «Digitaliseringsstrategi 2013-2016 for kommuner og fylkeskommuner»

Oppdatert 29.06.18: Første fase av dette prosjektet er nå levert, her kan du se video og lese mer om leveransen.

Alt i nettskyen

Den skrittvisede IKT-plattformen til KS-kommunene er på gang og tildels utdelt. Frahaut
Compliance and security issues slow down cloud adoption

Kilde: Rambøll (2018), IT i praksis
Move your customer data in-country

Existing Office 365 customers can migrate to their in-country datacenter geo

- Benefit from a seamless migration at no cost
- Migrate your Exchange Online, SharePoint Online and OneDrive for Business data content
- Enroll after GA. Eligibility is determined by signup country

Learn more about Office 365 Move Program in your country: aka.ms/move

*Customer data as described in the 'Location of Customer Data at Rest' section of Microsoft Online Services Terms (OST)*
PROTECT

Defense-in-Depth
- Monitoring and controls
- Identity and Access management
- Proper hygiene
- Security Development Lifecycle
- Data encryption

Microsoft Security posture

RESPOND

Closing the gap between discovery and action

DETECT

Extensive signal fabric
- Cloud scale intelligence
- Machine learning
- Behavioral monitoring
WHAT MUST BE **PROTECTED**?

- Identity
- Device
- Applications & data
- Infrastructure
Common concerns about the cloud

Is my content safe in your data centers?

Who has access to my organization’s content in the service?

What visibility do I have into the activity on my content in the service?

Can I encrypt everything so that it’s not possible for you to have access to my content?
Microsoft spends $1B+ on security R&D every year
These challenges require a UNIFIED RESPONSE
Microsoft CYBER DEFENSE OPERATIONS CENTER

- Centralized hub for cybersecurity and defense; uniting personnel, technology, and analytics
- 24 x 7 x 365 protection of Microsoft’s cloud infrastructure, customer-facing cloud services, products and devices, and internal resources
- 50+ Security experts and Data scientists
- Connected to 3500+ security professionals across Microsoft
- Closed-loop engineering: discoveries inform Security Development Lifecycle (SDL), Microsoft Research and drives better protection in products and cloud services
Microsoft Intelligent Security Graph
Unique insights, informed by trillions of signals

- **400B** emails analyzed
- **1.2B** devices scanned each month
- **200+** global cloud consumer and commercial services
- **930M** threats detected on devices every month
- **Botnet data from Microsoft Digital Crimes Unit**
- **Enterprise security for 90% of Fortune 500**
- **750M+ Azure user accounts**
- **18B+ Bing web pages scanned**
- **450B** monthly authentications

Shared threat data from partners, researchers, and law enforcement worldwide

Microsoft accounts

Outlook

OneDrive

Windows

Bing

Xbox Live

Azure

Microsoft
Intelligent Security Graph

- Malware Protection Center
- Cyber Hunting Teams
- Security Response Center
- Digital Crimes Unit
- Cyber Defense Operations Center

- Conditional Access
- Cloud App Security
- Event Management
- Rights Management
- Key Vault
- Security Center

- Active Protection Service
- Windows Update
- Office 365 Advanced Threat Protection
- SmartScreen

- Advanced Threat Analytics
- Azure Active Directory
- Active Directory
- Office 365
- PaaS
- IaaS
- SaaS

- Identity
- Apps and Data
- Infrastructure
- Device
CLOUD-POWERED CONDITIONAL ACCESS

**IF**
- Privileged user?
- Credentials found in public?
- Accessing sensitive app?
- Unmanaged device?
- Malware detected?
- IP detected in Botnet?
- Impossible travel?
- Anonymous client?

**THEN**

**User risk**
- High
- Medium
- Low

**Session risk**
- High
- Medium
- Low

**Actions**
- Allow access
- Require MFA
- Force password reset
- Deny access
- Limit access
Why Machine Learning? polymorphism

- 96% malware seen once and never again
- 3% seen 2-10
- 0.4% seen 11-100
- 0.01% seen on 1001+

Distribution curve of malicious downloads affecting more than one target

Download traffic:

<table>
<thead>
<tr>
<th>Hours</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Shared Responsibility for Workloads (based on Cloud Service Model)

<table>
<thead>
<tr>
<th>Responsibility</th>
<th>SaaS</th>
<th>PaaS</th>
<th>IaaS</th>
<th>On-prem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data governance &amp; rights management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client endpoints</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account &amp; access management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity &amp; directory infrastructure</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating system</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical hosts</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical network</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical datacenter</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Always retained by customer**

**Varies by Service Type**
- SaaS – App Configuration
- PaaS – App Code + Configuration
- IaaS – Operating System + Middleware + App Code + Configuration

**Transfers to Cloud Provider**
Examples of Shared Responsibilities

NIST 800-53

**ACCESS TO PRODUCTION ENVIRONMENT**
Set up access controls that strictly restrict standing access to customer’s data or production environment

**PROTECT DATA**
Encrypt data at rest and in transit based on industrial standards (BitLocker, TLS, etc.)

**PERSONNEL CONTROL**
Strict screening for employees, vendors, and contractors, and conduct trainings through onboarding process

**Microsoft’s responsibility**

**ACCESS TO PRODUCTION ENVIRONMENT**
Set up access control policy and SOP, leveraging Customer Lockbox / identity management solutions

**PROTECT DATA**
Encrypt data based on org’s compliance obligations. E.g. encrypt PII in transit between users, using its own encryption key, etc.

**PERSONNEL CONTROL**
Allocate and staff sufficient resources to implement and operate an organization-wide privacy program, including awareness-raising and training
Layered security approach

CUSTOMER MANAGED
- Service Encryption
- Azure Active Directory / MFA / Conditional Access
- Threat Management (EOP, ATP, TI, ASM)
- Mobile Device Management (EMS)
- Message Encryption and Rights Management
- Data Governance and classification controls

MICROSOFT MANAGED
- Secure Development Lifecycle
- DDos protection
- Multi-tenancy
- Incident response/CDOC
- Lockbox
- Access approval
- Perimeter
- Building
- Server environment
- Data-bearing device controls
## Shared Responsibility and Key Strategies

<table>
<thead>
<tr>
<th>Responsibility</th>
<th>SaaS</th>
<th>PaaS</th>
<th>IaaS</th>
<th>On-prem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information and Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Devices (Mobile and PCs)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accounts and Identities</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity and directory infrastructure</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Applications</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating system</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical hosts</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical network</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical datacenter</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Establish a Modern Perimeter**

**Modernize Infrastructure Security**

**“Trust but Verify” Each Cloud Provider**
THE TRUSTED CLOUD

Azure has the deepest and most comprehensive compliance coverage in the industry

GLOBAL

ISO 27001
ISO 27018
ISO 27017
ISO 22301
ISO 9001
SOC 1 Type 2
SOC 2 Type 2
SOC 3
CSA STAR Self-Assessment
CSA STAR Certification
CSA STAR Attestation

US GOV

FedRAMP
FedRAMP
DoD DISA SRG Level 2
DoD DISA SRG Level 4
DoD DISA SRG Level 5
NIST
SP 800-171
FIPS 140-2
Section 508 VPAT
ITAR
CJIS
IRS 1075

INDUSTRY

PCI DSS Level 1
CDSA
MPAA
FACT UK
Shared Assessments
FISC Japan
HIPAA / HITECH Act
HITRUST
GxP 21 CFR Part 11
MARS-E
IG Toolkit UK
FERPA
GLBA
FFIEC

REGIONAL

Argentina PDec
EU Model Clauses
UK G-Cloud
China JDPC
China GB 18030
China TRUCS
Singapore MTCS
Australia IRAP/CCSL
New Zealand GCIO
Japan My Number Act
ENISA IAF
Japan CS Mark Gold
Spain ENS
Spain DPA
India MoITY
Canada Privacy Laws
Privacy Shield
Germany IT Grundschutz workbook
Microsoft infrastructure investments

54 regions worldwide

140 available in 140 countries

* Two Azure Government Secret region locations undisclosed
Compliance Manager
Manage your compliance from one place

Ongoing risk assessment
An intelligent score reflects your compliance posture against regulations and standards

Actionable insights
Recommended actions to improve your data protection capabilities

Simplified compliance
Streamlined workflow across teams and richly detailed reports for auditing preparation

Compliance Manager is a dashboard that provides the Compliance Score and a summary of your data protection and compliance status as well as recommendations to improve data protection and compliance. This is a recommendation, it is up to you to evaluate and validate the effectiveness of customer controls as per your regulatory environment. Recommendations from Compliance Manager and Compliance Score should not be interpreted as a guarantee of compliance.
Expanded Scope for Compliance Manager

CLOUD SERVICES

Office 365 | Microsoft Azure | Microsoft Dynamics 365

REGULATIONS AND STANDARDS

NIST
National Institute of Standards and Technology
U.S. Department of Commerce
800-171

NIST
National Institute of Standards and Technology
U.S. Department of Commerce
800-53

NIST
National Institute of Standards and Technology
U.S. Department of Commerce
Cybersecurity Framework

FedRAMP
Federal Risk Authorization Management Program

CSA
Cloud Security Alliance

CCM™
Cloud Controls Matrix

ISO
International Organization for Standardization

1. Information Security Management System
2. Information Security Management System

HIPAA
Health Insurance Portability and Accountability Act

GDPR
General Data Protection Regulation

FFIEC
Federal Financial Institutions Examination Council

*Coverage of regulations and standards in Compliance Manager varies by product.*
### Office 365 in-Scope Cloud Services

The services listed here are included in the Office 365 certification:

- Exchange Online
- SharePoint Online
- Skype for Business
- Microsoft Teams
- Microsoft PowerApps
- Office Delve
- Office 365 Groups
- Office 365 Video
- Sway
- Microsoft StaffHub
- Microsoft Booking
- Microsoft Graph API
- Microsoft MyAnalytics
- Microsoft Planner
- Microsoft Stream

### Microsoft Managed Controls

#### Office 365 Access Control Control Family

<table>
<thead>
<tr>
<th>MS Control</th>
<th>Certification Control(s)</th>
<th>Description</th>
<th>Status</th>
<th>Test Date</th>
<th>Test Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-0100</td>
<td>GDPR: A.05.01.01, A.06.02.01, A.06.02.02, A.09.01.01, A.11.02.09, A.13.02.01</td>
<td>The organization develops, documents, and disseminates to Service Engineer Operations, Service Engineer Operations (GCC), Program Managers, Developers, Testers, Office 365 Trust team Program Managers, Office 365 Security Managers, and Business Continuity Management, an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.</td>
<td>Implemented</td>
<td>4/29/2016</td>
<td>Passed</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Tested By Third Party Independent Auditor</td>
<td></td>
</tr>
<tr>
<td>AC-0101</td>
<td>GDPR: A.13.02.01</td>
<td>The organization develops, documents, and disseminates to Service Engineer Operations, Service Engineer Operations (GCC), Program Managers, Developers, Testers, Office 365 Trust team Program Managers, Office 365 Security Managers, and Business Continuity Management, procedures to facilitate the implementation of the access control policy and associated access controls;</td>
<td>Implemented</td>
<td>4/29/2016</td>
<td>Passed</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Tested By Third Party Independent Auditor</td>
<td></td>
</tr>
</tbody>
</table>
Microsoft has implemented an account lockout for Office 365 of 5 failed attempts in 15 minutes, rather than the FedRAMP value of 3 failed attempts in 15 minutes, using Active Directory Group Policy. Microsoft has adopted this alternative implementation as an operational requirement of Office 365 in order to ensure system availability, especially during non-business hours.

Microsoft believes that the more restrictive value of 3 attempts exposes a risk to the availability of the system. Operational experience has shown that on-call personnel may inadvertently lock themselves out during non-business hours, resulting in delayed service response times.

Microsoft’s internal risk evaluations found that account lockout after 5 failed attempts in 15 minutes provides the best balance of risk from the threat of account breaches against risk of delayed service response times. Also, allowing 2 additional login attempts prior to lockout does not increase the likelihood of a successful brute-force attack.

The FedRAMP Organizational Defined Values require accounts to be locked after three failed access attempts within fifteen minutes. Workload threat modeling indicates that the risk of a denial-of-service that negatively affects system availability as a result of locking admin accounts exceeds the risk of loss of system confidentiality due to multiple failed login attempts. Workloads log and alert off of excessive failed login attempts and can take manual actions to prevent brute force access attempts even if the account does not automatically lock.

Microsoft believes that the more restrictive value of 3 attempts exposes a risk to the availability of the system. Operational experience has shown that on-call personnel may inadvertently lock themselves out during non-business hours, resulting in delayed service response times.

Microsoft’s internal risk evaluations found that account lockout after up to 10 failed attempts in 15 minutes provides the best balance of risk from the threat of account breaches against risk of delayed service response times. Also, allowing 2 additional login attempts prior to lockout does not increase the likelihood of a successful brute-force attack.
### Office 365 in-Scope Cloud Services

<table>
<thead>
<tr>
<th>MS Control</th>
<th>Certification Control(s)</th>
<th>Description</th>
<th>Assigned To</th>
<th>Status</th>
<th>Test Date</th>
<th>Test Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-0100</td>
<td>GDPR: Article 15(3)</td>
<td>The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.</td>
<td>BG</td>
<td>Implemented</td>
<td>9/25/2017</td>
<td>Passed</td>
</tr>
</tbody>
</table>

**Necessary Customer Actions:**

**Implement Data Classification**
Classify data with Labels for governance and to enforce policy (retention, disposition, etc.) based on that classification.

https://protection.office.com/#/tagslibrary

**Execute Content Search**
Use Content Search in the Security & Compliance Center to find content that’s classified with a specific label in response to a specific data request (e.g. Data Subject, etc.)

**Test Plan & Management Response:**

1. Review business processes and workflow supporting data subject requests
2. Review data classification configuration to protect sensitive data subject to GDPR requirements.
3. Review content search performed to satisfy data subject requests.
Compliance Manager – Roadmap

Ongoing risk assessment
✓ Automated and continuous monitoring with Secure Score integration – Q2CY19
✓ Extensibility to assess non-Microsoft applications – Q2CY19

Actionable insights
✓ Benchmarking with industry / regional peers – Q4CY19
A practical and repeatable cloud assessment approach

Step 1: Identify stakeholders and decide on governance
Step 2: Choose an appropriate reference framework
Step 3: Risk profiling & scoping
Step 4: Assess risks, controls & review security
Step 5: Assess compliance (per country)
Step 6: Prepare exit plans
Step 7: Define risk action plans and approve service
Step 8: Notify financial & privacy supervisors

Modern Cloud Risk Assessment Process

http://aka.ms/RAGuide

Setup Cloud Governance (one-time)
Assess Cloud Deployment (repeat cycle)
Control: Encryption with customer control

1. **Encryption in transit**
   - Data in transit between a user and the service
     - Protects user from interception of their communication and helps ensure transaction integrity
   - Data in transit between data centers
     - Protects from bulk interception of data

2. **Encryption at rest**
   - Data at rest
     - Protects from removal of physical media
   - **End-to-end encryption of communications between users**
     - Protects from interception or loss of data in transit between users

3. **Customer controlled keys**
   - Content level Encryption

4. **Control**
Transparency and control: running the service

Most operations are automated

Data Center operations do not require access to customer content

Rare occasions where humans need access to run data center operations

Humans have to meet clearance requirements and require 2 factor auth to request access

Any access is highly controlled with multiple levels of approval using Lockbox
Customer Lockbox

Meet Compliance Needs
Customer Lockbox can help customers meet compliance obligations by demonstrating that they have procedures in place for explicit data access authorization.

Extended access Control
Use Customer Lockbox to control access to customer content for service operations.

Visibility into actions
Actions taken by Microsoft engineers in response to Customer Lockbox requests are logged and accessible via the Management Activity API and the Security and Compliance Center.

[Diagram showing the process flow of submitting a request,审批, and approval.]
Transparency

Know where **your data is stored.**

Understand **who has access your data** and **under what circumstances.**

**Monitor** the state of your service, get historic view of uptime.

**Integrate** security events’ feeds into your company security dashboard.

Gain insight with access to **service dashboards & operational reporting.**
Privacy

Customer is **the owner** of their data

We **do not mine customer data** for advertising purposes

**Privacy controls** enable you to configure your company privacy policies

Microsoft **advocates for data privacy** on behalf of customers

Microsoft safeguards customer data with **strong contractual commitments**
Operational security

**Physical security** with 24-hour monitoring and multi-factor authentication

Admin **background checks**

**Zero-standing access** to data

**Data encryption** at-rest and in-transit

Red team / Blue team **penetration testing and incident response practice**

Product development using **Security Development Lifecycle**

**Bug bounty program** to identify vulnerabilities
Safeguarding your data

Identify, label, classify, set policies to help **protect information**.

Encrypt your data and restrict access using Azure Information Protection.

Safeguard information with Data Loss Prevention.

Get visibility into and improve your security position with Secure Score

Restrict unauthorized data sharing across apps with MAM.

Prevent data leaks with support for Windows Information Protection.

Manage data on devices through built-in MDM.

Securely communicate with customers using Message Encryption.
Compliance

Meet **compliance obligations** for data access with Customer Lockbox.

Monitor and investigate events related to your data with **full audit tracking**.

**Reduced cost and risk** with in-place intelligent Advanced eDiscovery.

Efficiently **perform risk assessment** with Service Assurance.

**Manage data retention** with Advanced Data Governance.
Cloud principles

It’s your data

You own it, you control it
We run the service for you
We are accountable to you

Built in security  Privacy by design  Continuous compliance

Transparent service operation
Thank You!
## Protecting Your Identities - Key Focus Areas

<table>
<thead>
<tr>
<th>Account Compromise</th>
<th>Account Abuse</th>
<th>Workstation Abuse</th>
<th>Monitoring &amp; Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect against the most prevalent account compromise techniques &amp; attacks</td>
<td>Prevent attackers using compromised accounts to move inside the network</td>
<td>Protect privileged access and combat insider threats by securing admin workstations</td>
<td>Detecting unexpected use of privileged accounts, logging and analysis</td>
</tr>
<tr>
<td>Next generation credentials to help eliminate passwords</td>
<td>Deploy credential theft mitigation techniques to limit lateral movement and elevation</td>
<td>Deploy and manage separate workstations for administrative tasks (physical or virtual)</td>
<td>Use solutions that can detect anomalous account behavior</td>
</tr>
<tr>
<td>Use multi-factor authentication to combat phishing</td>
<td>Limit the use of privileged accounts as far as possible</td>
<td>Lock down security settings on administrative workstations</td>
<td>Use intelligent instrumentation and threat analysis to establish a known-good baseline</td>
</tr>
<tr>
<td>Email sanitization to block unknown attacks from reaching the inbox</td>
<td>Use Just In Time admin/Just Enough admin to control and monitor access to data</td>
<td>Use application whitelisting to limit software that can be installed and run on admin workstations</td>
<td>Revoke unauthorized access to documents, wipe device data</td>
</tr>
</tbody>
</table>
## Protecting Your Devices – Key Focus Areas

<table>
<thead>
<tr>
<th>Security Basics</th>
<th>Access Controls</th>
<th>Management &amp; Policies</th>
<th>Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry-standard security fundamental practices</td>
<td>Use modern authentication technologies and controls to better secure access to devices</td>
<td>Further protect privileged access by securing administrative workstations</td>
<td>Use world class encryption to protect data on devices</td>
</tr>
<tr>
<td>Software/firmware update management</td>
<td>Next generation credentials to help eliminate passwords</td>
<td>Separate workstations for administrative tasks</td>
<td>Full disk encryption where possible</td>
</tr>
<tr>
<td>Backup strategy</td>
<td>Secure boot processes to “prove” the device can be trusted</td>
<td>Lock down security settings on administrative workstations</td>
<td>Mobile devices as well as PCs</td>
</tr>
<tr>
<td>Use and update a trusted antimalware solution</td>
<td>Use multi-factor authentication to combat phishing</td>
<td>Application whitelisting</td>
<td>Identify and protect business data on personal (BYOD) devices</td>
</tr>
</tbody>
</table>
### Protecting Your Data & Applications - Key Focus Areas

<table>
<thead>
<tr>
<th>Data Classification</th>
<th>Data Access Controls</th>
<th>Management &amp; Policies</th>
<th>Data Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifying and managing data based on business impact</td>
<td>Policies and strategies for controlling access to sensitive data</td>
<td>Identifying and controlling data and applications across the enterprise</td>
<td>Tactics and techniques for protecting data if the environment is compromised</td>
</tr>
<tr>
<td>Data classification strategy and automation</td>
<td>Minimize and control privileged accounts and workstations</td>
<td>Cloud application awareness and discovery</td>
<td>Use world class encryption to protect data at rest, in transit, in operation</td>
</tr>
<tr>
<td>High Value Asset protection</td>
<td>JIT/JEA to control and monitor access to sensitive data</td>
<td>Application whitelisting across the range of managed devices</td>
<td>Rights management &amp; data loss prevention</td>
</tr>
<tr>
<td>Data location policy</td>
<td>Backup and update management</td>
<td>Rights management and data loss prevention</td>
<td>Intelligent monitoring for exfiltration</td>
</tr>
</tbody>
</table>
## Protecting Your Infrastructure – Key Focus Areas

<table>
<thead>
<tr>
<th>Threat Intelligence</th>
<th>Inventory Management</th>
<th>Management &amp; Policies</th>
<th>Threat Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using information to help drive decisions</td>
<td>Strong hardware and software inventory management is key to success</td>
<td>Ensuring that the organization operates in accordance with security goals</td>
<td>Identifying, responding to and recovering from compromise, internal and external</td>
</tr>
<tr>
<td>Threat intelligence partners and feeds</td>
<td>Cloud application discovery &amp; management</td>
<td>JIT/JEA to control access to data</td>
<td>Anomalous behavior detection &amp; hunt teams</td>
</tr>
<tr>
<td>Automated intelligence analysis</td>
<td>Application whitelisting</td>
<td>Software supply chain security</td>
<td>Instrumentation, monitoring and analysis</td>
</tr>
<tr>
<td>Separation of business and private data</td>
<td>Network segmentation &amp; management</td>
<td>Active management of hardware and software including BYOD</td>
<td>Intelligent response and recovery</td>
</tr>
</tbody>
</table>
Backup slides - GDPR
SOLUTIONS TO HELP YOU
PREPARE FOR THE GDPR
The security capabilities you need, built into the products you already use

**Identity & access management**
Protect users’ identities & control access to valuable resources based on user risk level

- Azure Active Directory
- Conditional Access
- Windows Hello
- Windows Credential Guard

**Threat protection**
Protect against advanced threats and recover quickly when attacked

- Azure Advanced Threat Protection
- Windows Defender
- Advanced Threat Protection
- Office 365 Advanced Threat Protection
- Office 365 Threat Intelligence

**Information protection**
Ensure documents and emails are seen only by authorized people

- Azure Information Protection
- Office 365 Data Loss Prevention
- Windows Information Protection
- Microsoft Cloud App Security
- Office 365 Advanced Security Mgmt.
- Microsoft Intune

**Security management**
Gain visibility and control over security tools

- Azure Security Center
- Office 365 Security Center
- Windows Defender Security Center

Powered by the Intelligent Security Graph
How do I get started?

1. Discover  
   Identify what personal data you have and where it resides

2. Manage  
   Govern how personal data is used and accessed

3. Protect  
   Establish security controls to prevent, detect, and respond to vulnerabilities & data breaches

4. Report  
   Keep required documentation, manage data requests and breach notifications
Discover:
Identify what personal data you have and where it resides

In-scope:
Any data that helps you identify a person
- Name
- Email address
- Social media posts
- Physical, physiological, or genetic information
- Medical information
- Location
- Bank details
- IP address
- Cookies
- Cultural identity

Inventory:
Identifying where personal data is collected and stored
- Emails
- Documents
- Databases
- Removable media
- Metadata
- Log files
- Backups

Example solutions

- Microsoft Azure
  - Microsoft Azure Data Catalog
- Enterprise Mobility + Security (EMS)
  - Microsoft Cloud App Security
- Dynamics 365
  - Audit Data & User Activity
  - Reporting & Analytics
- Office & Office 365
  - Data Loss Prevention
  - Advanced Data Governance
  - Office 365 eDiscovery
- SQL Server and Azure SQL Database
  - SQL Query Language
- Windows & Windows Server
  - Windows Search
2 Manage:
Govern how personal data is used and accessed within your organization

Data governance:
Defining policies, roles and responsibilities for the management and use of personal data
- At rest
- In process
- In transit
- Storing
- Recovery
- Archiving
- Retaining
- Disposal

Data classification:
Organizing and labeling data to ensure proper handling
- Types
- Sensitivity
- Context / use
- Ownership
- Custodians
- Administrators
- Users

Example solutions
- Microsoft Azure
  Azure Active Directory
  Azure Information Protection
  Azure Role-Based Access Control (RBAC)
- Enterprise Mobility + Security (EMS)
  Azure Information Protection
- Dynamics 365
  Security Concepts
- Office & Office 365
  Advanced Data Governance Journaling (Exchange Online)
- Windows & Windows Server
  Microsoft Data Classification Toolkit
Protect:
Establish security controls to prevent, detect, and respond to vulnerabilities and data breaches

Preventing data attacks:
Protecting your data
- Physical datacenter protection
- Network security
- Storage security
- Compute security
- Identity management
- Access control
- Encryption
- Risk mitigation

Detecting & responding to breaches:
Monitoring for and detecting system intrusions
- System monitoring
- Breach identification
- Calculating impact
- Planned response
- Disaster recovery
- Notifying DPA & customers

Example solutions
Microsoft Azure
- Azure Key Vault
- Azure Security Center
- Azure Storage Services Encryption

Enterprise Mobility + Security (EMS)
- Azure Active Directory Premium
- Microsoft Intune

Office & Office 365
- Advanced Threat Protection
- Threat Intelligence

SQL Server and Azure SQL Database
- Transparent data encryption
- Always Encrypted

Windows & Windows Server
- Windows Defender Advanced Threat Protection
- Windows Hello
- Device Guard
4 Report:
Keep required documentation, manage data requests and breach notifications

**Record-keeping:**
Enterprises will need to record the:
- Purposes of processing
- Classifications of personal data
- Third-parties with access to the data
- Organizational and technical security measures
- Data retention times

**Reporting tools:**
Implement reporting capabilities
- Cloud services (processor) documentation
- Audit logs
- Breach notifications
- Handling Data Subject Requests
- Governance reporting
- Compliance reviews

---

**Example solutions**

- **Microsoft Trust Center**
  Service Trust Portal

- **Microsoft Azure**
  Azure Auditing & Logging
  Azure Data Lake
  Azure Monitor

- **Enterprise Mobility + Security (EMS)**
  Azure Information Protection

- **Dynamics 365**
  Reporting & Analytics

- **Office & Office 365**
  Service Assurance
  Office 365 Audit Logs
  Customer Lockbox

- **Windows & Windows Server**
  Windows Defender Advanced Threat Protection