Microsoft

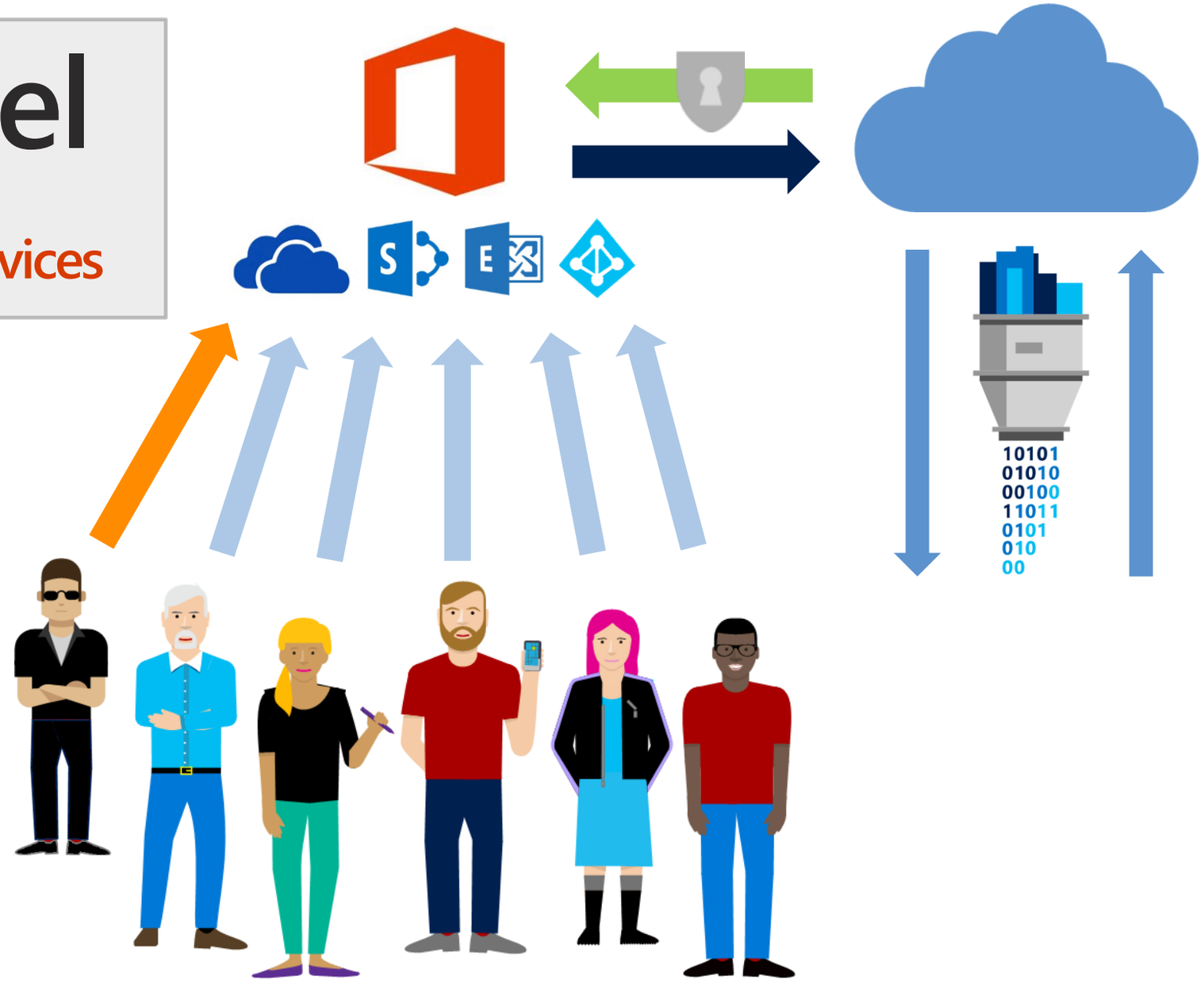
Identity is the New Security Boundary

Paul Hughs
Security Specialist
State & Local Government

New Model

What changed?

Cloud Apps + Mobile Devices



Trusted User Phishing Attack

Remediate automatically and respond quickly when a new targeted phishing strategy emerges

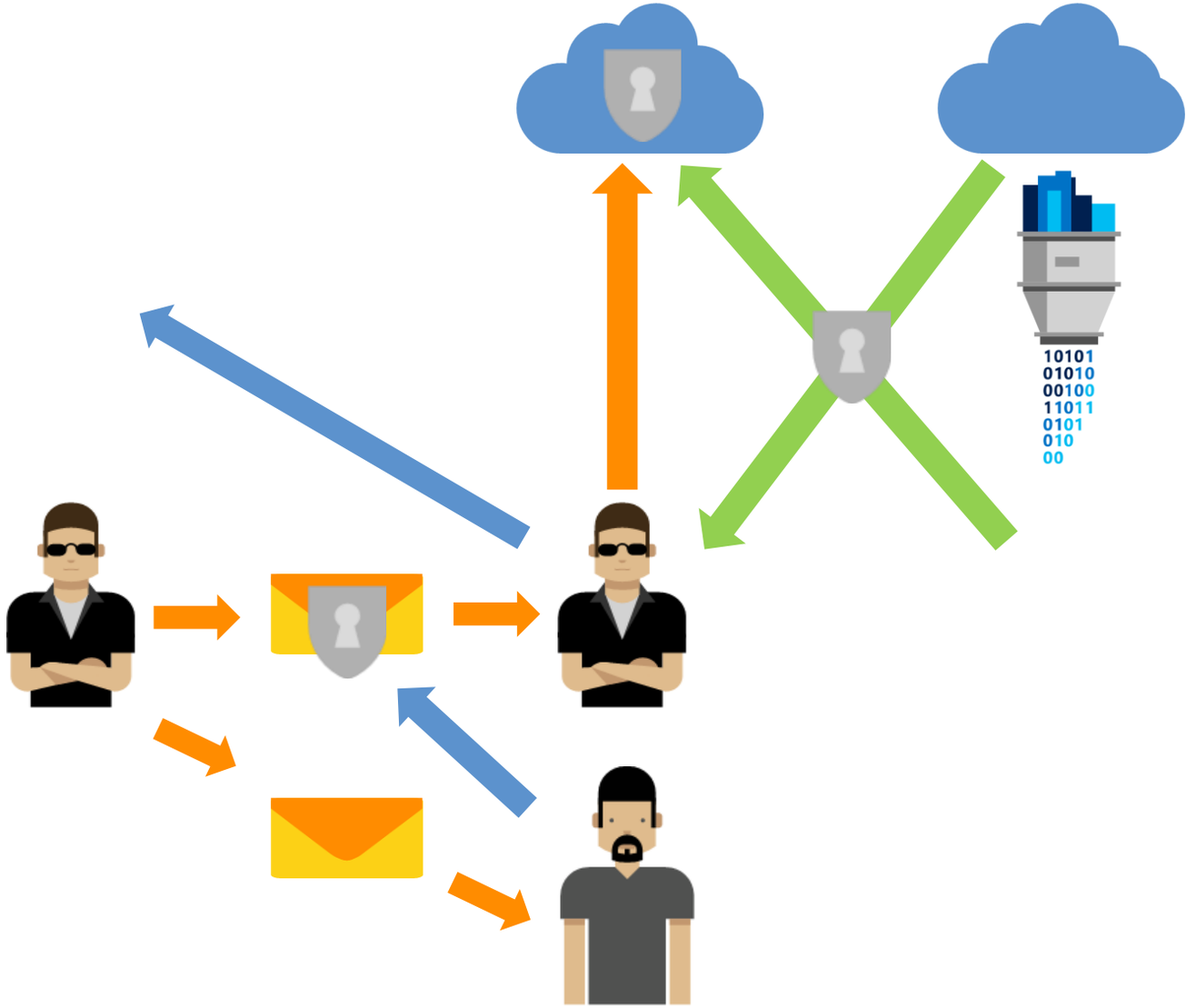
CAS

ATP

Power BI

TI

Azure



Email	Exchange Online Protection **Block Known Bad Mail**	Office 365 Advanced Threat Protection **Protect Unknown Links**	Office 365 Advanced Threat Protection **Block Unknown Malware**
Identity	Conditional Access **Block Risky Sign In**	Multi-factor Authentication **Challenge Risky Sign In**	Azure Identity Protection **Detect Risky Sign In**
Behavior	Microsoft Cloud App Security **Detect Known Attacks**	Microsoft Cloud App Security **Track Unknown Attacks**	Windows Defender **Detect Endpoint Attack**
Insights	Threat Intelligence **Investigate Attack**	Power BI **Correlate Attack Vectors**	Windows Defender ATP **Investigate Endpoint**

Phishing Defense-in-depth Capabilities

Azure Active Directory P1 conditional access policies and MFA block attackers from signing in to Office 365.
Azure Active Directory P2 baselines and monitors user logins, detect anomalies, and applies risk tags to accounts and sessions.

Office 365 Advanced Threat Protection protects users from phishing URLs at time-of-click and allows attack URL blocking.
Office 365 Threat Intelligence defeats outbound phishing obfuscation with enhanced message reporting and correlation.

Microsoft Cloud App Security provides forensic behavioral data with event enrichment and multiple pivots for attack investigation, maintains known attack signature policies, and tracks indications of compromise for discovering unknown attacks.

Power BI visually correlates data gathered from threat assessments and indications of compromise in order to determine likely sources of compromise and common attack vectors.

Azure Automation dramatically reduces response times by enforcing account protection, and remediation based on risk.
Azure Machine Learning reduces the time and complexity of attack detection and trains environment-specific models.

Microsoft

THANK YOU