A tailor-made support M365

Microsoft 365: The foundation for a new dimension of security for your organization

Microsoft 365

adista

Better be secured

1. Multi-factor authentication
   Conditional access
2. Email Defense Strategy
   Group management and O365 defense
3. Backup of the data
4. Mobile device management
5. Confidentiality, compliance and integrity of information assets

Customized support by adista

Better be authenticated

Multi-factor authentication
Conditional access

Email Defense Strategy
Group management and O365 defense

Backup of the data

Mobile device management

Confidentiality, compliance and integrity of information assets

Authentication methods

Trusted environments

Application and information system access profiles

Remote access connection strategy

Strategy for risky connections

Alert strategy and preventive actions

- Any Time
- Any Where
- Any Device
- Any Content
- Protect
- Govern
- Regulate
- Secure

adista

Secure authentication

Microsoft Authenticator

The use of multi-factor authentication has many advantages given the current issues related to the evolution of work methods, but also in the context of cybersecurity and new regulations in force.

Prevent cyber attacks

The MFA solution instantly secures data and IT resources against identity theft, account spoofing and phishing.

Promote employee mobility and productivity

Secure access to the organization's information system and applications or remote connection to the network via a VPN, without depending on specific hardware.

Comply with regulatory requirements

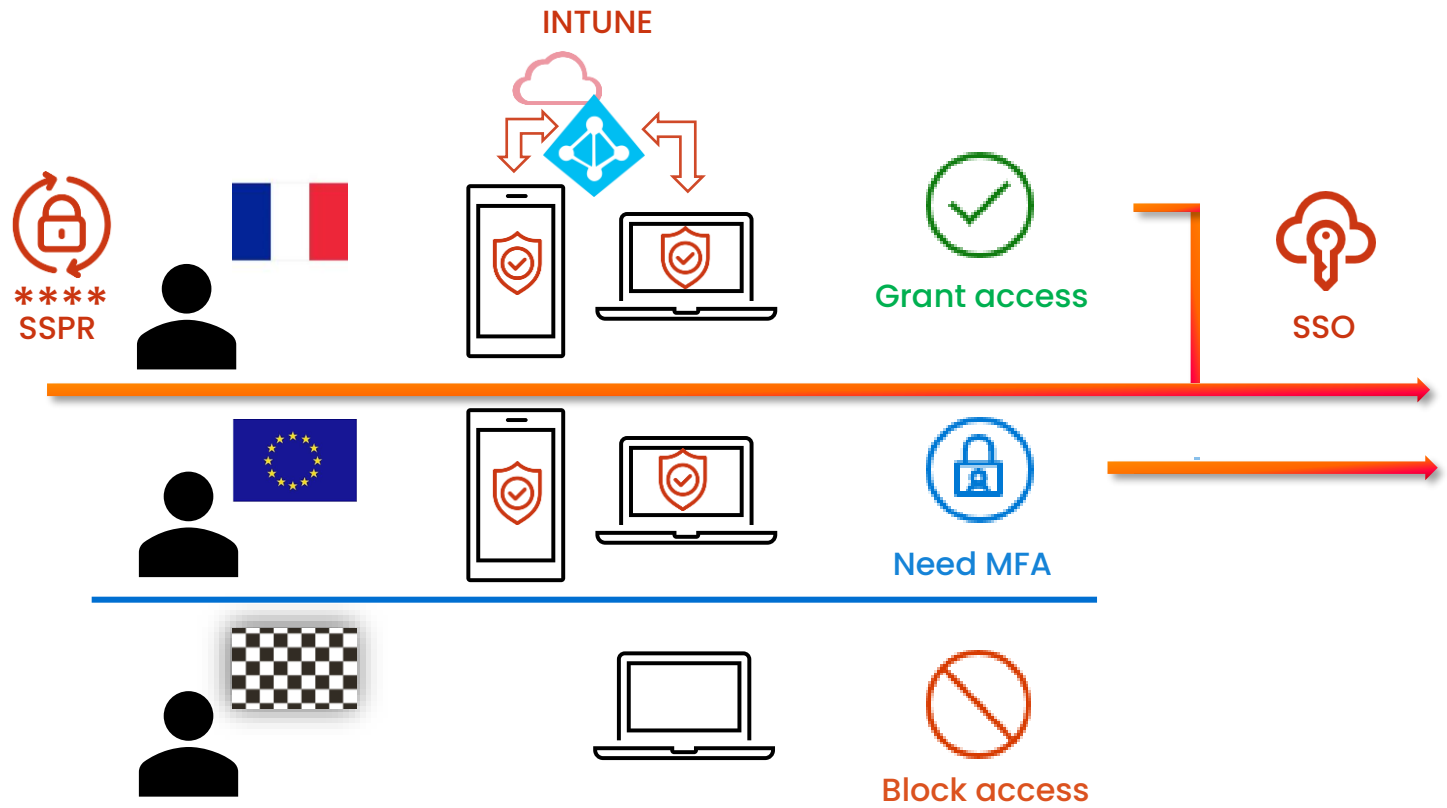
Data security regulations are becoming increasingly stringent, raising important compliance issues in the management and protection of personal and organizational data.

Enhanced User Experience

Simplify the login experience by enabling your users to log in quickly and easily, from any device, anywhere with or without passwords.

Conditional access

IMPROVE YOUR SECURITY



Microsoft Cloud

+ 3 000
Cloud SaaS apps

On-premises apps

Better be compliant

1

Multi-factor authentication
Conditional access

2

Email Defense Strategy
Group management and O365 defense

- Advanced email defense strategy
- Administrator role management
- External sharing strategy
- Cross-Tenant Collaboration / Synchronization
- Teams Lifecycle
- Security Group Strategy
- Teams creation strategy
- Mapping of user / group rights

3

Backup of the data

4

Mobile device management

5

Confidentiality, compliance and integrity of information assets

- Hidden URLs
- Redirections d'URL
- Altered Logos
- Usurpation of name
- Neighboring domain
- Remote images

adista

Email protection

vade

Faced with more and more sophisticated attacks, the protection of your mailboxes requires a new approach.

Vade uses artificial intelligence and especially machine learning to perform a real-time behavioral analysis of the origin, content and context of emails.

Full integration with the Microsoft 365 environment

Protection against phishing: Behavioral analysis based on machine learning algorithms allows the analysis and detection of fraudulent emails implementing bypass mechanisms based on signature analysis

Protection against spear phishing: Artificial intelligence, including anomaly detection and natural language processing, can identify identity theft attempts and malicious structures in fraudulent emails

Malware and ransomware prevention: Threat data from more than 1 billion mailboxes is leveraged to detect and block the most sophisticated malware and ransomware

Email security
COMPARATIVE

	Windows Defender EOP	Windows Defender ATP
Identified threats		
Basic signature-based protection	✓	✓
Blacklisted spam	✓	✓
Blacklisted malware	✓	✓
Blacklisted Phishing	✓	✓
Unidentified threats		
0 day Malware/Phishing/Spam Detection	✓	✓
Basic IP/Domain Name/URL Reputation	✓	✓
Machine learning & heuristics / basic	✓	✓
Reputation analysis / complex		✓
Anti-Phishing detection and protection		
Real-time URL scanning	✓	✓
Malicious URL Protection	✓	✓
Request for sensitive data	✓	✓
Detection of proven identity theft	✓	✓
Detection of a similar sender during spoofing	✓	✓
User Convenience		
Low priority email classification	✓	!
1-click unsubscribe	✓	✗
Advanced unsubscribe	✓	✗

EOP = Exchange Online Protection

ATP = Advance Threat Protection

! = Limited to spam only and not other low-priority messages (newsletters, social network notifications, etc.)

Better be saved

1

Multi-factor authentication
Conditional access

2

Email Defense Strategy
Group management and O365 defense

3

Backup of the data

4

Mobile device management

5

Confidentiality, compliance and integrity of information assets

Restore BACKUP service

Office 365
VEEAM

- Emails
- Contacts
- Calendars
- SharePoint
- Teams
- OneDrive

Your organization's data is valuable, it's important to back it up.

Microsoft 365 includes retention mechanisms.
In this context, Adista offers the Veeam Backup service that allows you to back up Exchange data (email, contact, calendar), Sharepoint (where your folders and files are stored), Teams, and users' personal OneDrive.

This service allows you to backup your data daily for 365 days

You retain ownership of your data at all times.

We can restore, transfer your data emails, files, ... in case of

Crash of your information system or Microsoft

Restore a set of deleted data

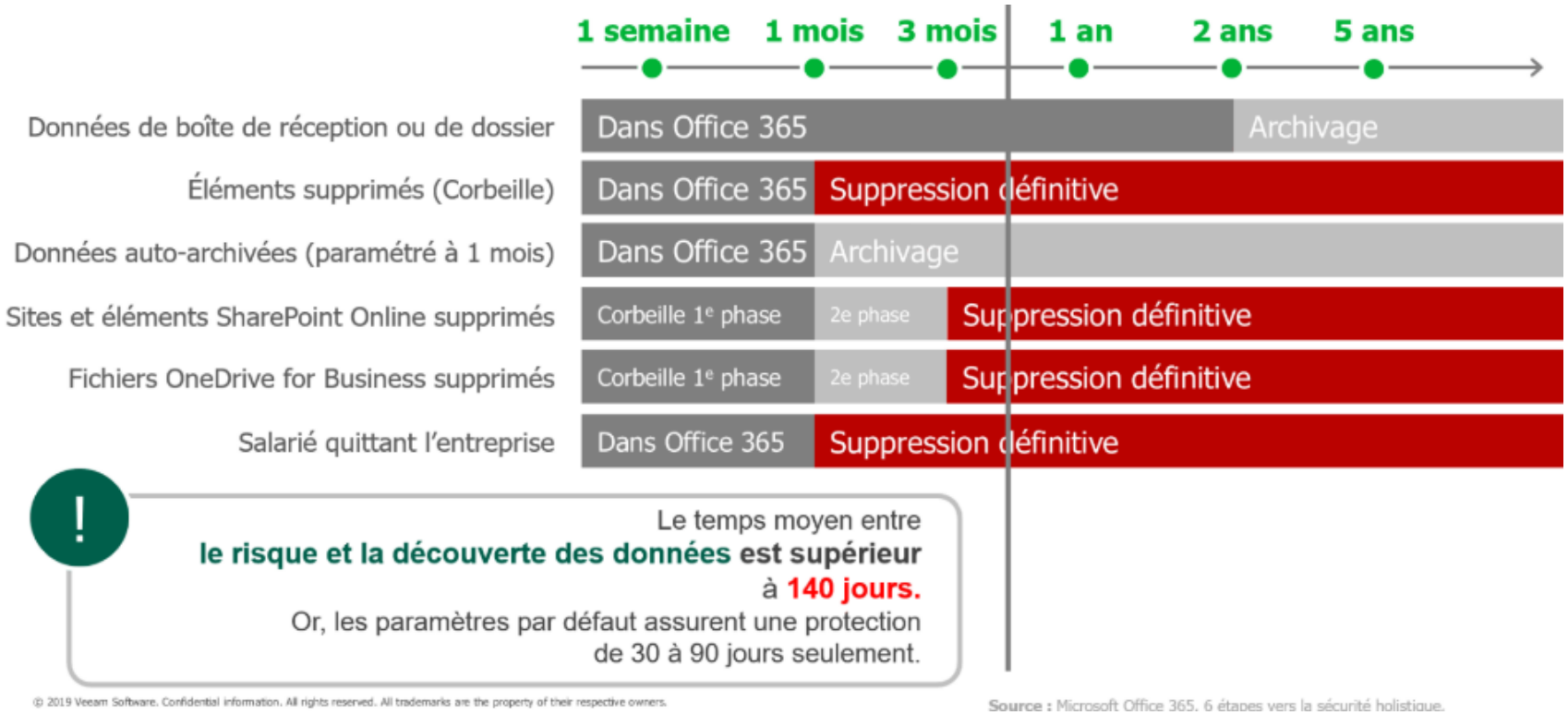
Fast" transfer of your data to a temporary holder following a hacking, ransomware, ...

Transfer of your data to another functional environment than Microsoft

adista

Retention strategies

WHAT EXACTLY IS MICROSOFT BACKUP?



Source : Microsoft Office 365. 6 étapes vers la sécurité holistique.

Better be managed

1

Multi-factor authentication
Conditional access

2

Email Defense Strategy
Group management and O365 defense

3

Backup of the data

4

Mobile device management

- Device compliance
- Data encryption
- Security by user profile
- Application deployment
- Remote inventory and management
- Autopilot Deployment

5

Confidentiality, compliance and integrity of information assets

Mobile Device Management

- Securing the equipment pool
- User profile management
- User access compliance
- Autopilot device deployment
- Application Deployment
- Easy inventory
- Zero Trust Strategy

Intune is an interoperable cloud service for providing comprehensive mobile device management.

Intune enables you to have a productive mobile workforce by eliminating security vulnerabilities inside and outside your organization.

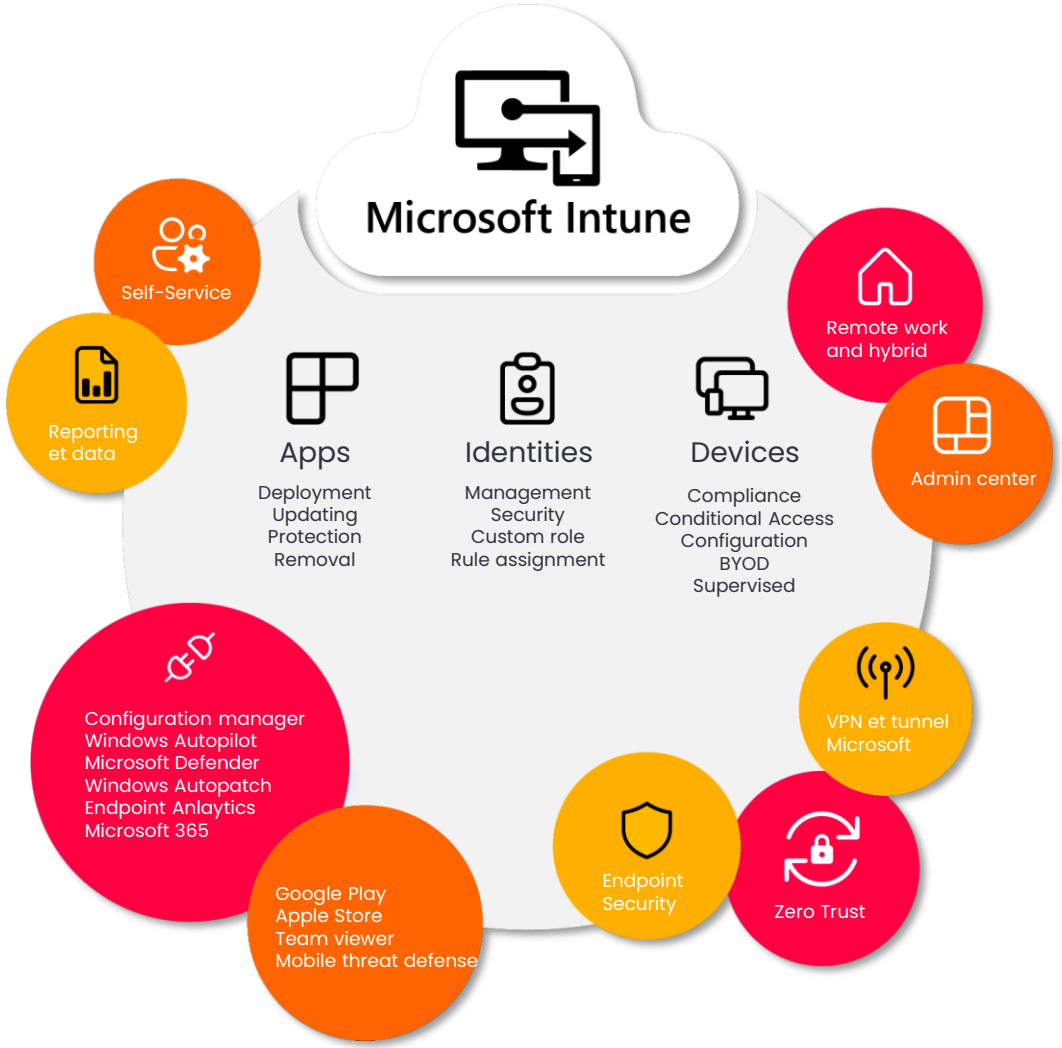
Define rules and configure policies for a range of devices, whether personal or organizationally supervised in a bring your own device (BYOD) mode

Control user and device access. Protect your organization's data by controlling what information users can access and what they can share.

Ensure that the devices used by your organization's members comply with your security requirements. If devices are not compliant, you can apply alerts, messages or automated actions to minimize risk.

adista

Microsoft Intune
WHAT EXACTLY DOES IT DO?



Better be confidential

Multi-factor authentication
Conditional access

Email Defense Strategy
Group management and O365 defense

Backup of the data

Mobile device management

Confidentiality, compliance and integrity of information assets

- Legal retention strategy
- Suspicious Activity Alert Strategy
- Strategy for auditing activity on the tenant
- Data Loss Strategy
- Data sensitivity strategy

- Securing shares
- Guest user access level
- Level of confidentiality
- Document life cycle
- Real-time alerts/actions
- Data loss prevention
- Encryption

adista

Data governance

Microsoft Azure
Information Protection

The multiplication of information channels and data sources implies a complex supervision.

Analyze your data

Identify important information in the cloud and your local environment.

Protect your data

Protect your data throughout its lifecycle by applying sensitivity labels linked to protective actions such as encryption, access restrictions, visual markings and more.

Prevent data loss

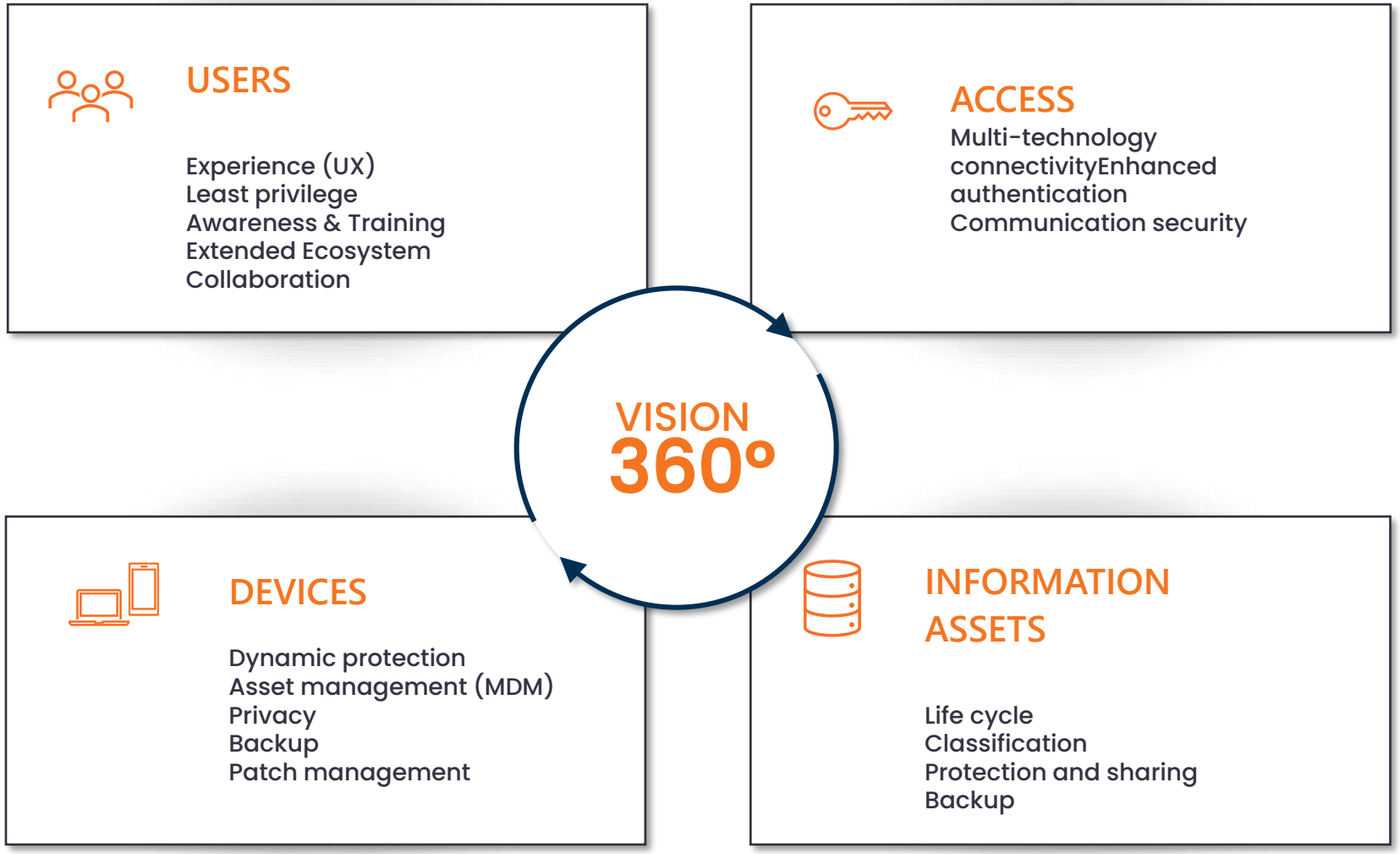
Apply a consistent set of data loss protection policies in the cloud, in your on-premises environments, and at your endpoints to monitor, prevent, and address risky activities involving sensitive data.

Govern your data

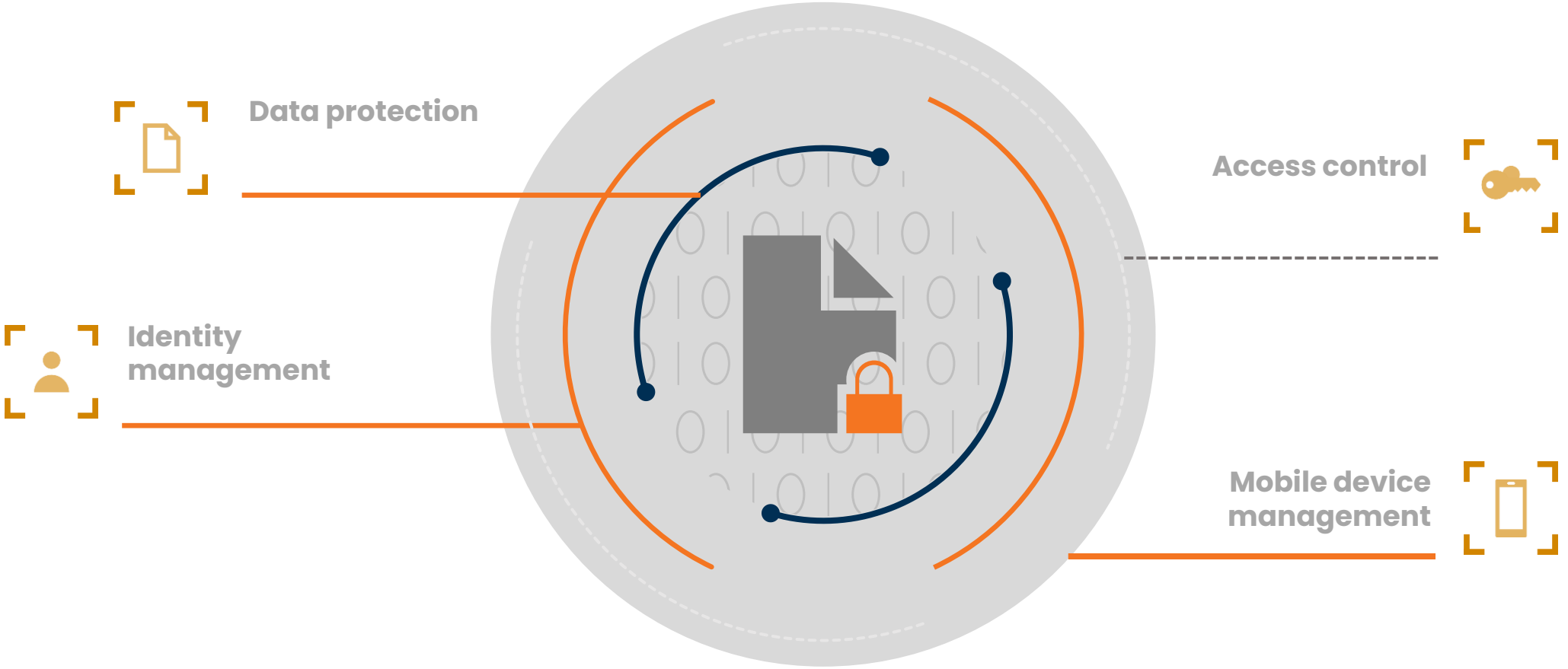
Manage the information lifecycle and records intelligently with on-premises management, automated policies, defensible destruction, and predefined data connectors.

Data governance

A CONFIDENTIALITY AND PREVENTION STRATEGY



Zéro trust
A DEFENSE IN DEPTH STRATEGY



Thanks