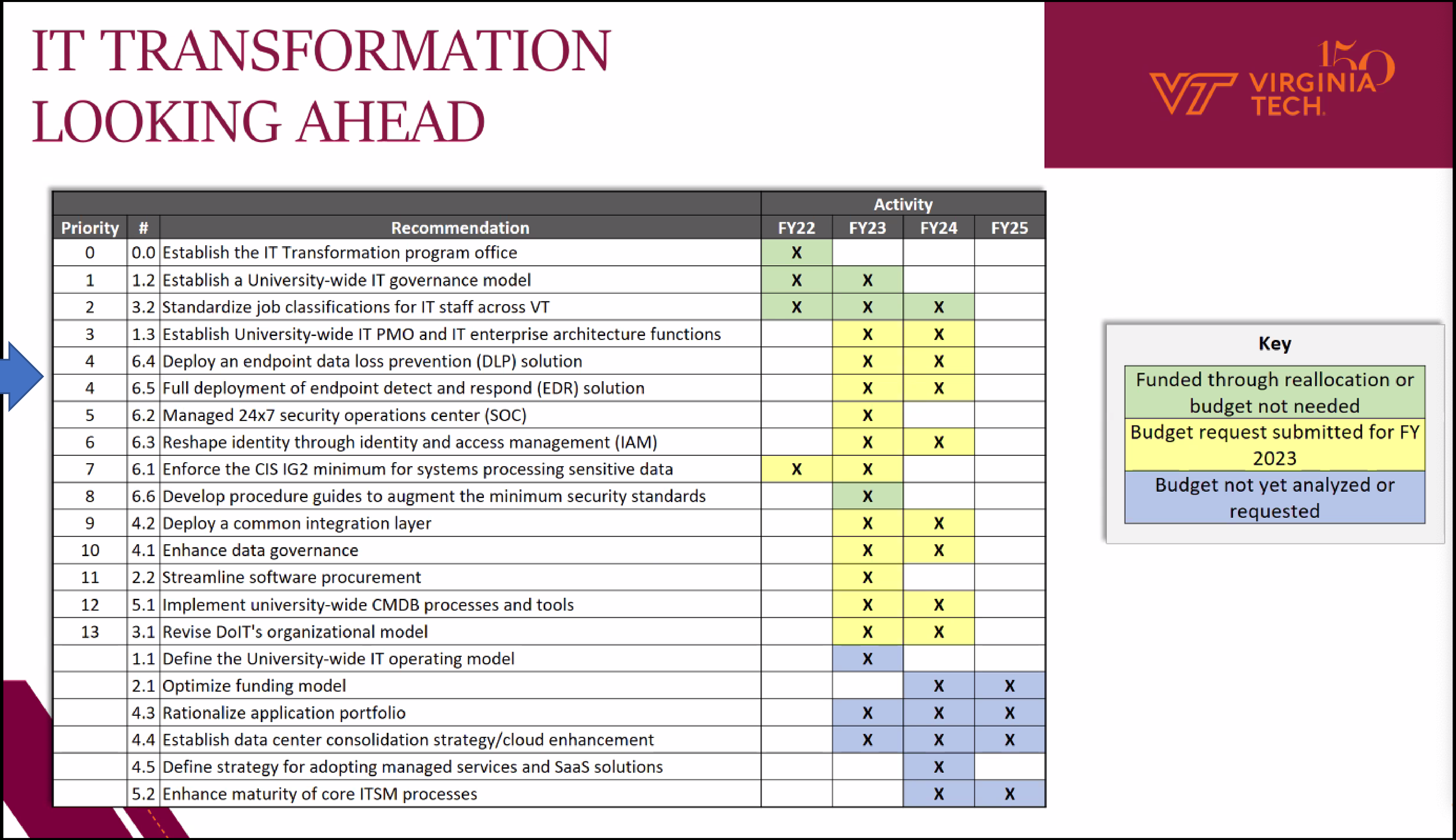
IT Transformation - Improved Endpoint Protection (IEP)

V1.1 - 20221017

M. DeBonis

Background to IEP



IT TRANSFORMATION LOOKING AHEAD

VIRGINIA TECH 150

			Activity			
Priority	#	Recommendation	FY22	FY23	FY24	FY25
0	0.0	Establish the IT Transformation program office	🟩 X			
1	1.2	Establish a University-wide IT governance model	🟩 X	🟩 X		
2	3.2	Standardize job classifications for IT staff across VT	🟩 X	🟩 X	🟩 X	
3	1.3	Establish University-wide IT PMO and IT enterprise architecture functions		🟨 X	🟨 X	
4	6.4	Deploy an endpoint data loss prevention (DLP) solution		🟨 X	🟨 X	
4	6.5	Full deployment of endpoint detect and respond (EDR) solution		🟨 X	🟨 X	
5	6.2	Managed 24x7 security operations center (SOC)		🟨 X		
6	6.3	Reshape identity through identity and access management (IAM)		🟨 X	🟨 X	
7	6.1	Enforce the CIS IG2 minimum for systems processing sensitive data	🟨 X	🟨 X		
8	6.6	Develop procedure guides to augment the minimum security standards		🟩 X		
9	4.2	Deploy a common integration layer		🟨 X	🟨 X	
10	4.1	Enhance data governance		🟨 X	🟨 X	
11	2.2	Streamline software procurement		🟨 X		
12	5.1	Implement university-wide CMDB processes and tools		🟨 X	🟨 X	
13	3.1	Revise DoIT's organizational model		🟨 X	🟨 X	
	1.1	Define the University-wide IT operating model		🟦 X		
	2.1	Optimize funding model			🟦 X	🟦 X
	4.3	Rationalize application portfolio		🟦 X	🟦 X	🟦 X
	4.4	Establish data center consolidation strategy/cloud enhancement		🟦 X	🟦 X	🟦 X
	4.5	Define strategy for adopting managed services and SaaS solutions			🟦 X	
	5.2	Enhance maturity of core ITSM processes			🟦 X	🟦 X

Key

- 🟩 Funded through reallocation or budget not needed
- 🟨 Budget request submitted for FY 2023
- 🟦 Budget not yet analyzed or requested

What is EDR and DLP

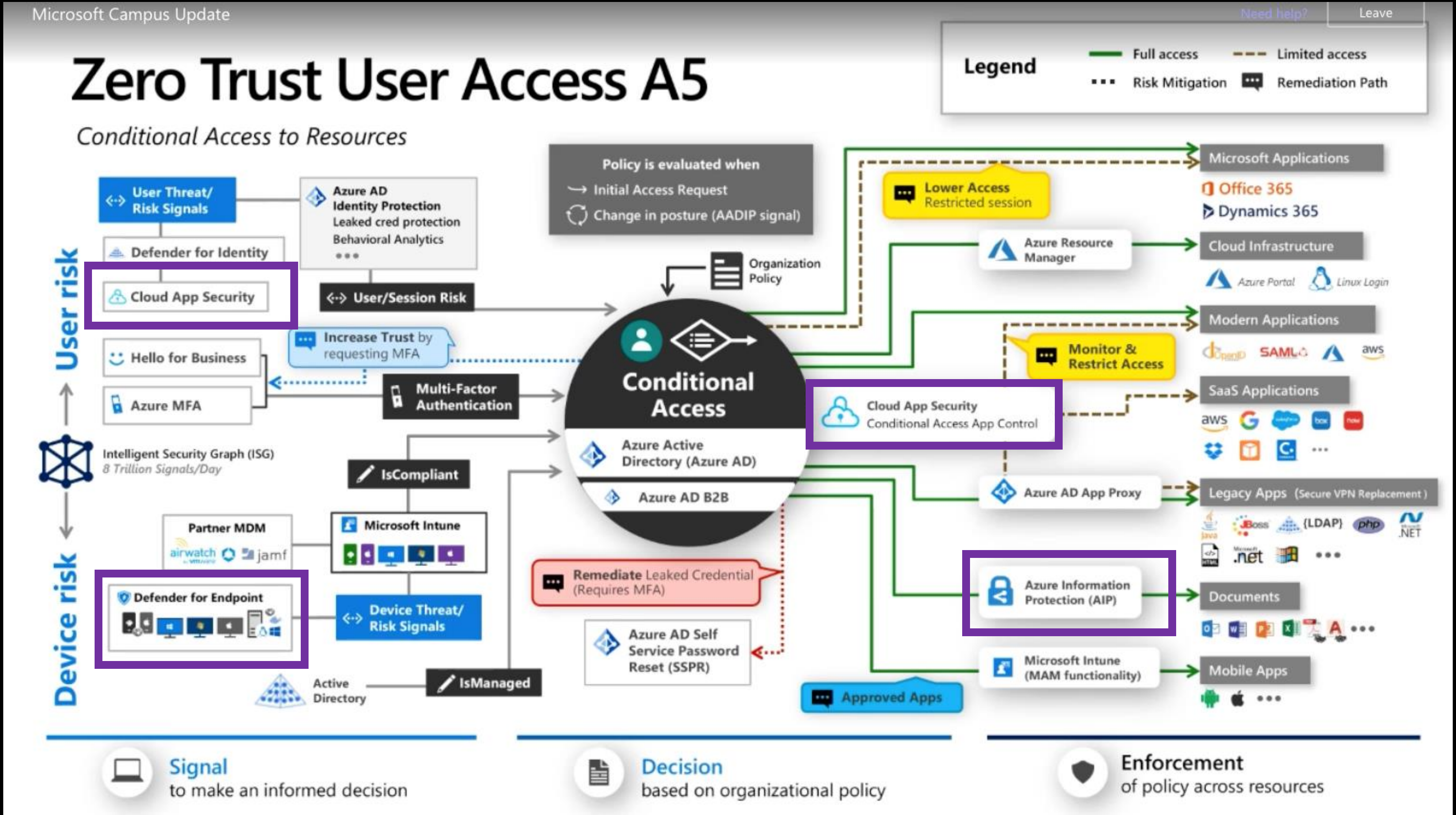
EDR

- Endpoint Detection & Response
- "What happened and what is currently happening on an endpoint?"
- e.x. - A ransomware dropper installed via a web drive-by

DLP

- Data Loss Prevention
- "What types of data do you have and what are you allowed to do with it?"
- e.x. - Trying to upload a file marked PII to a 3rd party file storage service like Dropbox

Supporting technology



Microsoft Campus Update

Need help? Leave

Zero Trust User Access A5

Conditional Access to Resources

Legend: Full access; Limited access; Risk Mitigation; Remediation Path

Policy is evaluated when
- Initial Access Request
- Change in posture (AADIP signal)

User risk

User Threat/ Risk Signals

Azure AD Identity Protection
Leaked cred protection
Behavioral Analytics
•••

Defender for Identity

Cloud App Security

User/Session Risk

Increase Trust by requesting MFA

Hello for Business

Azure MFA

Multi-Factor Authentication

Intelligent Security Graph (ISG)
8 Trillion Signals/Day

Device risk

IsCompliant

Partner MDM
airwatch jamf

Microsoft Intune

Defender for Endpoint

Device Threat/ Risk Signals

Active Directory

IsManaged

Organization Policy

Conditional Access

Azure Active Directory (Azure AD)

Azure AD B2B

Remediate Leaked Credential (Requires MFA)

Azure AD Self Service Password Reset (SSPR)

Approved Apps

Lower Access
Restricted session

Azure Resource Manager

Monitor & Restrict Access

Cloud App Security
Conditional Access App Control

Azure AD App Proxy

Azure Information Protection (AIP)

Microsoft Intune (MAM functionality)

Microsoft Applications
Office 365
Dynamics 365

Cloud Infrastructure
Azure Portal
Linux Login

Modern Applications
OpenID SAML aws

SaaS Applications
aws •••

Legacy Apps (Secure VPN Replacement)
Java JBoss (LDAP) php .NET .net •••

Documents
•••

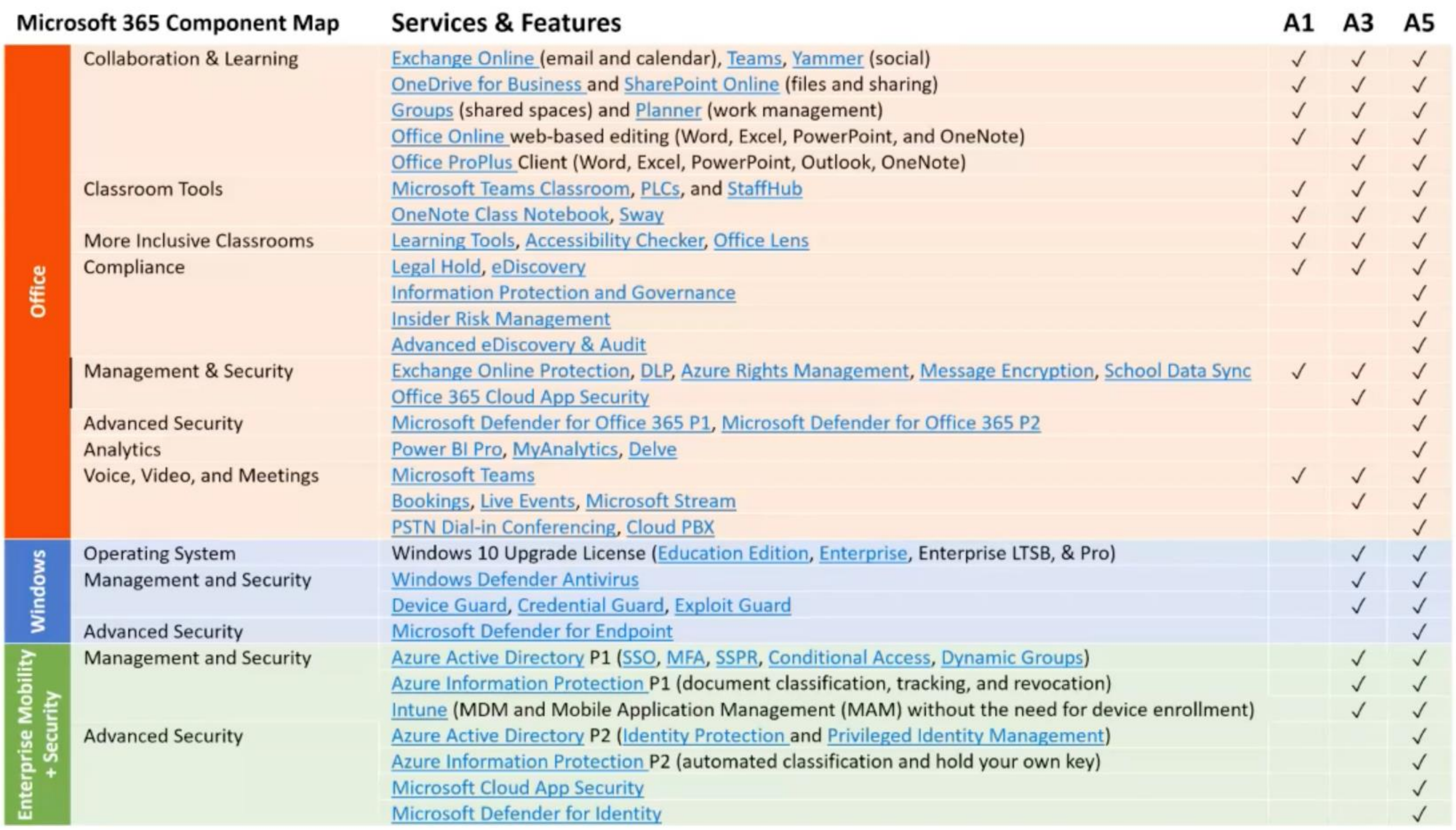
Mobile Apps
•••

Signal
to make an informed decision

Decision
based on organizational policy

Enforcement
of policy across resources

Licensing



Microsoft 365 Component Map		Services & Features	A1	A3	A5
Office	Collaboration & Learning	Exchange Online (email and calendar), Teams, Yammer (social)	✓	✓	✓
		OneDrive for Business and SharePoint Online (files and sharing)	✓	✓	✓
		Groups (shared spaces) and Planner (work management)	✓	✓	✓
		Office Online web-based editing (Word, Excel, PowerPoint, and OneNote)	✓	✓	✓
		Office ProPlus Client (Word, Excel, PowerPoint, Outlook, OneNote)		✓	✓
	Classroom Tools	Microsoft Teams Classroom, PLCs, and StaffHub	✓	✓	✓
		OneNote Class Notebook, Sway	✓	✓	✓
	More Inclusive Classrooms	Learning Tools, Accessibility Checker, Office Lens	✓	✓	✓
	Compliance	Legal Hold, eDiscovery	✓	✓	✓
		Information Protection and Governance			✓
		Insider Risk Management			✓
		Advanced eDiscovery & Audit			✓
	Management & Security	Exchange Online Protection, DLP, Azure Rights Management, Message Encryption, School Data Sync	✓	✓	✓
		Office 365 Cloud App Security		✓	✓
	Advanced Security	Microsoft Defender for Office 365 P1, Microsoft Defender for Office 365 P2			✓
	Analytics	Power BI Pro, MyAnalytics, Delve			✓
	Voice, Video, and Meetings	Microsoft Teams	✓	✓	✓
		Bookings, Live Events, Microsoft Stream		✓	✓
		PSTN Dial-in Conferencing, Cloud PBX			✓
Windows	Operating System	Windows 10 Upgrade License (Education Edition, Enterprise, Enterprise LTSB, & Pro)		✓	✓
	Management and Security	Windows Defender Antivirus		✓	✓
		Device Guard, Credential Guard, Exploit Guard		✓	✓
	Advanced Security	Microsoft Defender for Endpoint			✓
Enterprise Mobility + Security	Management and Security	Azure Active Directory P1 (SSO, MFA, SSPR, Conditional Access, Dynamic Groups)		✓	✓
		Azure Information Protection P1 (document classification, tracking, and revocation)		✓	✓
		Intune (MDM and Mobile Application Management (MAM) without the need for device enrollment)		✓	✓
	Advanced Security	Azure Active Directory P2 (Identity Protection and Privileged Identity Management)			✓
		Azure Information Protection P2 (automated classification and hold your own key)			✓
		Microsoft Cloud App Security			✓
		Microsoft Defender for Identity			✓

Scope

All University owned endpoints (laptops, desktops)

- Includes Windows, MacOS, Linux OSes
- Does not include server OSes (that's another thing...)
- Does not include mobile devices

Includes SaaS solutions for end-to-end DLP protection

- M365
- Google Workspace

Project status

- Charter signed
- Steering Committee formed
- CCS position posted (review starts 10/14)
- Microsoft Defender for Endpoint (MDE) pilot mode complete
- MDE service in production
  - https://4help.vt.edu/sp?id=sc_cat_item&sys_id=3776f9e01b8b01107dcddb1fdc4bcb07
- Exchange Online DLP for social security numbers and credit card warnings has been running in the environment since March 2021

IT Transformation dashboard

- https://svpcbo.vt.edu/Initiatives/ittransformation/dashboard.html

Q&A

IT Transformation - Improved Endpoint Protection (IEP)

V1.1 - 20221017

M. DeBonis