Improved Endpoint Protection (IEP) initiative

DCSS Spring 2023 presentation

V1.0 - 20230327

Marc DeBonis

Director – Collaborative Computing Solutions

http://ccs.vt.edu

Background

IT TRANSFORMATION LOOKING AHEAD

			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

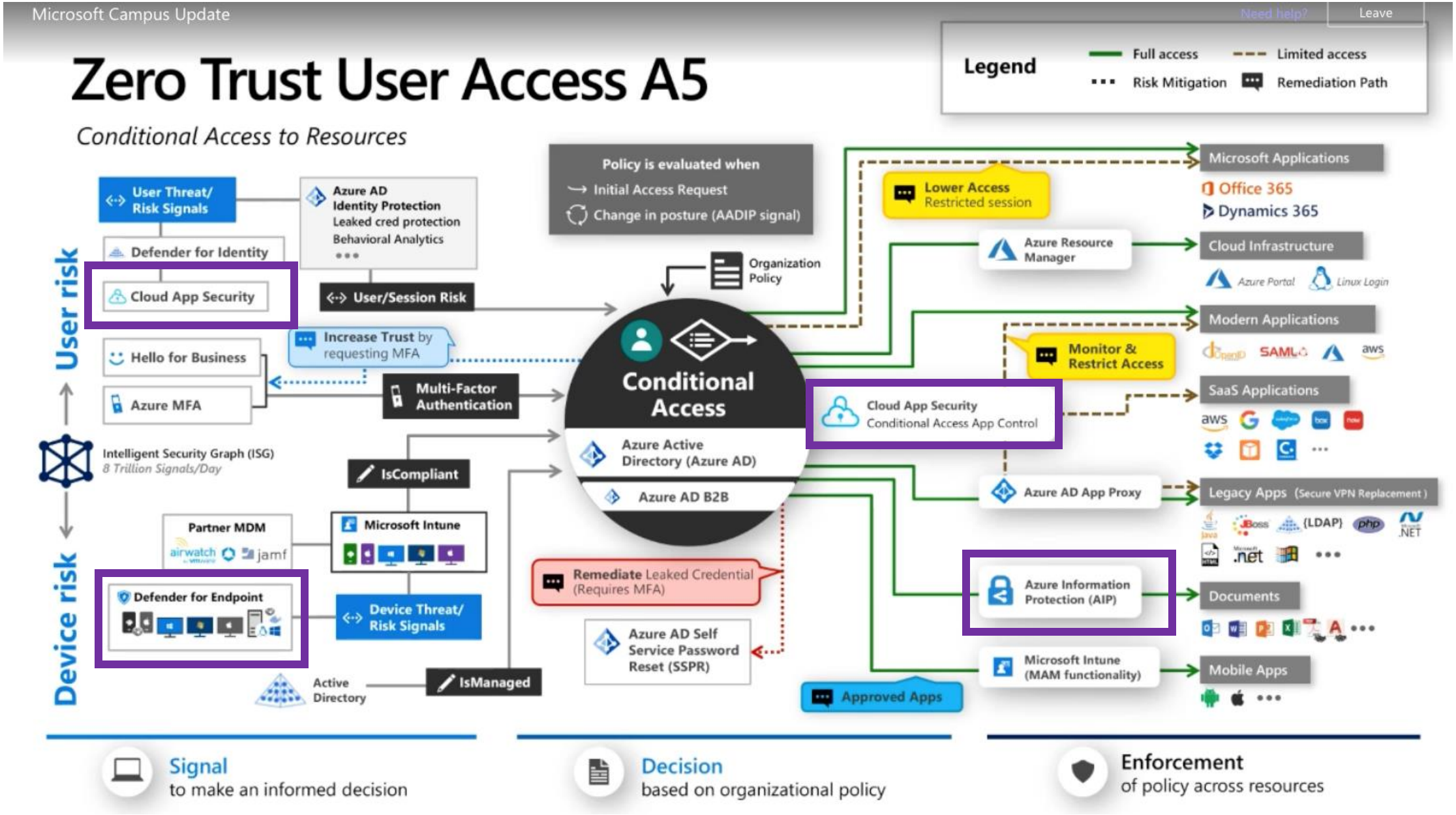
- Funded through reallocation or budget not needed
- Budget request submitted for FY 2023
- Budget not yet analyzed or requested

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 Mega

Supporting technology



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
  - Does not include mobile devices
- Includes SaaS solutions for end-to-end DLP protection
  - M365
  - Google Workspace

Status

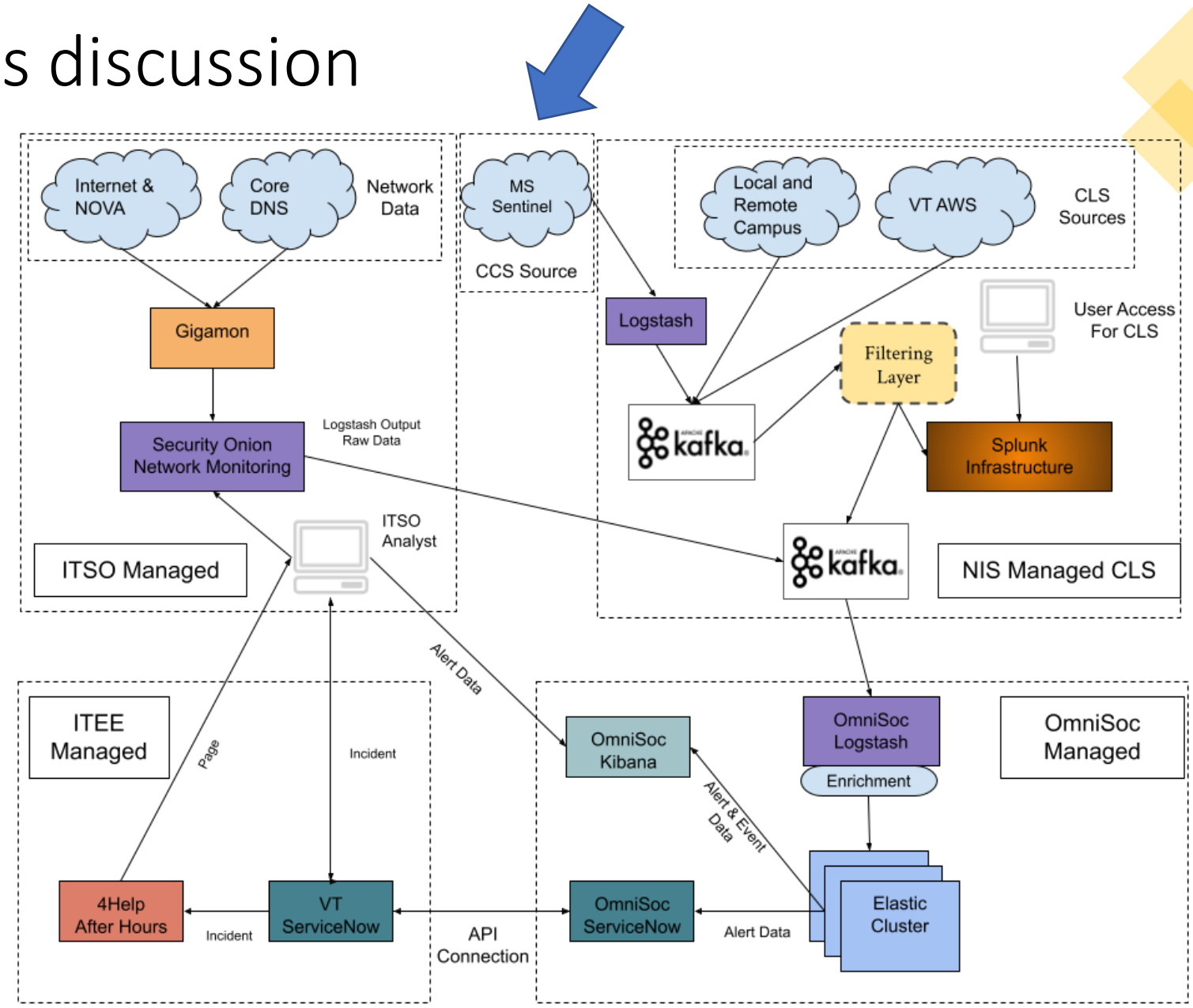
- Charter signed (September 2022)
- Steering Committee formed (October 2022)
- CCS position hired (February 2023)
- Microsoft Defender for Endpoint (MDE) in operational mode
  - 7500+ endpoints, 29+ different departments and growing!
- Exchange Online DLP for social security numbers and credit card warnings has been running in the environment since March 2021

Security Operations Center integration plan status

- Meetings with Microsoft, VT, and the OmniSOC (partner)
- MS is testing a solution to push events from Sentinel Security Information and Event Manager (SIEM)
- VT will ingest the alerts using an on-campus Logstash data pipeline
- Logstash will filter and forward events to the existing Kafka instance to stream events to OmniSOC.
- OmniSOC will parse these events and include in 24x7 notification

MDE and ITSO access discussion

- ITSO graphic regarding event ingestion
- Discussion of MS Sentinel data sending to SOC
- Status of providing ITSO access to M365\MDE security roles



Showing ROI (Return on Investment)

- 7,604 endpoints running MDE, 29 departments enrolled in service
- From 12/14/2022 to 3/28/2023, the service detected and mitigated

- High Alerts
  - 3 high-severity malware attacks prevented
  - 4 ransomware-linked emerging threats

- Medium Alerts
  - 4 attempts to exploit a remote code execution vulnerability
  - 3 active ‘Patcher’ hack tool process
  - 1 COM hijacking
  - 1 active exploit of unsecure code

- Low Alerts
  - 61 active unwanted software apps were blocked
  - 7 malwares prevented from executing/blocked
  - 23 exploit malwares prevented
  - 28 hack-tools prevented
  - 4 phish credential theft detected/prevented
  - 9 remote-shell backdoor exploits prevented
  - 2 suspicious behavior events from software blocked

- Informative
  - 559 unwanted software apps were prevented
  - 531 malwares were prevented
  - 22 malwares detected in Outlook pst or zip archive files
  - 1 suspicious connection blocked by network protection

Alert definitions

Severity	Recommended response
High	There is a high probability that your resource is compromised. You should look into it right away. Defender for Cloud has high confidence in both the malicious intent and in the findings used to issue the alert. For example, an alert that detects the execution of a known malicious tool such as Mimikatz, a common tool used for credential theft.
Medium	This is probably a suspicious activity might indicate that a resource is compromised. Defender for Cloud's confidence in the analytic or finding is medium and the confidence of the malicious intent is medium to high. These would usually be machine learning or anomaly-based detections, for example a sign-in attempt from an unusual location.
Low	This might be a benign positive or a blocked attack. Defender for Cloud isn't confident enough that the intent is malicious and the activity might be innocent. For example, log clear is an action that might happen when an attacker tries to hide their tracks, but in many cases is a routine operation performed by admins. Defender for Cloud doesn't usually tell you when attacks were blocked, unless it's an interesting case that we suggest you look into.
Informational	An incident is typically made up of a number of alerts, some of which might appear on their own to be only informational, but in the context of the other alerts might be worthy of a closer look.

DLP – Sensitivity labels

- Understanding Microsoft 365 Sensitivity Labels
  - https://4help.vt.edu/spid=kb_article&sys_id=6d001b391b351154a6396571604bcb47
  - https://it.vt.edu/content/dam/it_vt_edu/policies/Standard-for-High-Risk-Digital-Data-Protection.pdf
  - This methodology is based on data type
- Should it be changed to support labels based on risk classification?
  - https://security.vt.edu/resources/sensitiveinfo.html
  - https://it.vt.edu/content/dam/it_vt_edu/policies/Virginia-Tech-Risk-Classifications.pdf
- Which mode is easier for automated classification?

DLP – Retention labels

- We worked with the Ryan Speer, Director of Records Management, Library
- Next Steps
  - Collect feedback and revise plan as needed
  - Launch a pilot in Production with a limited number of departments
  - Note: The Retention Labels plan focuses on retention only. We are NOT enforcing the deletion of content using the labels.

IEP University-level communication

- Initiative dashboard
  - https://evpcoo.vt.edu/Initiatives/ittransformation/dashboard.html
- IT Transformation IEP project
  - https://evpcoo.vt.edu/Initiatives/ittransformation/projects/cybersecurity/improved-endpoint-protection.html
  - This includes the new FAQ
- VT News article (VTX)
  - https://vtx.vt.edu/notices/2023/02/it-security-endpoint-protection.html
- BOV resolution
  - "RESOLUTION ON INFORMATION TECHNOLOGY MONITORING"
  - https://vtx.vt.edu/articles/2023/03/bov-march-2023-overview.html

How to get involved

- Contact your Organizational Unit (OU) admin to discuss endpoint management next steps
  - To determine your OU admin
    - Go to http://mycat.ccs.vt.edu and log in with your Hokies account
    - Note your OU Admin(s)
  - Contact them for endpoint UEM setup and EDR sign-up
    - Available UEM solutions include JAMF, Intune, BigFix, GPO, Ansible, etc.
    - They should submit a SN ticket to request signing up for UEM (if not already) and MDE
- Log into Service Now, search for term "MDE"
  - RITM: "Microsoft Defender for Endpoint Service"
  - KB: "Understanding Microsoft's Defender for Endpoint"

Questions?