Establishing your Cybersecurity Strategy

David McCormick
Identify & Mobility Specialist
Microsoft Ireland

Top Technology Trends

Internet of Things

Integrated Devices & Ecosystems

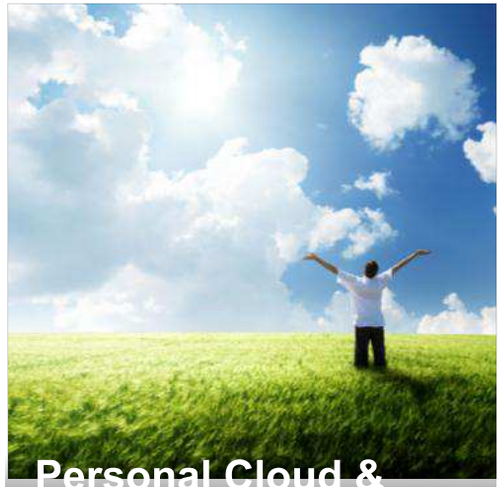
Cloud Computing

Strategic Big Data

In-Memory Compute Actionable Analytics

Enterprise Risk Mgt. & Cybersecurity

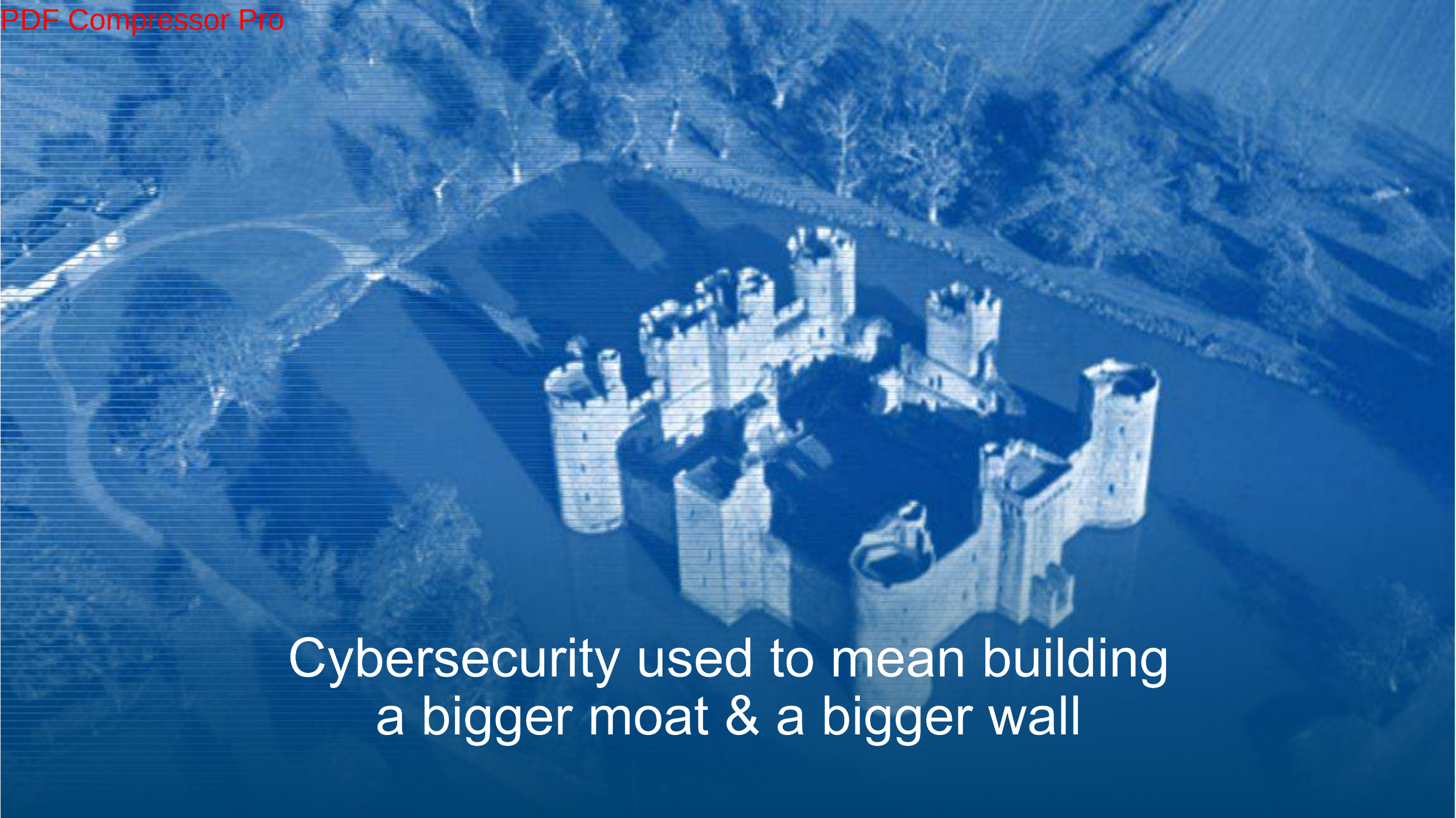
Enterprise App Stores & HTML5 Growth



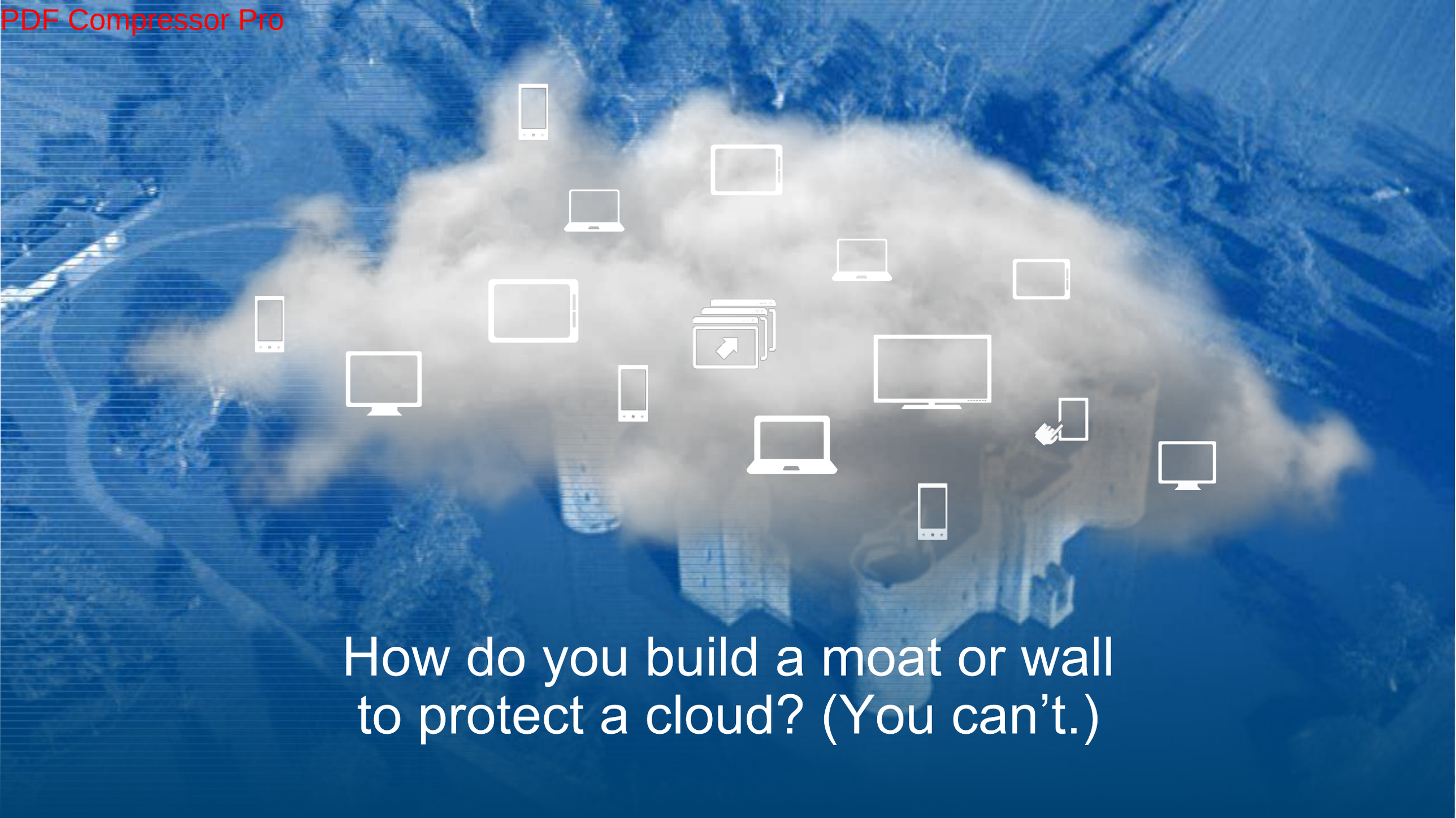
Personal Cloud & Seamless Device Exp.

Business & Niche Social Computing

Wearable Technology & Natural U.I.



Cybersecurity used to mean building
a bigger moat & a bigger wall



How do you build a moat or wall to protect a cloud? (You can’t.)

Complex Challenges

Driving need for new security approach

$1 Trillion

Global **cost of computer crime**

Malicious software

Exponential Growth of IDs

250% rise in **Mobile Malware**

Widespread **legacy technology**

Targeted attacks

More sophisticated **attacks**

5x more **compromised records**

Data theft & insider leaks

77 Million user accounts **stolen**

200,000 credit card accounts **stolen**

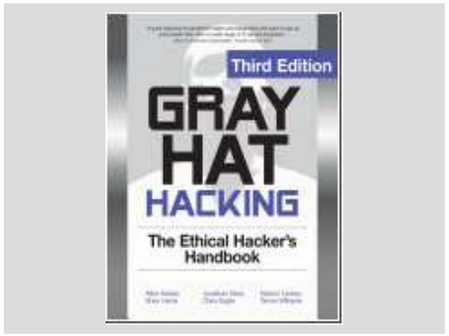
Cyber terrorism & hacktivism

90,000 **email addresses stolen** from US military contractor

24,000 **files stolen** from Pentagon

Threats & Actors: Moving from Fun to Cash

- Cyber-crime
- Cyber-espionnage
- Cyber-terrorism
- Cyber-war



There are 3 Categories of organizations,

Those who have been attacked, know & reported

Those who have been attacked, know & did not report

Those who don't know yet!

How Microsoft can help

Identity Security

Cloud is the "new normal"

Growing use of cloud services requires a smart Security & Identity foundation.

Assess your cloud Security & Identity readiness

Define and deploy your cloud identity

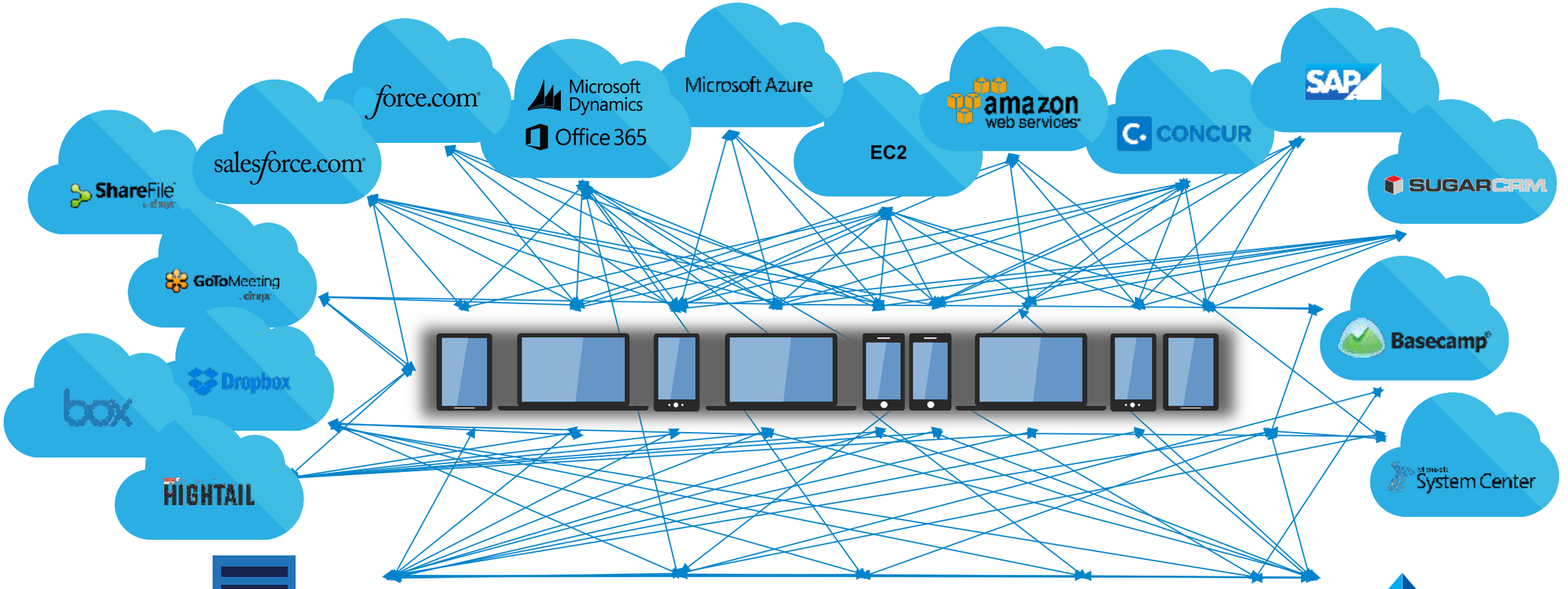
Implement the cloud security measures that fit your organization

Update your policies and **administration model**

Help **provide security** for your cloud administrators

Build added security into your cloud workloads

The current identity reality…

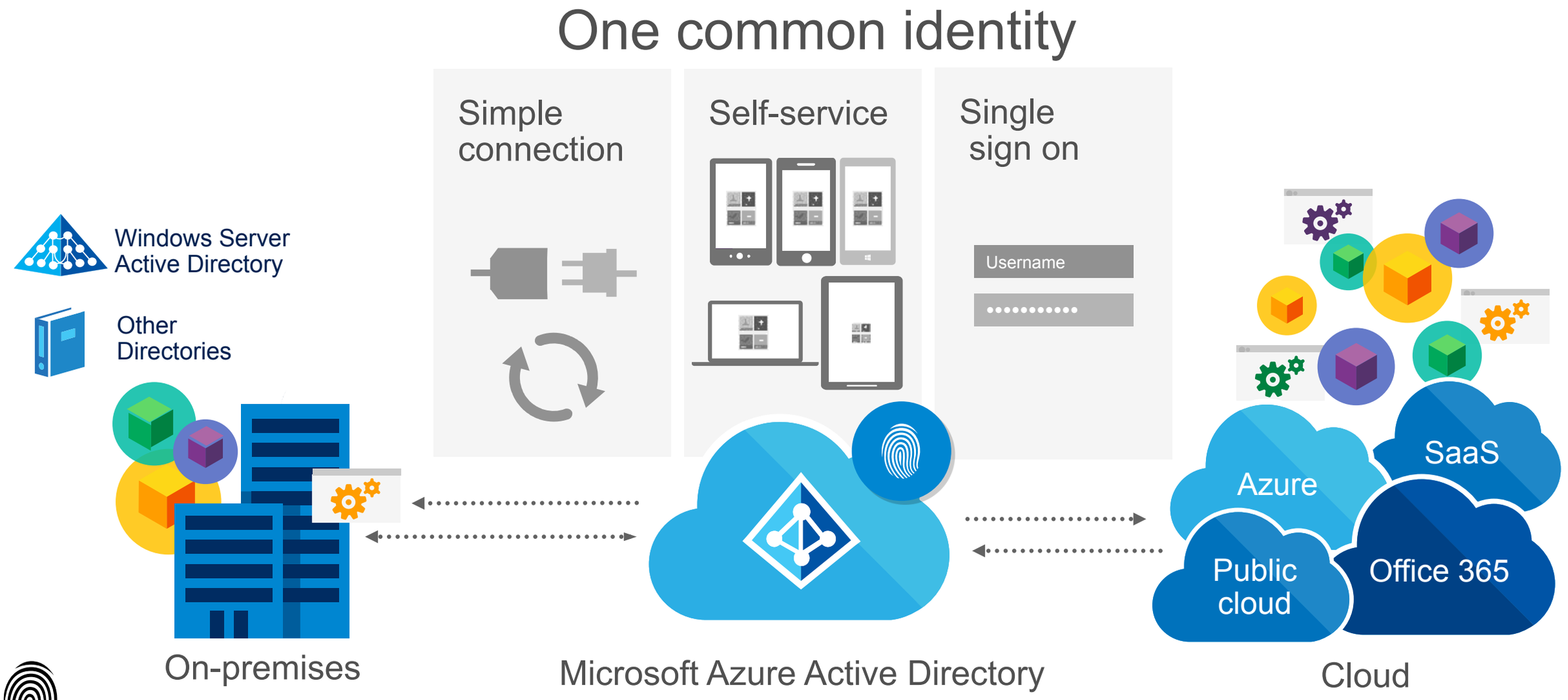


On-Premises

Managed devices

Private Cloud

Integrated Identity as the control plane



Identity Driven Security

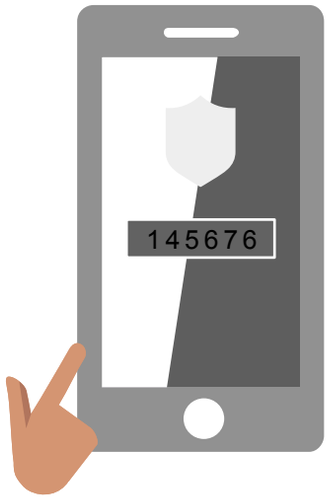
Intelligent cloud

Machine learning

Security reports

Privileged Identity Management

App security

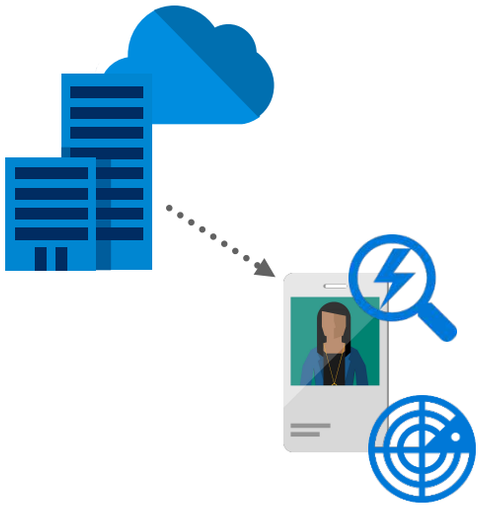


Conditional access

Multi-factor authentication

Cloud App Discovery

Detect threats



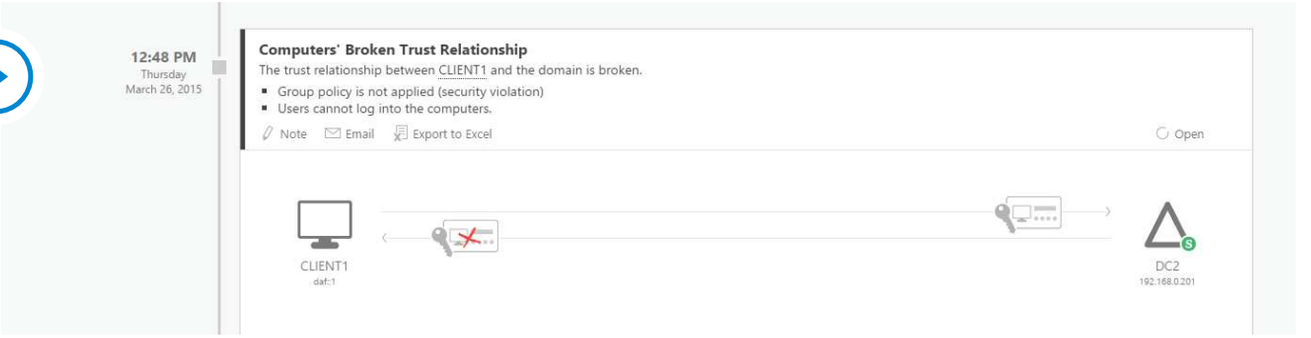
User behavioral analysis

Simple attack timeline

How Microsoft Advanced Threat Analytics works

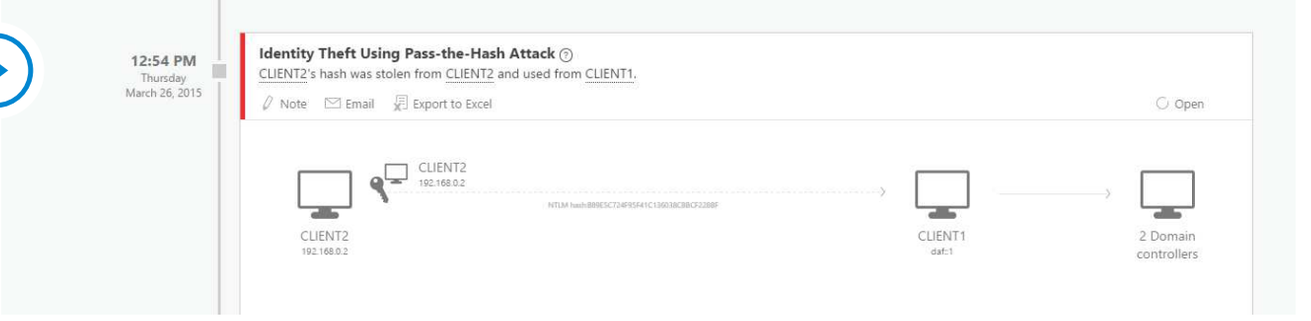
Security issues and risks

- Broken trust
- Weak protocols
- Known protocol vulnerabilities



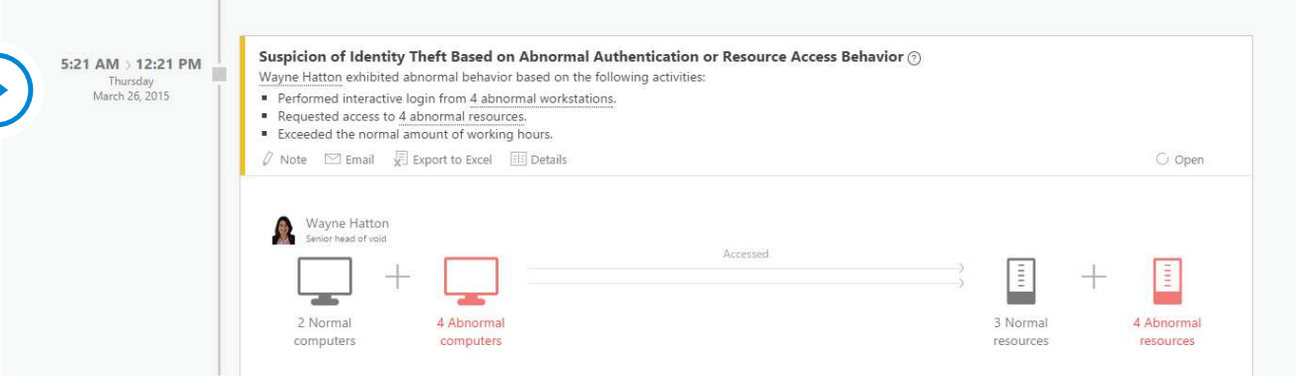
Malicious attacks

- Pass-the-Ticket (PtT)
- Pass-the-Hash (PtH)
- Overpass-the-Hash
- Forged PAC (MS14-068)
- Golden Ticket
- Skeleton key malware
- Reconnaissance
- BruteForce

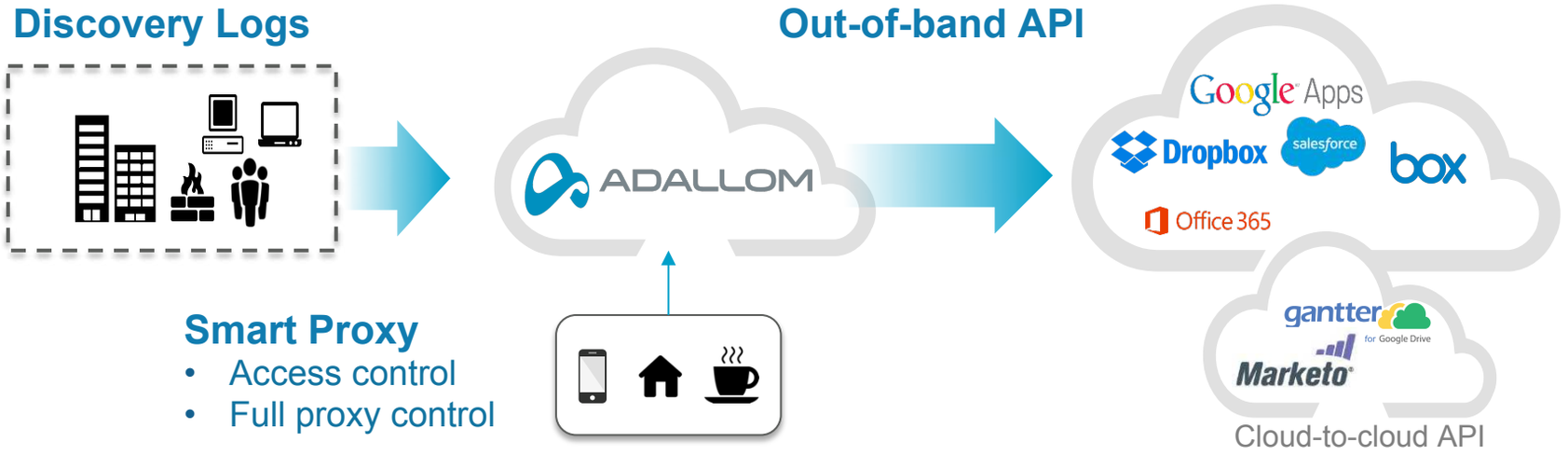


Abnormal Behavior

- Anomalous logins
- Remote execution
- Suspicious activity
- Unknown threats
- Password sharing
- Lateral movement



Deployment Overview



Phase 0: Discovery — Discovery of unsanctioned cloud apps

Phase 1: Governance & Security — Out-of-band governance and security

Phase 2: Access Control — In-line access controls *"Allow based on device (managed/ unmanaged), IP, location, user, role, posture"*

Phase 3: Session Controls — In-line session controls *"Allow Sales to download Box documents on unmanaged devices, but encrypt/IRM"*

Mobility Solutions

Mobility is a game changer

In order for modern IT to provide controlled access to the right services while minimizing the risk of leakage, the very foundations of your identity and security systems must be adapted to mobile devices through innovative supplemental capabilities

Define and deploy your mobile **identity**

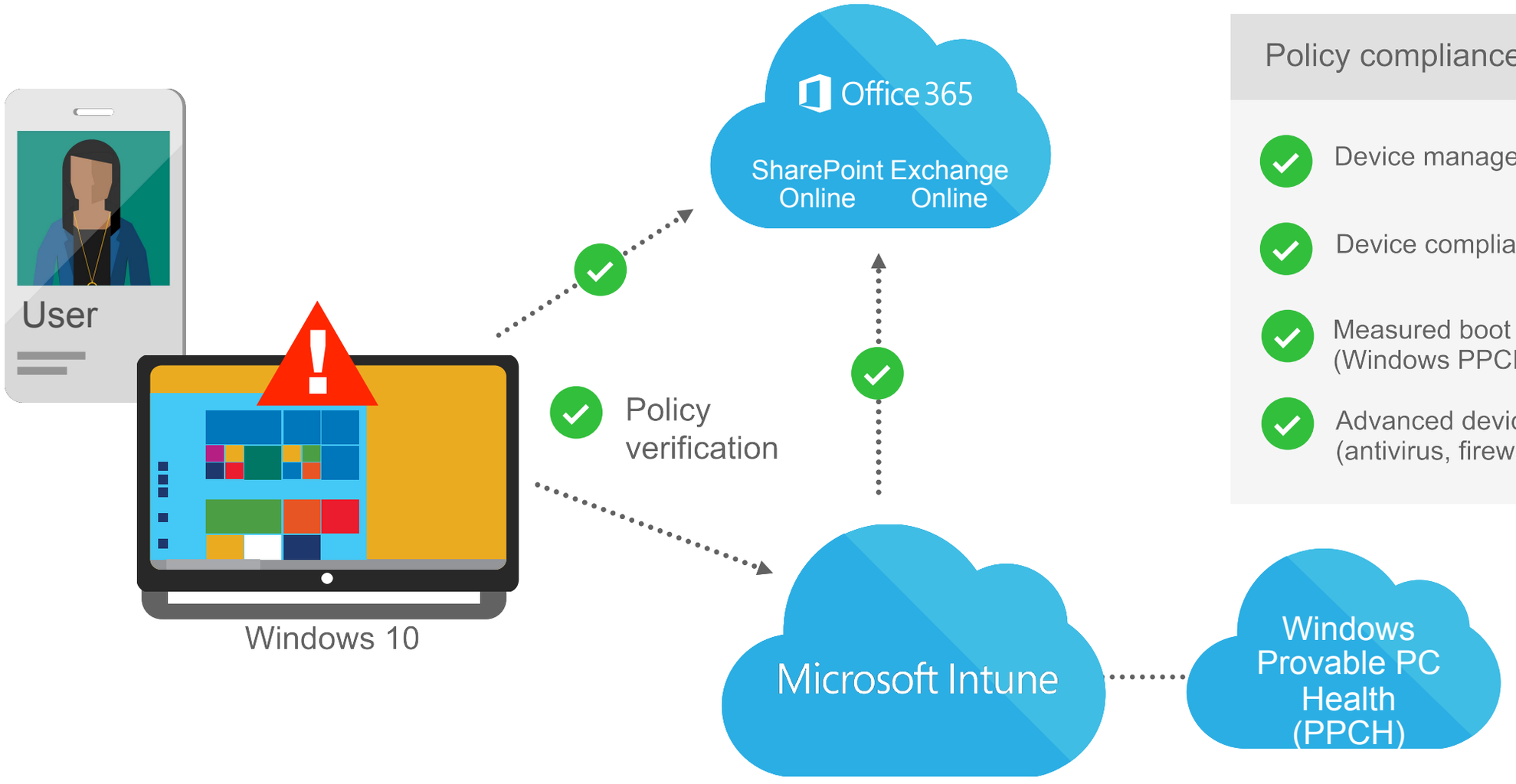
Help secure your data that is in transit or is stored on devices

Deploy
More secure devices

Manage your devices life cycle

Managed email and productivity

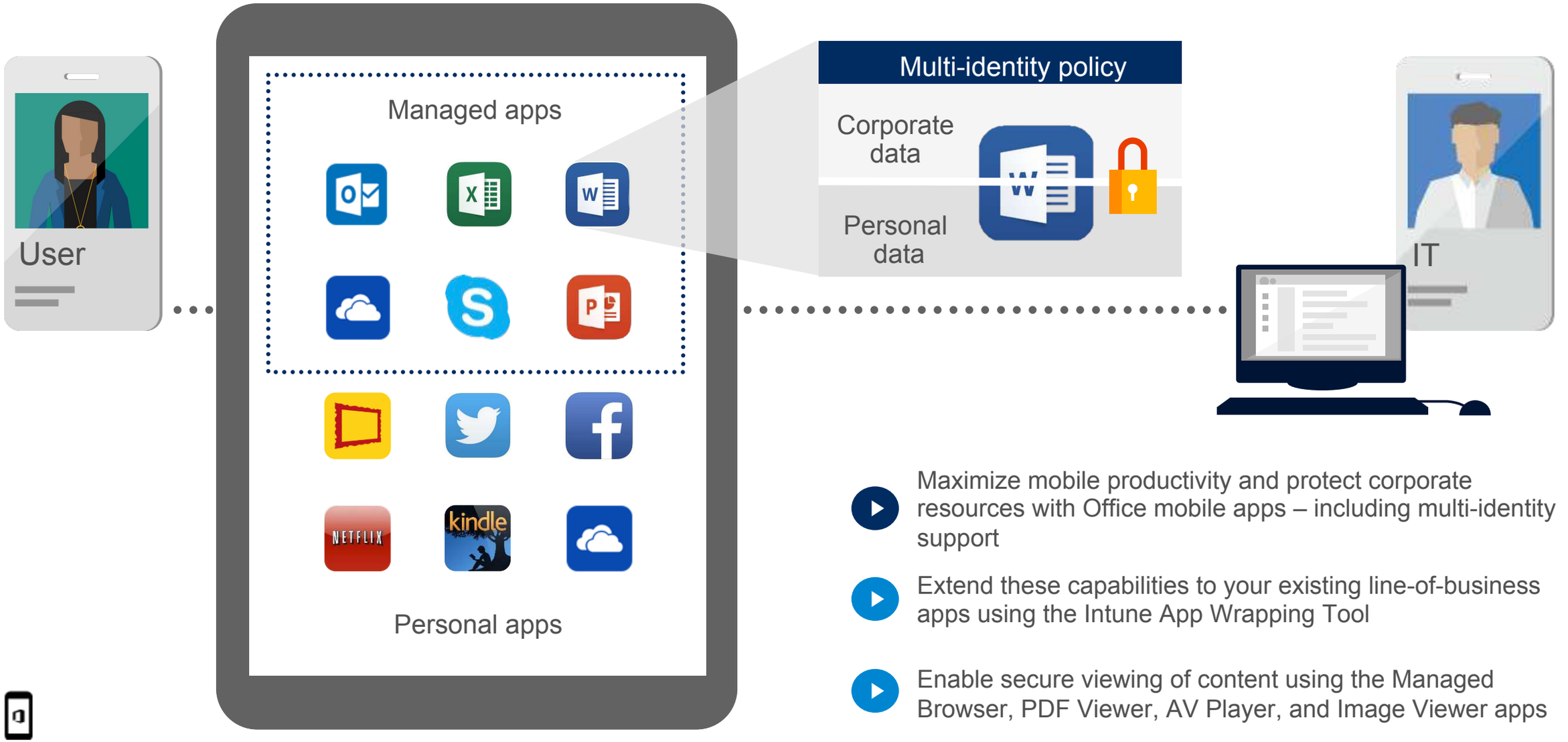
Conditional access



Policy compliance verification

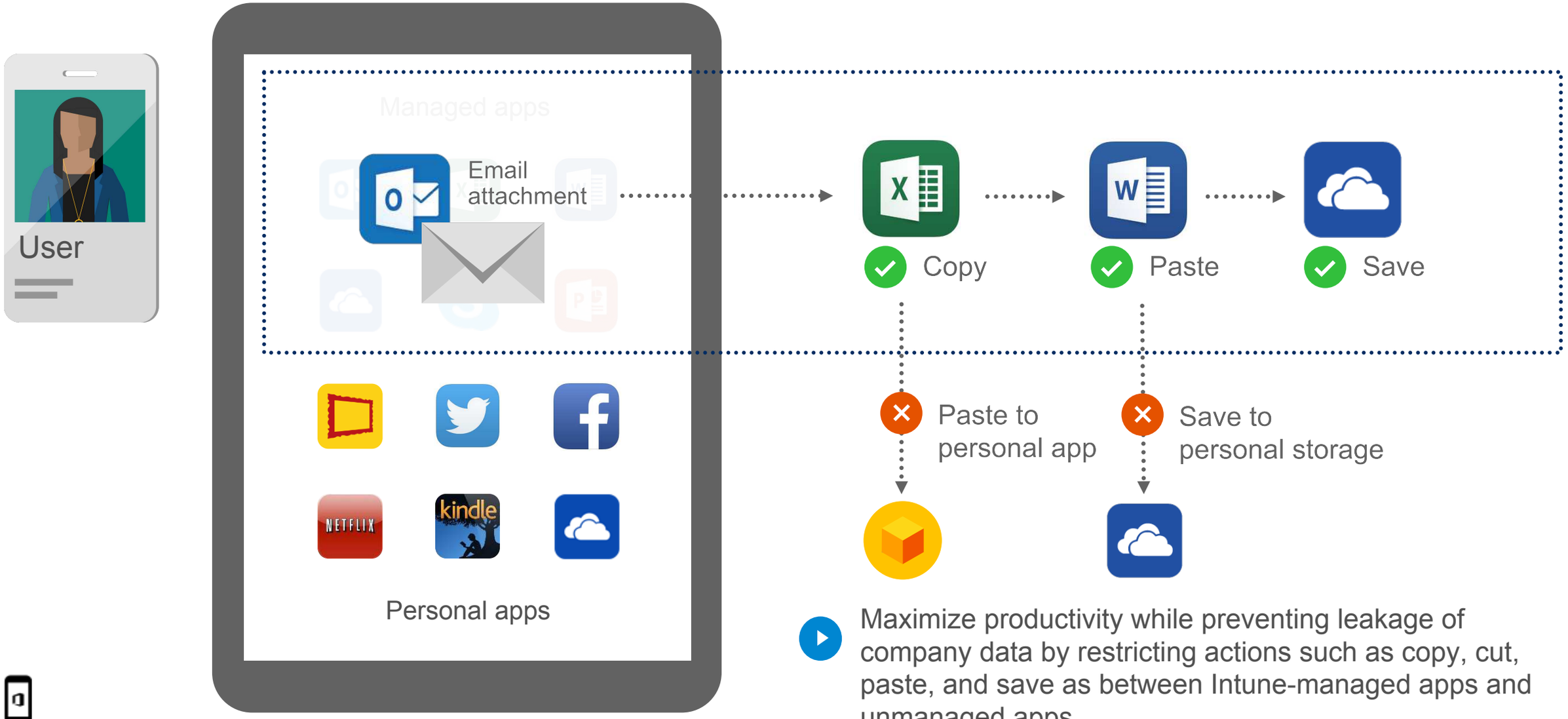
- Device management
- Device compliance
- Measured boot integrity status (Windows PPCH)
- Advanced device compliance (antivirus, firewall, patch state, etc.)

Mobile application management



- Maximize mobile productivity and protect corporate resources with Office mobile apps – including multi-identity support
- Extend these capabilities to your existing line-of-business apps using the Intune App Wrapping Tool
- Enable secure viewing of content using the Managed Browser, PDF Viewer, AV Player, and Image Viewer apps

Mobile application management



Information Protection

Information protection is at the nexus of the transformation

It is the solution to the diametrically opposed challenges of protecting intellectual property from rising threats and making it available from almost anywhere on any device.

Assess your critical data

Help **protect data** that is hosted on your infrastructure by using tailored solutions

Deploy secure devices for people who are processing data

Define and **apply security policies** to your data in motion

Concerns…

My existing DLP protection is too reactive. Can data be ‘born encrypted’?

IT must ‘reason over data’ to stay compliant, yet we need our sensitive data to be encrypted.

How do I prepare for a fading perimeter?

We want small steps to protect data now! We’re don’t want to slowly implement the ‘perfect grand solution’.

Data privacy is mandated!

Peer-to-peer federation is not practical or scalable. How do we establish ‘trust’?

Azure Rights Management

- Encryption
- Access control
- Policy enforcement
- Document tracking
- Document revocation
- Classification and labeling

Email

Files

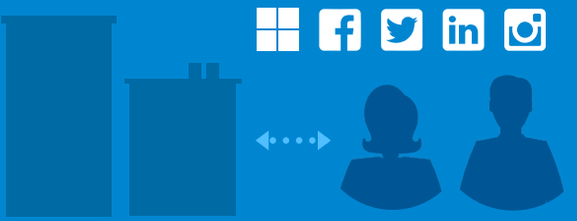
SAP

SIEMENS

LOB apps

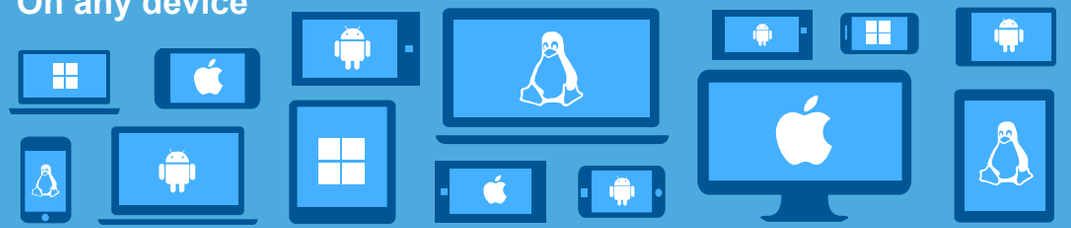
Share internally

Share externally (B2B)



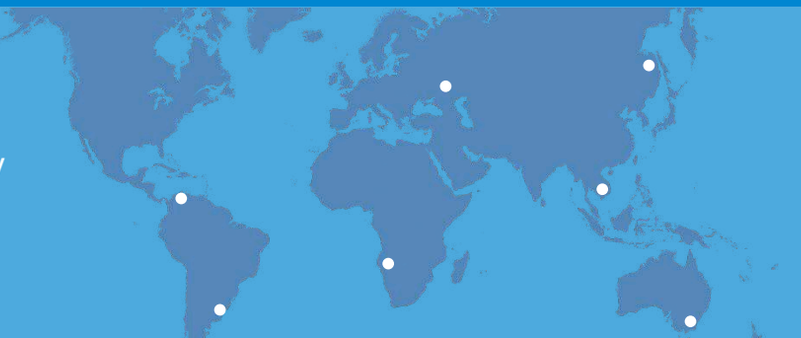
Share externally (B2C)

On any device



In any part of the world

- US
- EU
- APAC
- China
- Germany



Encrypt files and data

- Protect ANY File
- Share with ANY Person
- View on ANY Device
- Track & Manage from the cloud