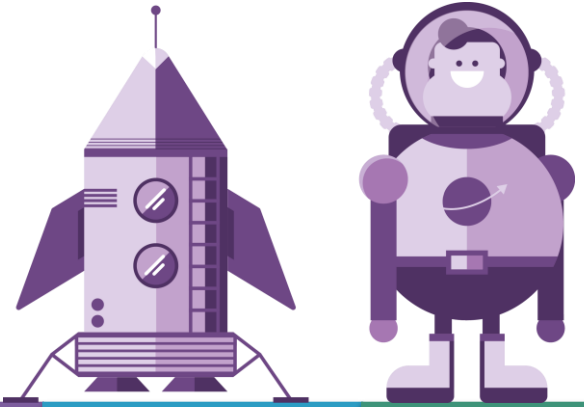
Is the Cloud Secure Enough?

Andrew Quinn

13/2/2019



How does the Cloud Affect Me?

There is no cloud

it's just someone else's computer

All clouds are not created equal

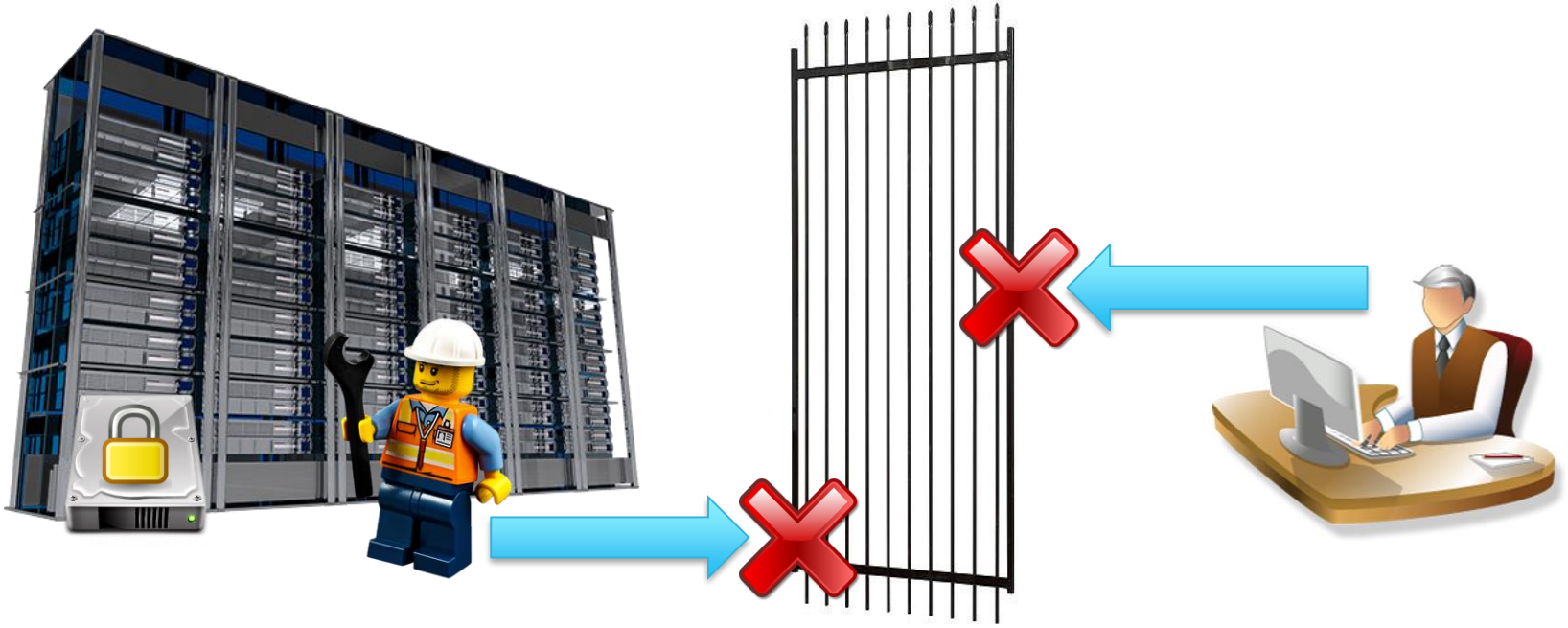
- Physical Security
- Authorisation & Authentication
- Identity and Access
- Network Security
- Intrusion Detection & Prevention
- Vulnerability Management
- Patch Management
- Software Development
- Incident Management
- Monitoring
- Data Security
- Encryption at Rest
- Secure Communications
- Logging

Ask

Doing it Right: Office 365

- Physical security:
  - Perimeter boundary
  - Video monitoring
  - Infrared
  - Motion sensors
  - Biometrics
  - Access lists
  - Manned checkpoints
  - Vehicle traps
  - Layered approach
  - Seismic rack anchors

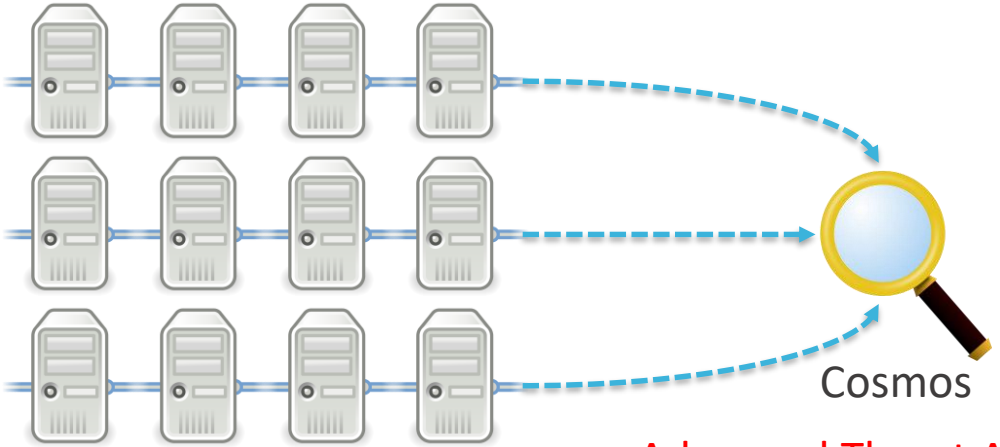
Doing it Right: Office 365



Doing it Right: Office 365

AppLocker

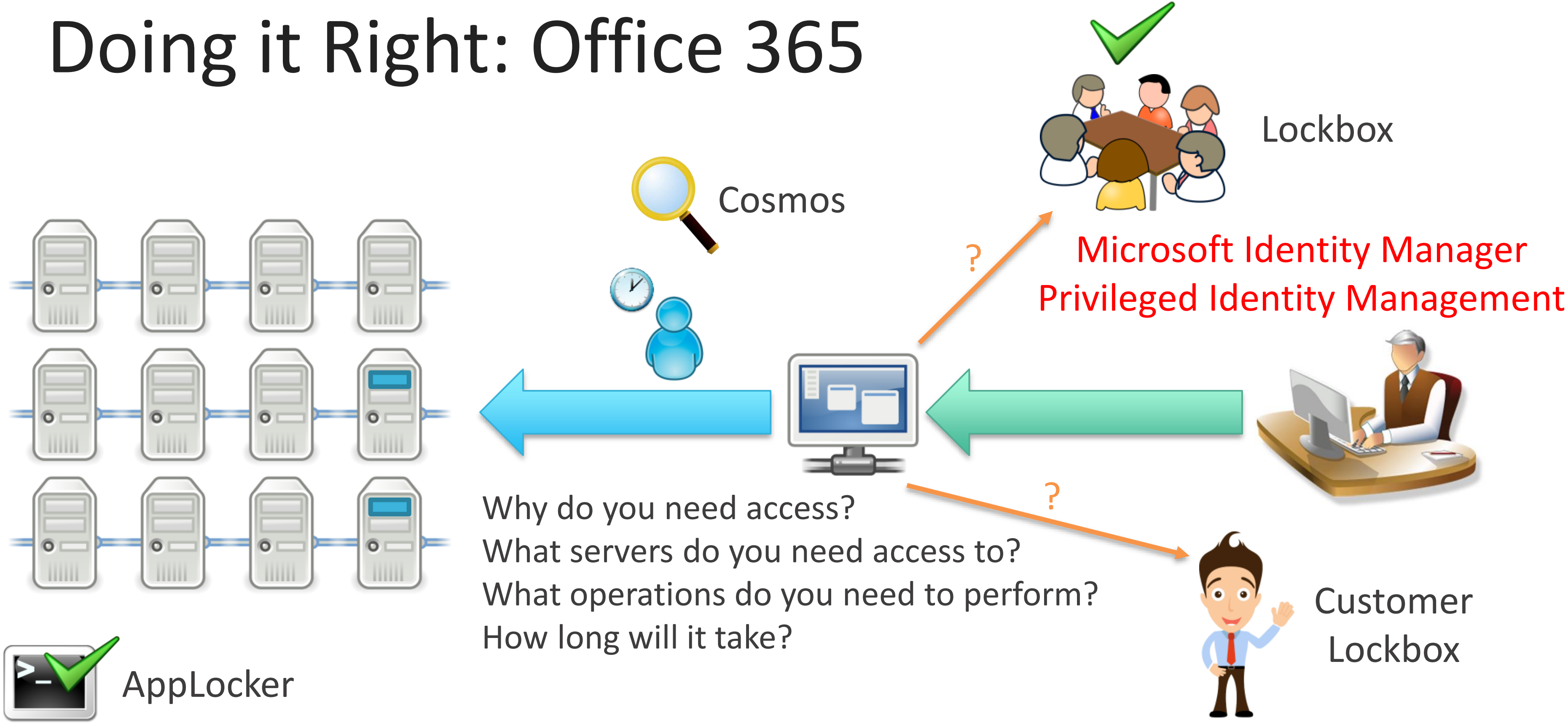
AppLocker



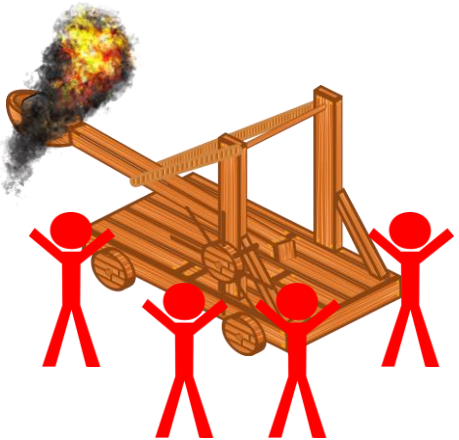
Cosmos

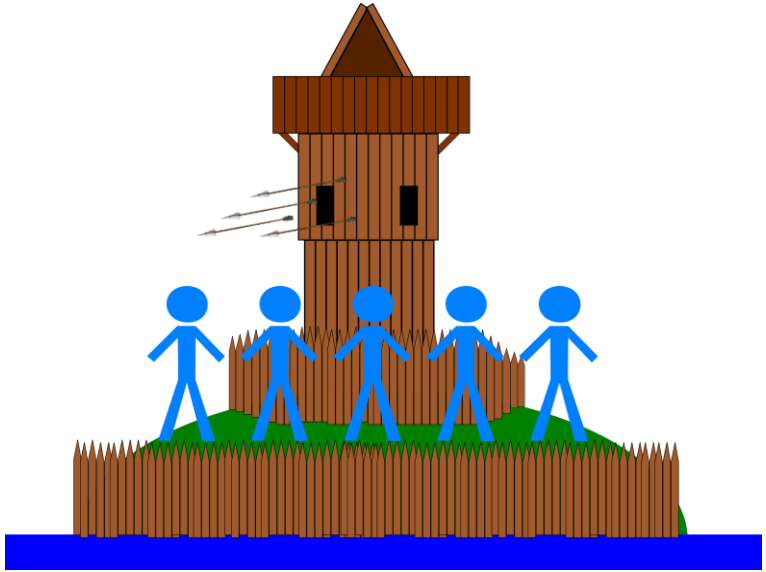
Advanced Threat Analytics

Doing it Right: Office 365



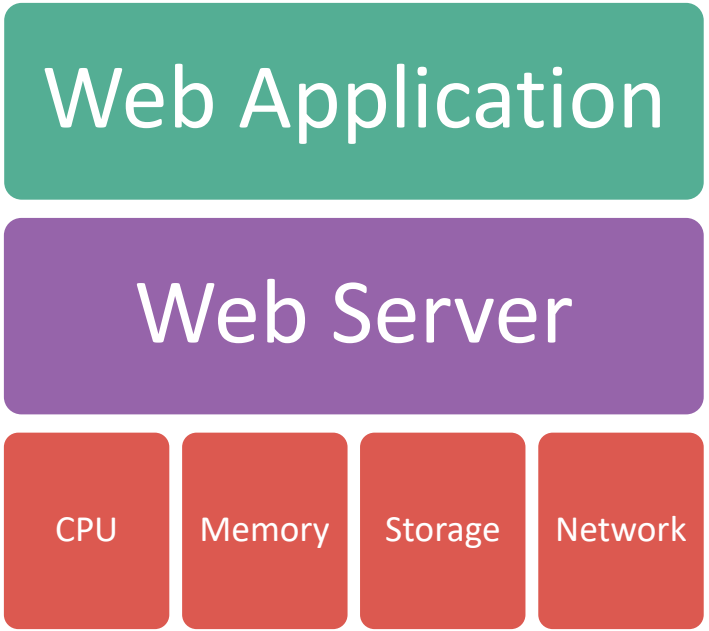
Doing it Right: Office 365





What type of Cloud?

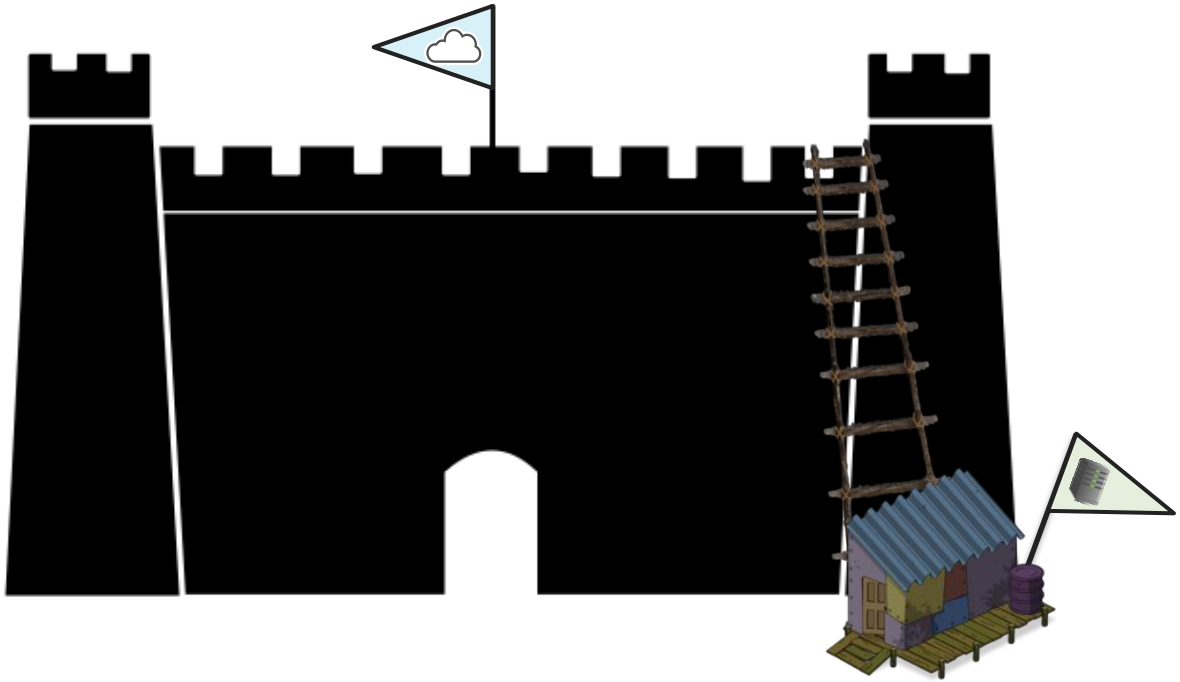
- Software as a Service (SaaS)
  - SharePoint Online
- Platform as a Service (PaaS)
  - Azure Web Apps
- Infrastructure as a Service (IaaS)
  - Azure Virtual Machines



Shared Security Model

Component	On-Premises	Infrastructure-aaS	Platform-aaS	Software-aaS
Applications	You	You	You	Vendor
Data	You	You	You	Vendor
Runtime	You	You	Vendor	Vendor
Middleware	You	You	Vendor	Vendor
Operating System	You	You	Vendor	Vendor
Virtualization	You	Vendor	Vendor	Vendor
Servers	You	Vendor	Vendor	Vendor
Storage	You	Vendor	Vendor	Vendor
Networking	You	Vendor	Vendor	Vendor
Devices	You	You	You	You
Identity & Access	You	You	You	You

Shared Security Model



It’s all Remote Access

Breach Demonstration

Securing the Cloud

NIST Cybersecurity Framework

1. Identify - Understand your environment
2. Protect - Limit and contain breaches
3. Detect - Limit the time between breach and response
4. Respond - Minimise impact, report if required
5. Recover - Restore services, data, capabilities

Cover the Basics

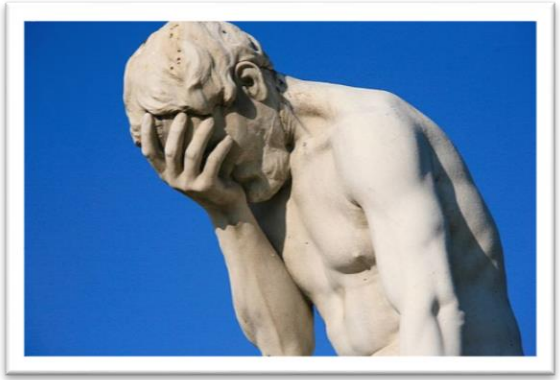
- Patching Regime
- Secure Devices
- Complex Passwords
- Lifecycle Management
- Malware Protection
- NCSC 10 Steps to Cyber Security
- Cyber Essentials

Arm your Users

- Educate
  - Password Reuse
  - Spotting Fraudulent Emails & Websites
  - Reporting Breaches & Suspicious Activity
- Customise Logon Screen
- Anti-Spoofing & Anti-Phishing
- Phishing Simulation

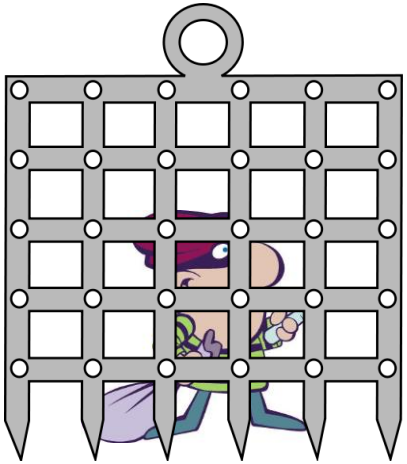
Prevent Mistakes

- Sharing Controls
  - External Sharing
  - Sensitive Data
- Data Loss Prevention
- Policy-Based Encryption
- Rights Management
- Block Insecure Passwords



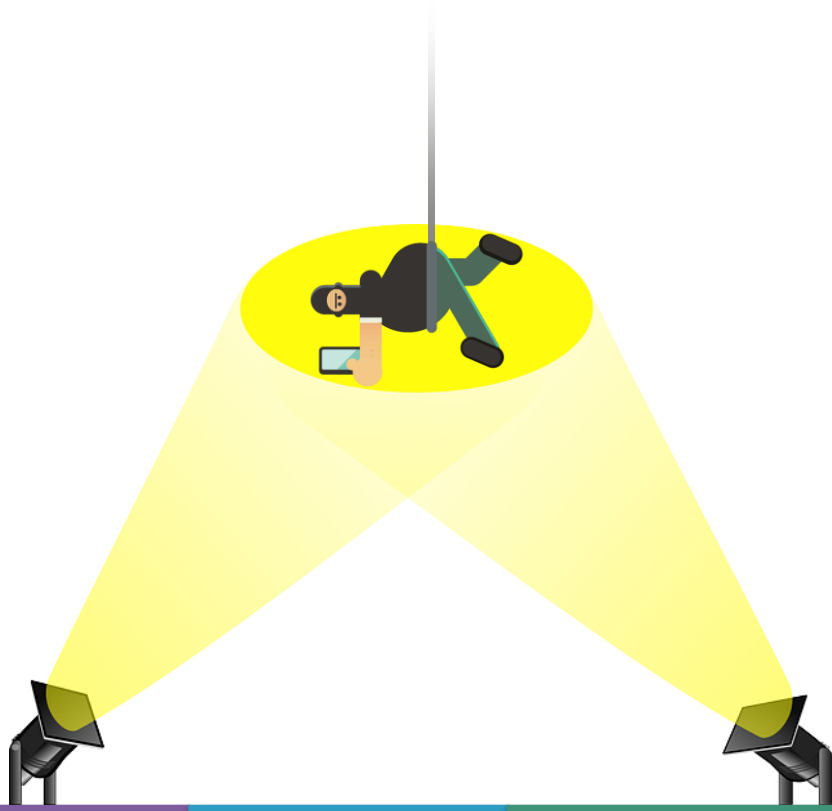
Mitigate Breaches

- Multifactor Authentication
- Conditional Access
- Risk Based Actions (AAD IP)
- Sharing Controls
- DLP & Encryption
- Credential Guard
- Privileged Identity Management



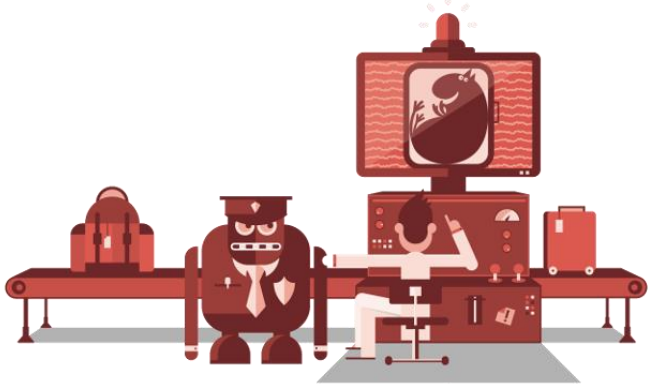
Detect Breaches

- Median Detection Time: **146 Days**
- Behavioural & Rule-Based Analysis
  - Cloud App Security
  - Advanced Threat Analytics
- Alert Policies
- Password Compromise (Darknet)
- Audit Logging & Analysis



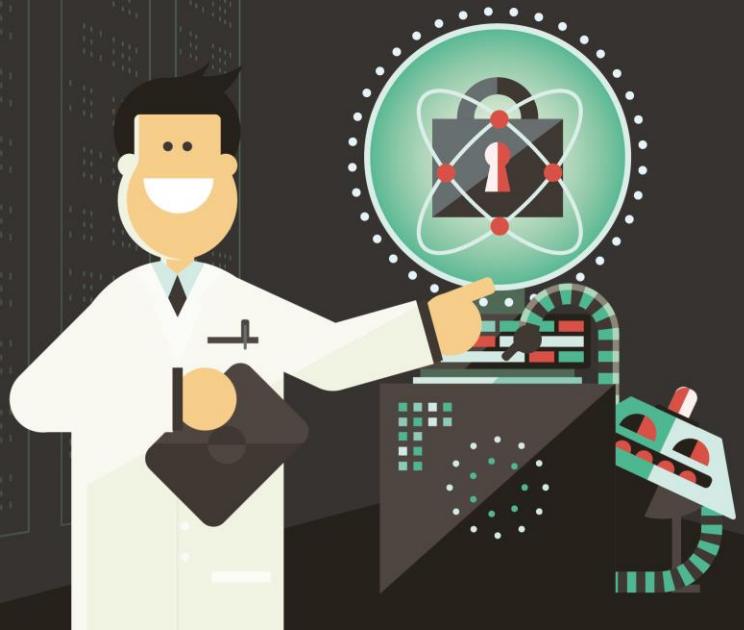
Verify Secure Configuration

- Desired State Configuration Checks
- Monitor Cloud App Usage
- Identity Protection Policies
- Review Audit Logs & Reports
- Test for Insecure Passwords



w@terstons

Cyber Security



w@terstons

- Information Security Strategies
- Managed Security Services
- Cyber Essentials
- GDPR
- ISO 27001

waterstons.com/security security@waterstons.com 0345 094 094 5

CYBER ESSENTIALS PLUS

GDPR

bsi. ISO/IEC 27001 Information Security Management

Keep in Touch


andrew.quinn@waterstons.com


www.waterstons.com/people/andrew-quinn


0345 094 094 5


@WaterstonsLtd


/in/AndrewMRQuinn

w@terstons