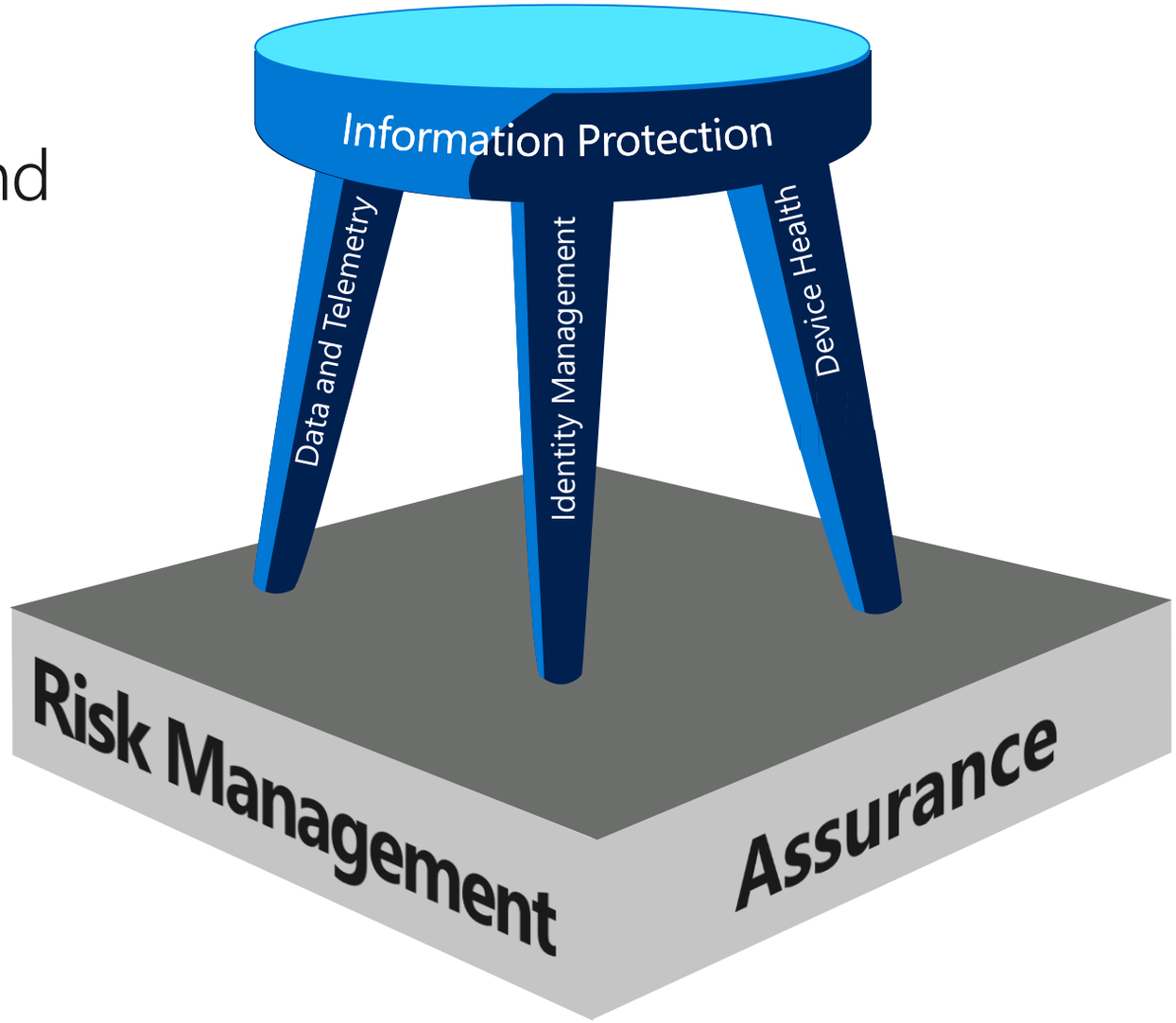
Speaking of security: Device health

Agenda

- Security focus
- Digital security strategy
- Security world view
- Why device health
- Where we are at
- Key investment areas
- Overcoming challenges
- Keeping up with evolving threats
- Goal state
- Key recommendations

Security focus

Balancing identity management, device health, data and telemetry, and information protection with risk management and assurance as the foundation.

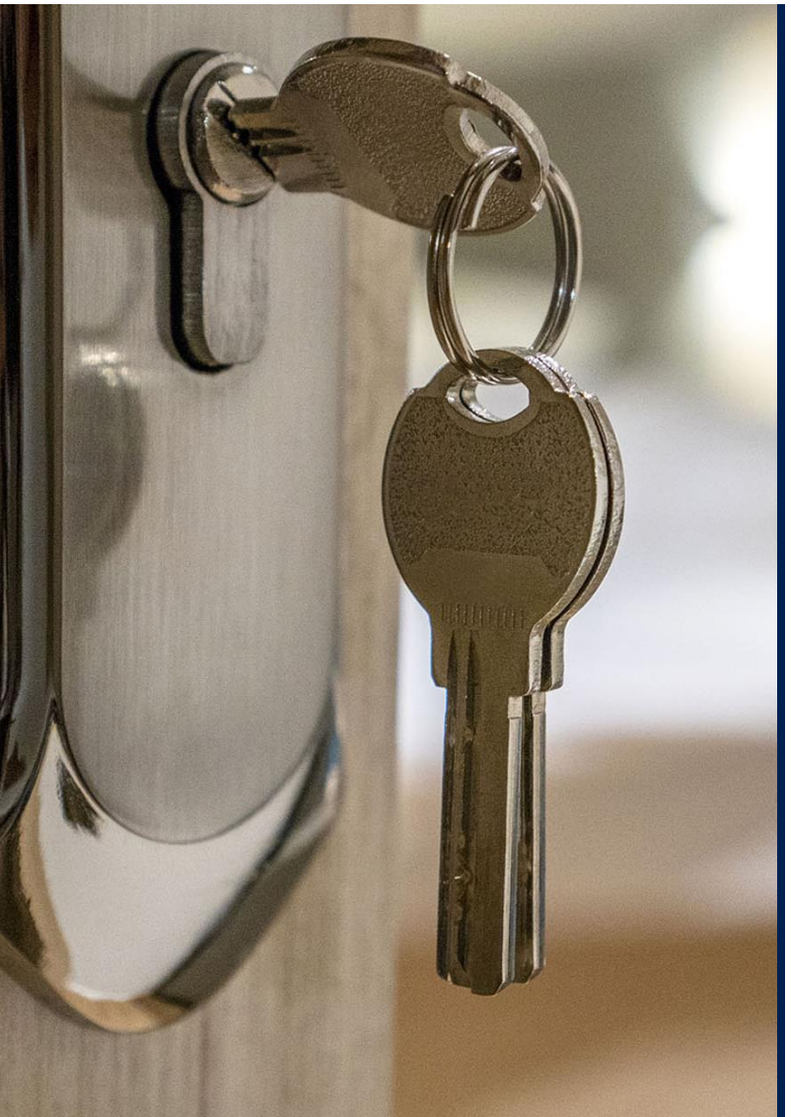


2019 Digital security strategy

	Risk Management	Assurance	Identity Management	Device Health	Data & Telemetry	Information Protection
EPICS	All internet facing interfaces are compliant Tier 1 critical services are resilient	Accelerate cloud security capabilities	Eliminate passwords Protect the administrators Simplify provisioning, entitlements, and access management	Evolve endpoint protection Only allow access from healthy devices Zero trust networks	Detect threats through user behavior anomalies	All Microsoft data is classified, labeled and protected
SERVICES	Business response and crisis management Compliance Enterprise business continuity management Enterprise security governance and risk Security education and awareness Security incident response Security standards and configuration	App & Infrastructure security Emerging security products External assessments Red team penetration testing Supply chain security	Administrator role services Authentication Certificate management Credential management Provisioning, entitlement management, and synchronization	Endpoint protection Phishing protection SAW HRE Vulnerability management Virtualization	Data intelligence Security intelligence platform Security monitoring Threat intelligence	Data loss prevention Insider threat

Security tools engineering

Security world view



Opportunities

Globalization: more markets, customers, and business potential

Always-on access provides **more productivity**

Ability to **analyze massive data** sets at scale and speed

Scalable, cloud based storage: efficient, cost effective, and secure

Modern engineering: allows for more agility in building capabilities, features, and in responding to threats

Risks

Globalization can lead to **"digital xenophobia"**

More lucrative targets give rise to more **dangerous threat actors**

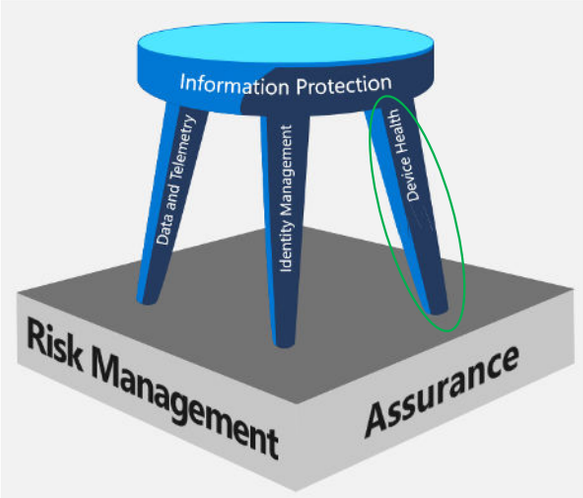
More surface area for attacks/exposure to harm, including **supply chain**

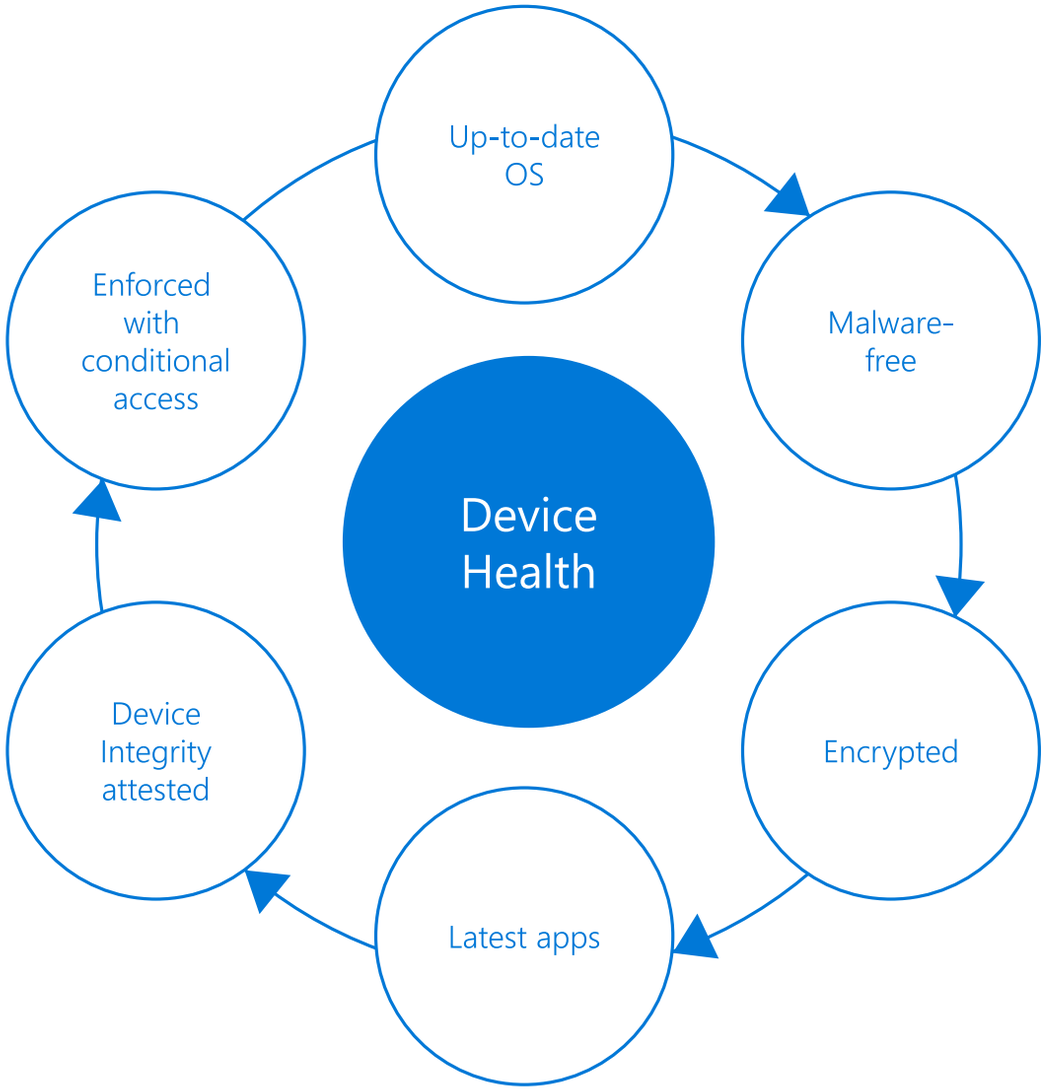
The client-to-cloud world requires a control shift
(Identity is the new perimeter)

Device health

Why device health

Unmanaged devices are a powerful entry point for attackers and present a high risk to the enterprise.





Device health

Where we're at

Edge protections of the past are no longer effective in the cloud.

Unmanaged personal devices allowed for work present unprecedented risk.

Key Investment Areas

Endpoint Protection

Conditional Access

Device health

Only allow access from healthy devices

Admins must use secure devices for all activities performed with elevated privileges

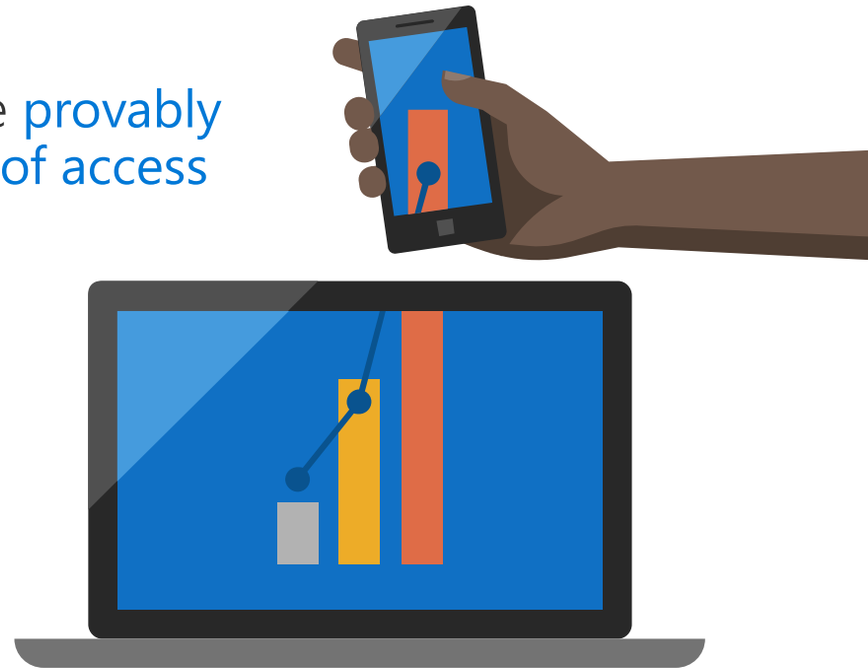
Devices must be managed for access

Additional device compliance policies required over time (encryption, anti-malware, minimum OS level, hardware config., etc.)

Protect the endpoint

Modern endpoint protection on every device (pre-and post-boot protection, cross-platform coverage)

Devices must be provably healthy at time of access



Device health

Evolving threats

As malicious actors continue evolving the threat landscape with ever more sophisticated attacks:

Prioritize fixes

Ensure most prevalent models are updated to the latest model specific BIOS fixes

Reduce footprint of legacy hardware

Eliminate vulnerabilities specific to legacy hardware

Modern threats require modern hardware and security features

Move to modern devices

Goal state

Today

Network Boundary Reliant

Reporting/Reactive

Some devices managed

Ongoing patching, updates, device hygiene

Significant effort fingerprinting

Device Health with AAD CA and Intune

No unknown devices get access

Reduced surface area for attack

Holistic Endpoint Protection

Patching, updates, device hygiene enforceable

Restored visibility to the environment

Increased resistance to malware

Conditional Access as a service

Key recommendations

Communicate, communicate, communicate!

Start small

Start with devices used by admins

Have a plan ready to leverage a crisis

Educate your senior leaders

Resources

Access all IT Showcase resources at Microsoft.com/ITShowcase

- Webinar: Speaking of security: A discussion with Bret Arsenault, CISO at Microsoft
- The importance of device health
- Device Health content suite
- Client security: shifting paradigms to prepare for a cloud-only future
- Microsoft uses Windows Defender ATP antivirus capabilities to boost malware protection
- Protecting high-risk environments with secure admin workstations
- IT expert roundtable: How Microsoft secures elevated access with tools and privileged credentials

Microsoft

Microsoft IT Showcase

How Microsoft does IT

Visit the website
http://www.microsoft.com/itshowcase

Thank you