Microsoft

Rise of Human Operated Ransomware across Asia

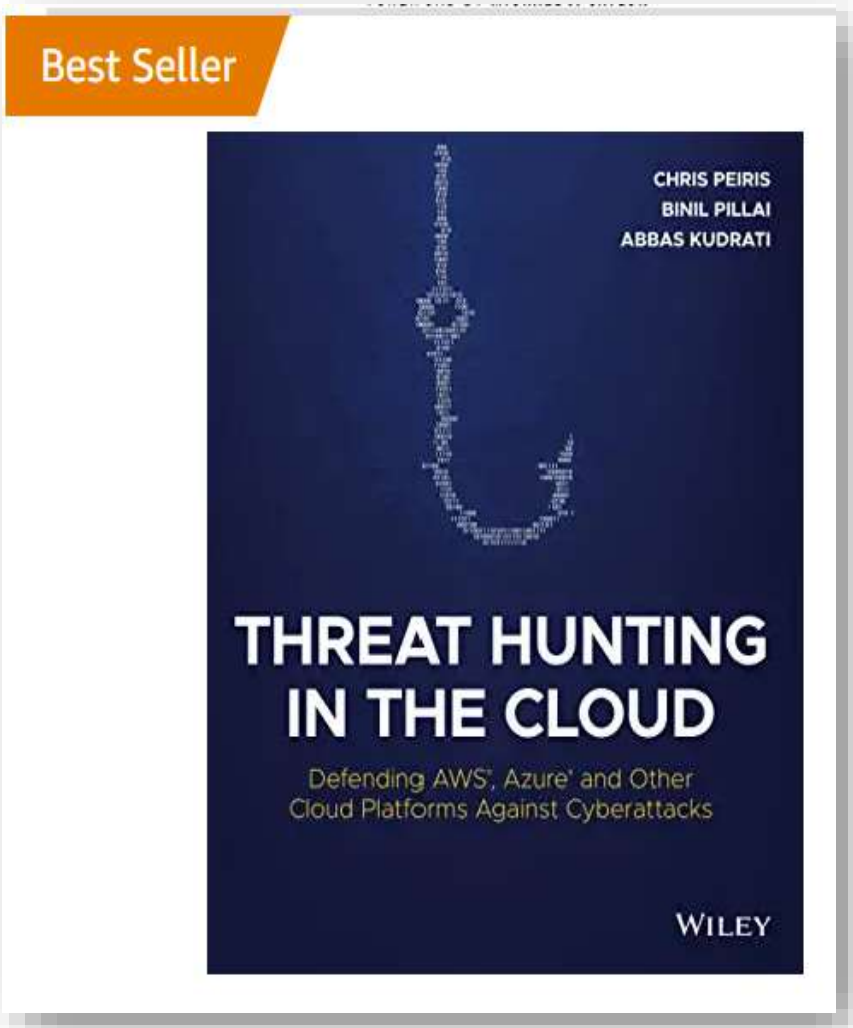
Abbas Kudrati
APAC Lead Chief Cybersecurity Advisor
Abbas.Kudrati@Microsoft.Com
@askudrati
https://aka.ms/abbas

About me

"You join Microsoft, not to be cool
but to make others cool"
Satya Nadella

- **Cybersecurity practitioner and CISO with 25 years of experience in Information / Cybersecurity.**
- **Part time Cybersecurity Professor with Deakin and LaTrobe University in Melbourne, Australia.**
- **Expertise in Zero Trust, Cybersecurity Strategy, Security Operations, Risk, Compliance, Cloud Security and Architecture.**

Upcoming books



Available now on Amazon.

Work in progress

Zero Trust Journey across the Digital Estate

By

Abbas Kudrati & Binil Pillai

Target release by Feb 2022.

Work in progress

Digitization Risks in Post Pandemic World

By

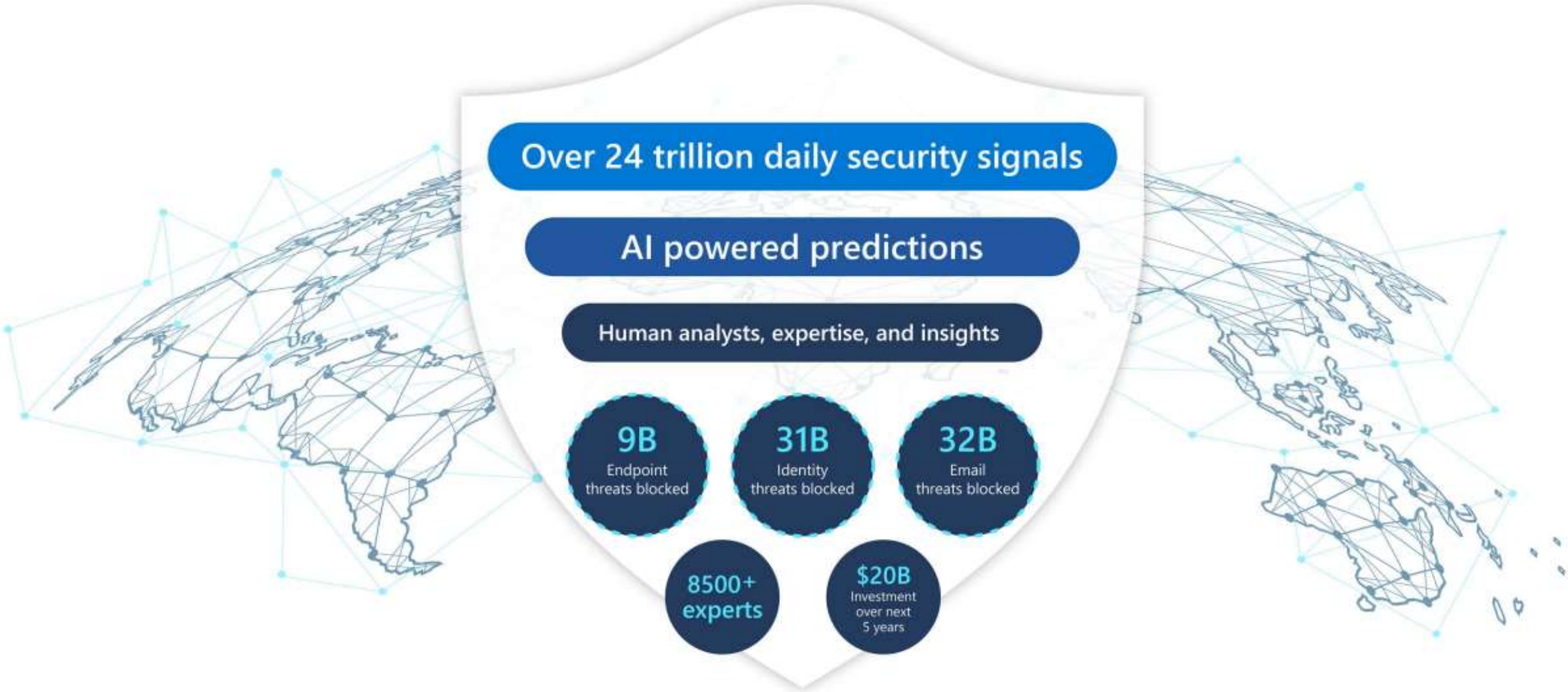
Ashish Kumar, Abbas Kudrati & Shashank Kumar

Packt›

Target release by March 2022.

Microsoft security signals

Volume and diversity of signals processed by Microsoft



July 1, 2020 through June 30, 2021

The growing threat of cybercrime

- A threat to national security
- Cybercriminals attacking all sectors
- Ransomware attacks increasingly successful
- Cybercrime supply chain continues to mature

POSITIVE TRENDS

- Transparency: governments and companies coming forward
- Priority: new laws, task forces, resources, partnerships

The cybercrime economy and services

WITH NO TECHNICAL KNOWLEDGE OF HOW TO CONDUCT A CYBERCRIME ATTACK, AN AMATEUR THREAT ACTOR CAN PURCHASE A RANGE OF SERVICES TO CONDUCT THEIR ATTACKS WITH ONE CLICK.

Ransomware and extortion

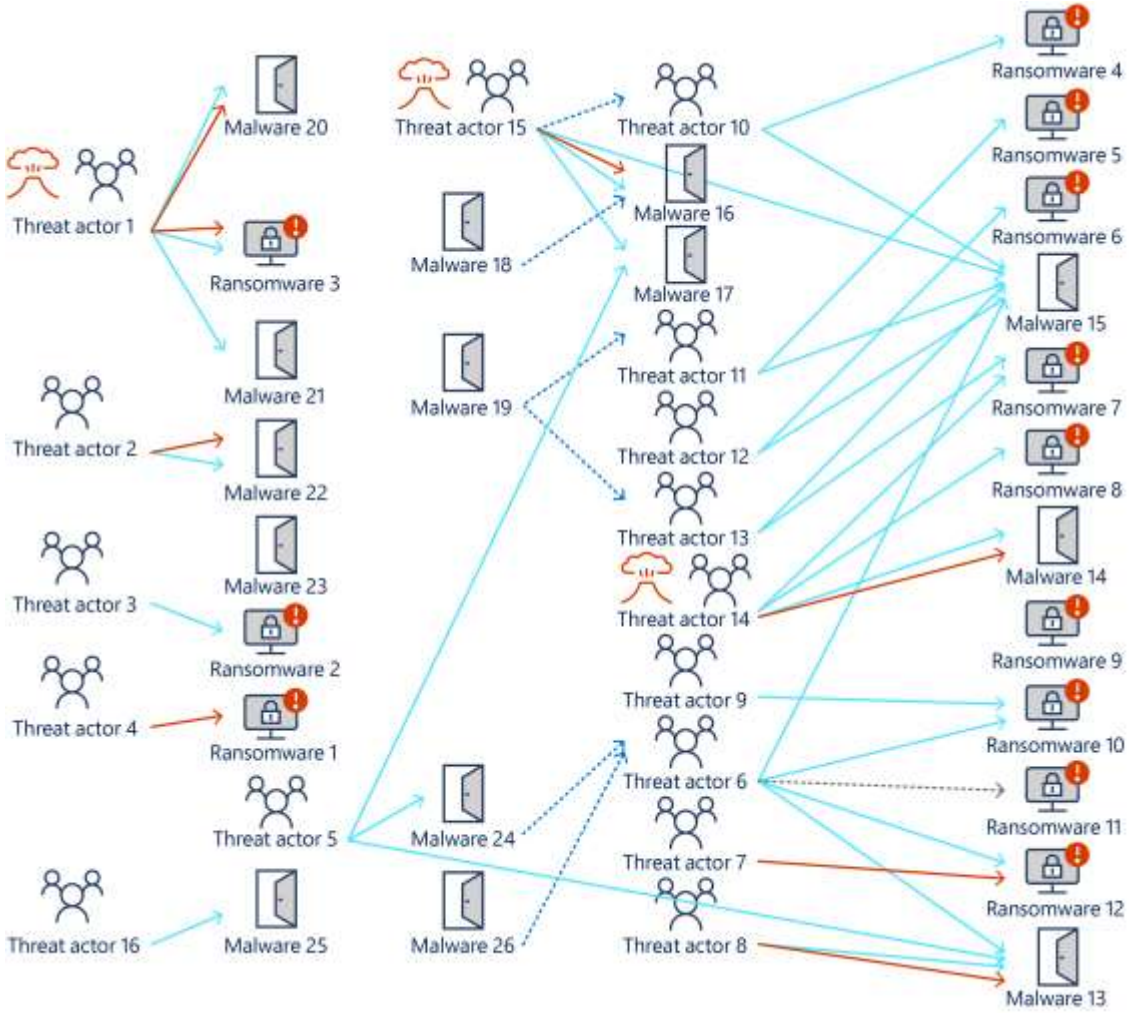
Criminal economics: A changing business model

Ransomware taxonomy

Primary role	Description
Develops	Writes the malware
Deploys	Sends phishing emails, deploys ransomware
Provides access	Malware that loads other malware, or a group that sells access as a service
Manages/operates	Leadership of a group (such as MAZE cartel membership) and/or function that provides coordination (such as managing or operating a central extortion leak site)
Publicly reported connection	A publicly reported connection exists

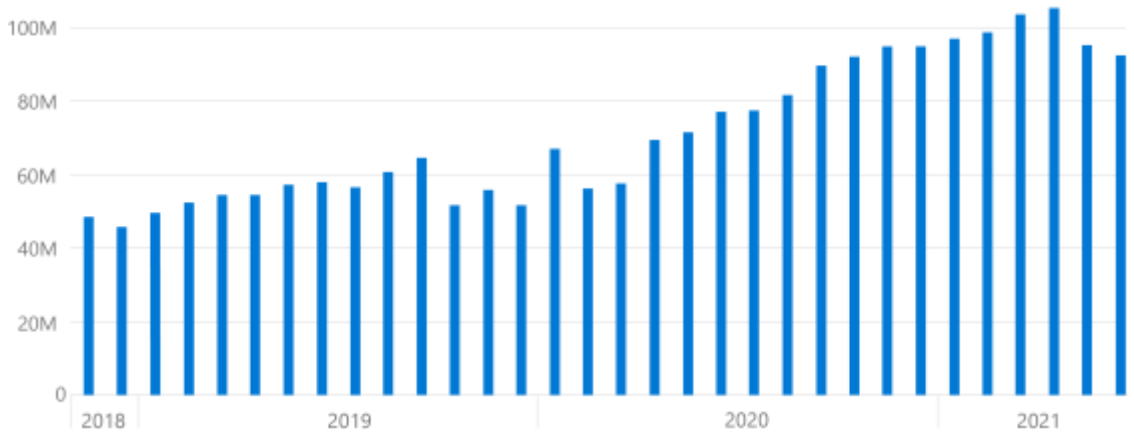
Ransomware syndicates and affiliates work together toward interconnected threats. Rather than one individual behind a ransomware attack, there are multiple groups of individuals, similar to a shared business model.

Sample analysis of roles and relationships between entities within the



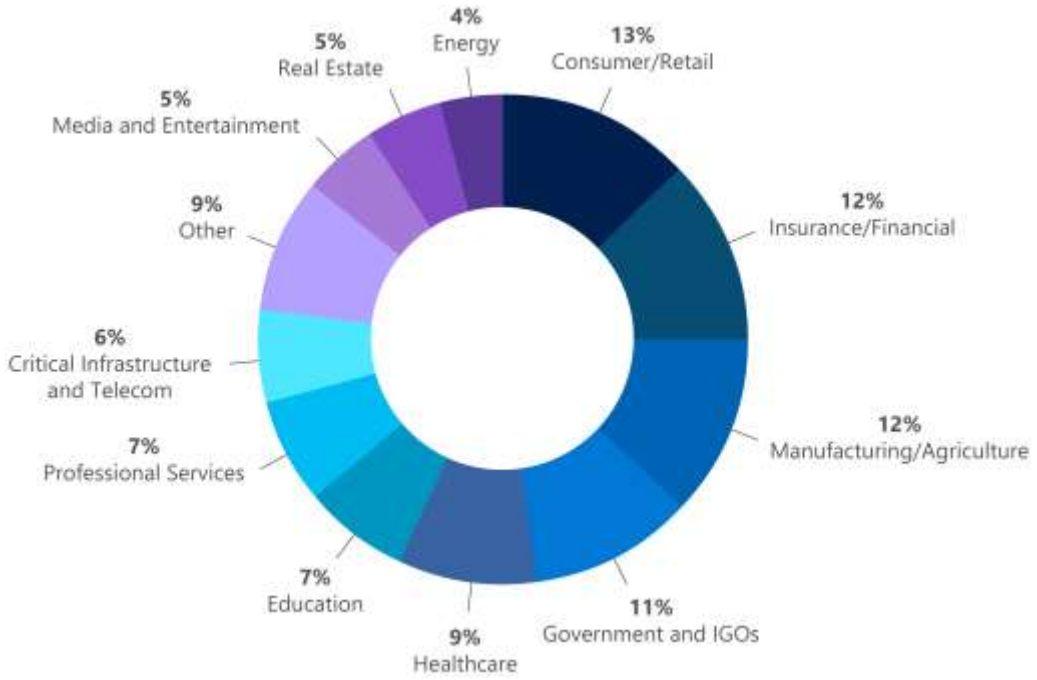
What we're seeing in ransomware data and signals

Ransomware encounter rate (machine count): Enterprise customers (Defender data)



Overall increase in ransomware encounters, with notable surge to consumer and commercial encounters in late 2019,6 when RaaS started to grow, and in early 2020 at the onset of the COVID-19 pandemic.

DART ransomware engagements by industry (July 2020-June 2021)



Deploy ransomware protection

The stakes have changed. There is a massive growth trajectory for ransomware and extortion.

Malicious email techniques

Collection

- Previous phish
- Purchasing list of email addresses
- Reconnaissance of specific targets
- Web-scraping

Lure development

- Current events
- Fake reply
- Impersonation
- Role-specific themes

Sender infrastructure

- Attacker-created sender
- Legitimate service abuse
- Compromised sender account
- Botnet

Email development

- Email header spoofing
- Encoded headers
- Hidden HTML attributes
- Invisible characters
- Procedurally generated image

Delivery

via: File

- Cloud-hosted file
- File container
- Password-protected file
- Uncommon file type

via: Link

- Domain impersonation
- Infinite subdomain
- Malformed URL
- URL redirector
- URL shortener
- Use of CAPTCHA
- Victim identifiable URL
- Compromised domain

ATTACKER OBJECTIVES

DEVICE CODE AUTHENTICATION PHISHING

CONSENT PHISHING

INTELLECTUAL PROPERTY THEFT

DISCOVERY / RECONNAISSANCE

EXTORTION

FINANCIAL FRAUD

CREDENTIAL PHISHING

MALWARE EXECUTION

All types of businesses are being targeted

"Over **1700** Organizations…
attacked by #Ransomware groups."

twitter.com/darktracer_int

Victim	Ransomware Group	Victim	Ransomware Group	Victim	Ransomware Group	Victim	Ransomware Group
4datanet.com		HNOLOGIES	MAZE	Fresh Water Systems	MAZE	https://prakhinlaw.com/	NetWalker
4th Judicial Distr			MAZE	Fuel Transport	MAZE	https://www.redplanethotels.com/	NetWalker
Aban Offshore			MAZE	Furniture Row & Visser Precision	DoppelPaymer	Hustech Installations AG hustech.ch	Sodinokibi (REvil)
Action for a Bett			DoppelPaymer	Fusion Connect, Inc.	MAZE	HYMAN GROUP COMPANIES	Sodinokibi (REvil)
Actuaries and As			MAZE	GAM - https://gamrentals.com	NetWalker	IBMC College	DoppelPaymer
Adam Kutner Ca			DoppelPaymer	GAR Equipment	Conti	ICM - International Commerce & Market	DoppelPaymer
Adams County M		PA.	MAZE	GCL System Integration Technology Co	MAZE	IHI-CSI.DE	CL0P
Adif (adif.es)			Pysa	Geidi.com	Sodinokibi (REvil)	Illinois Valley Community College	Pysa
Aebel		nt, LLC [NASA Contr	DoppelPaymer	Genesis Products Inc.	Sodinokibi (REvil)	Image one - https://i1ind.com/	Conti
Affordacare Urge		oment, Inc.	DoppelPaymer	Gestoria Auto Gestion	Conti	INDIABULLS.COM	CL0P
AFPA			MAZE	Ghantoo Group	MAZE	Indian River Transport Ltd.	MAZE
Agromart Group			MAZE	GILMER - Independent School District	AKO	Indoco Remedies Ltd	Nefilim
Agrosuper		://www.drivestream.co	NetWalker	Global Union Canada	Suncrypt	Information Connectivity Solutions Lim	MAZE
Ahmed Almazro		uncanco.com)	Sodinokibi (REvil)	Go West Tours	DoppelPaymer	Innotech-Execaire Aviation Group	MAZE
Aigües de Terras			Nefilim	GOODMANMINTZ	Sodinokibi (REvil)	Innovex	MAZE
Alaska General S		nc.	Sodinokibi (REvil)	Goodwill Industries of Kanawha Valley,	DoppelPaymer	INRIX.COM	CL0P
ALFANAR - https			Sodinokibi (REvil)	greatnortherncorp.com	Sodinokibi (REvil)	insport.com.au	Sodinokibi (REvil)
Aliansce Sonae			Conti	Greenville Technical College gvltec.ed	Avaddon	Instituto Costarricense de Acueductos y	MAZE
Allard		t Supply	MAZE	Groupe Cactus	Sodinokibi (REvil)	Integrity	MAZE
Allfasteners		sia - https://www.edip	NetWalker	Groupe Igrec, igrec.fr	MAZE	Interstate Restoration	MAZE
Alliance Building Services	Pysa	BostonCoach	Conti	Clayton Industries	MAZE	EDP Group	Ragnar_Locker	Groupe Interway	MAZE	J.W. Smith Customs Broker Ltd.	MAZE
Allison-Smith Company LLC	Sodinokibi (REvil)	Bouygues Construction	MAZE	ClearOne	MAZE	EFCO forms	Avaddon	Groupe Lefebvre M.R.P.	Pysa	Jacitara	MAZE
AMA Freight	MAZE	Brennercom AG	MAZE	CLLB Rechtsanwälte	MAZE	Egypt Yellow Pages Online	MAZE	Groupe Tech Industries	MAZE	JAMESTAN - Engineering LTD	AKO
Amacon - https://www.amacon.com	NetWalker	BRETAGNE TELECOM	DoppelPaymer	Clopay Ames True Temper Holding Co	DoppelPaymer	ehalc.com	Sodinokibi (REvil)	Grubman Shire Meiselas & Sacks	Sodinokibi (REvil)	Jands - https://www.jands.com.au	NetWalker
American Osteopathic Association	MAZE	bridgevacuum - bridgevacuum.com	NetWalker	Club Fitness	MAZE	Einhell Germany AG	MAZE	Grupo Damm	Sekhmet	jnbs	Sodinokibi (REvil)
Amicorp Group	Sodinokibi (REvil)	Bridgford Foods - www.bridgford.com	NetWalker	Coaching Headset Systems	DoppelPaymer	electric gas industries association inc	Conti	Grupo JdCocenzo	MAZE	John Christner Trucking	MAZE
Amphastar Pharmaceuticals, Inc	DoppelPaymer	brookfield.com	DarkSide	Columbus Metro Federal Credit Union	MAZE	Electricaribe	MAZE	Grupocif	Pysa	John Hardy	Pysa
Andrew Cross & Co.	MAZE	Brooks International	Sodinokibi (REvil)	COMHAR, INC	MAZE	Elsa LLC	Sodinokibi (REvil)	GSR srl	MAZE	Johnbear	Conti
Ansen Corporation	MAZE	Brown Automotive Group Ltd	Sodinokibi (REvil)	Commercial Development Company, In	DoppelPaymer	Empire Communities Corp.	DoppelPaymer	GST Autoleather Company	Ragnar_Locker	Johnson Air Products	MAZE
Antonio Citterio Architetto	MAZE	BROWN-FORMAN CORPORATION	Sodinokibi (REvil)	Community Development Bank	DoppelPaymer	Engineering Consultants Group	MAZE	Guillevin International Co.	MAZE	Joliet Park District	Conti
Apollo Tyres Ltd	NetWalker	Bruckner Truck Sales Inc	Conti	Complite Cash	DoppelPaymer	Entrust Energy - https://www.entrustener	NetWalker	HAC	Pysa	JX Enterprises, Inc	MAZE
AppliChem GmbH	MAZE	Bruns Building & Development	AKO	Comwave	MAZE	eurecat.com	Sodinokibi (REvil)	HAKUYOHIN	Sodinokibi (REvil)	Karmsund Maritime Offshore Supply AS	MAZE
Arabian Industries	MAZE	BRUSCHI S.P.A.	MAZE	Condie Construction Company	MAZE	Excis Ltd	Sekhmet	Haldiram Snacks Pvt. Ltd.	MAZE	Karmsund.no	Suncrypt
Argus Management Company, LLC	MAZE	Burger king Jamaica	Nefilim	Conduent, Inc. & Unamic	MAZE	EXECUPHARM.COM	CL0P	Hamilton-Brown	AKO	KCG, Inc.	DoppelPaymer
Armour & Associates	Sodinokibi (REvil)	BURHANIGLASS.AE	Sodinokibi (REvil)	Conklin Office Furniture	MAZE	Express Manufacturing, Inc.	MAZE	Handelshof Stendal GmbH	MAZE	Kenneth Cole Productions	Sodinokibi (REvil)
Artech Information Systems LLC	MAZE	Burton Lumber	MAZE	Container Graphics Corporation - https:	NetWalker	Faic	Pysa	Haywood County Schools Network	Suncrypt	Kent County Trading Ltd	DoppelPaymer
Arteris SA	Nefilim	Busch's Inc.	MAZE	Container Marketing, Inc	DoppelPaymer	Fairfax County Public Schools	MAZE	Hedinger & Lawless, LLC	MAZE	Kerr Controls Limited	MAZE
ASCENT Network	Sodinokibi (REvil)	C & K Market, Inc.	MAZE	Cornet Vincent Ségurel	MAZE	Famisanar	Pysa	HEDLAW - Law & Business Law	MAZE	Kimchuk Inc.	DoppelPaymer
ASU Inc. - ASU-NVG.COM	AKO	Caldwell Toyota	MAZE	Corporate Renaissance Group - https://	NetWalker	Faxon Machining, Inc.	MAZE	Henning Harders Pty Ltd	MAZE	KollerCraft	MAZE
Asunaro Aoki Construction Co.,Ltd.	DoppelPaymer	Callaway Architecture, LLC	DoppelPaymer	Cosan	Nefilim	FERSPED Inc.	MAZE	Hershey Equipment Co Inc	Conti	Kristin Tarbet, Plastic Surgeon	MAZE
athrone.com	Sodinokibi (REvil)	Cambria County, Pennsylvania	Conti	COTTONWOOD FINANCIAL INC	Sodinokibi (REvil)	FGXI	Sodinokibi (REvil)	HMR Ltd - Hammersmith Medicines Res	MAZE	KUHNLE-TOURS GmbH	MAZE
Atlanta Computer Group, Inc.	MAZE	Canadian Tire	NetWalker	CPFL Energia	MAZE	Filtration Group	Conti	Hms Insurance Associates, Inc	Conti	L&F DISTRIBUTORS (LNF)	MAZE
Atlas Machinery	MAZE	Canon USA, Inc.	MAZE	CRE Credit Services	NetWalker	Fincamex	Pysa	Hoa Sen Group	MAZE	Laboratoires Expanscience	MAZE
Austin College	NetWalker	Canpar Express	DoppelPaymer	Cretsenbelledonne	Pysa	Fisher & Paykel	Nefilim	Hodell-Natco Industries, Inc.	MAZE	Lakeland Community College	MAZE
australian company ARAFMI	Sodinokibi (REvil)	Capital Lumber Company	MAZE	Critical Control Energy Services	MAZE	Florida Chamber of Commerce	Conti	HOEDLMAYR.COM	CL0P	Lally Ford	MAZE
Automatic Handling International - http	NetWalker	Carbon Power and Light	Conti	CSA Group	MAZE	Florsheim Homes	MAZE	Holston Gases	MAZE	Landmarkresort hotel beach	Conti
aVINC	MAZE	CAT RICAMBI SRL Italy car sale compa	Sodinokibi (REvil)	CU Collections	MAZE	FlorStar - https://www.florstar.com	NetWalker	Holy-Dis	MAZE	Lawyers network	MAZE
Axxess International Inc	Conti	Catania, Mahon & Rider, PLLC	Ragnar_Locker	CubeLogic - https://www.cubelogic.com	NetWalker	Fondazione Arena di Verona	MAZE	Homestead Management Corporation	MAZE	Lectra	MAZE
Bailey&Galyen Attorney	Ragnar_Locker	CB Masonry	Conti	Curtze Food Service	MAZE	FPI Management	Suncrypt	Horizon Controls	Conti	Lee & Associates, LLC	MAZE
Baker Wotring LLP	MAZE	CBKLAW	Sekhmet	Cutrale (oranges)	MAZE	Fraser Wheeler & Courtney LLP	Sodinokibi (REvil)	Hot Line Freight Systems	DoppelPaymer	Léon Grosse	MAZE

Ransomware statistics and trends

Ransomware is one of the top threats in cybersecurity. With **878 cyberattacks in 2020**, **18%** of which **were ransomware**, according to the Identity Theft Resource Center.

Organizations around the world are being held hostage by ransomware, with many paying up solely to avoid the cost and downtime of not paying the criminals.

In short, cybercriminals are making and demanding more money than ever.

- The **average ransom paid increased 171% from 2019 to 2020** ($115,123 to $312,493), said the 2021 Unit 42 Ransomware Threat Report.
- The highest ransom paid **doubled from 2019 to 2020 from $5 million to $10 million**.

Source: https://www.csoonline.com/article/3634869/top-cybersecurity-statistics-trends-and-facts.html

S$ 3.6M

Average organizational cost of a data breach in ASEAN in 2019*

96 percent of Singaporean businesses reported suffering a data breach between September 2018 and September 2019.*

Singapore, January 2019: second health data breach in six months*

Philippines, January 2019: Cebuana's marketing server breached*

"More than 900,000 clients of Philippine-based pawnshop Cebuana were affected by a data breach"

Thailand and Vietnam, March 2019: Toyota suffers a chain of data breaches*

Singapore, July 2018: the city-state suffers its largest data breach*

"largest data breach in its history with 1.5 million patients affected by it, including Prime Minister Lee Hsien Loong"

Philippines, May 2018: Wendy's and Jollibee asked to take preventive measures against data breaches*

* https://www.csoonline.com/article/3532816/the-biggest-data-breaches-in-southeast-asia.html

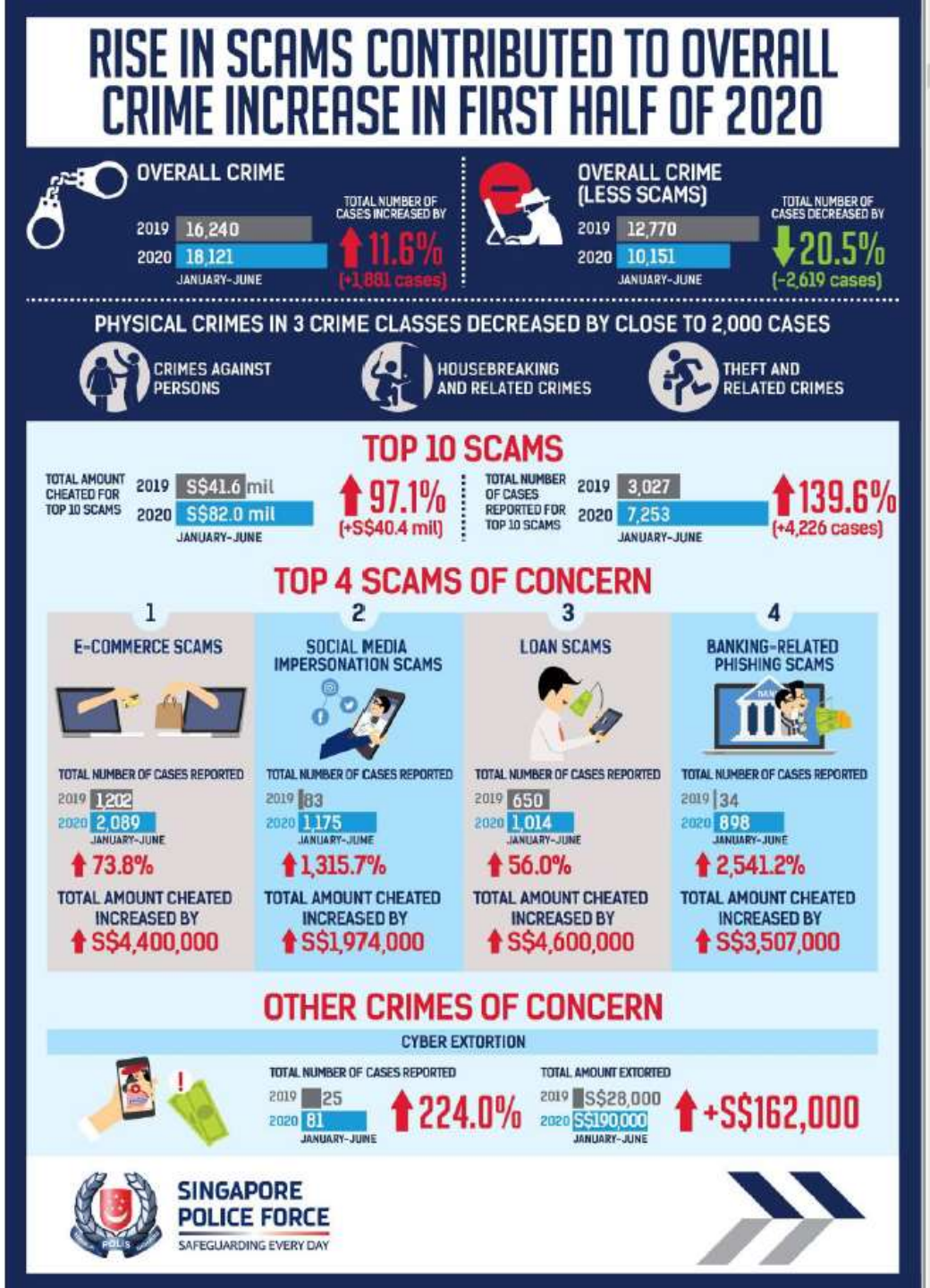
Banking-related phishing scams spike more than 2,500% in first half of 2020 in Singapore

CNA, Singapore

The scammers told the victim that his accounts have been hacked and they needed his OTPs to disable his bank accounts.

Police warned that platforms like IMO, Viber and WhatsApp were also commonly used by these scammers to communicate with their victims.

E-COMMERCE SCAMS REMAIN TOP SCAM TYPE

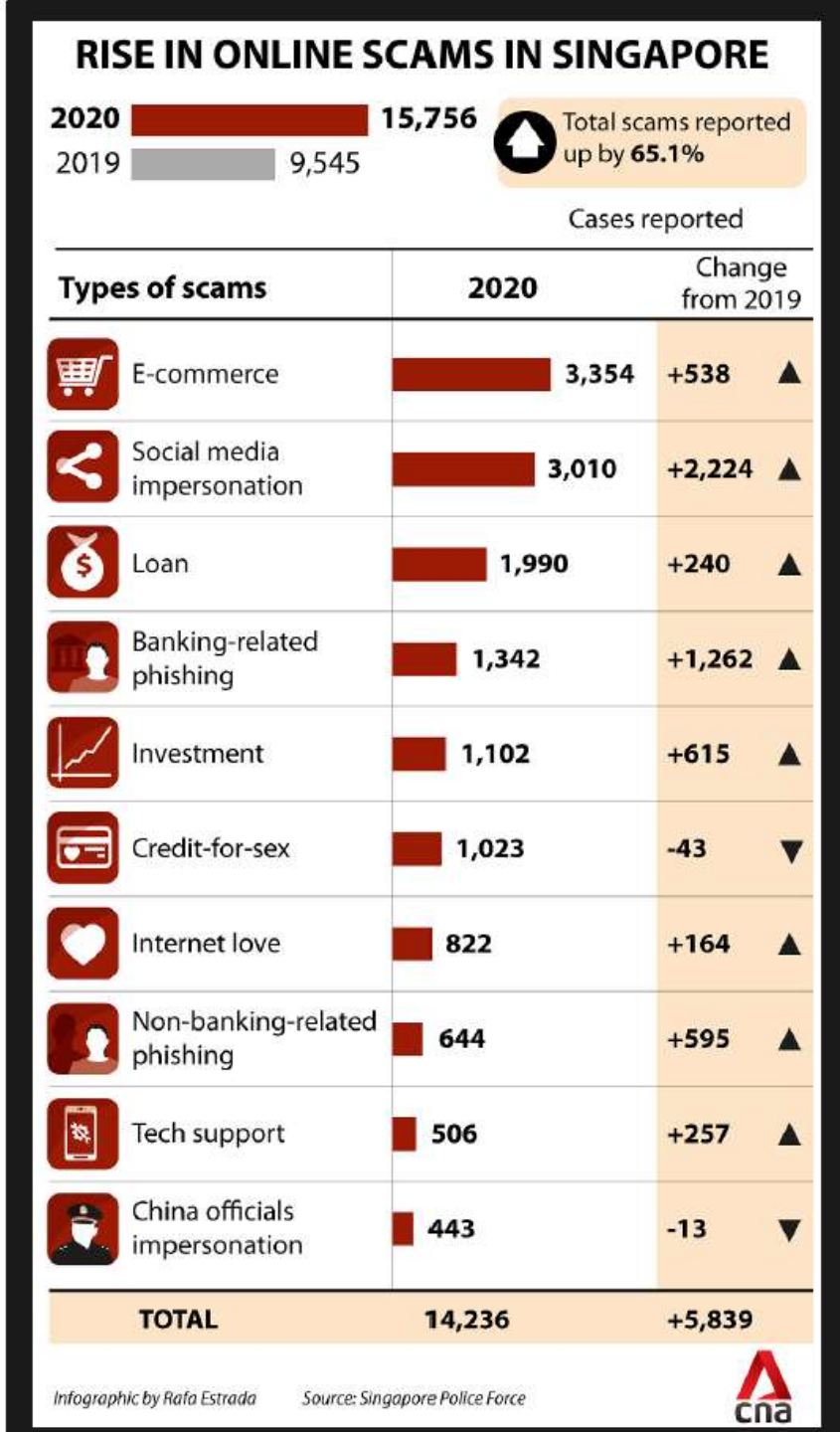


More than 180 investigated over scams involving S$1.5 million in Singapore

"Scammers would often claim to help their victims sign up for online contests or promotions which turned out to be fake.

"Their victims would later discover that unauthorised transactions had been made from their bank accounts or mobile wallets,"

Instagram and Facebook were the most common social media platforms where such scams took place



Southeast Asia a hotbed for phishing attacks

During the first half of 2019

Philippines had the highest percent of phishing victims at 17.3%.

→

Malaysia scored the second highest at 15.829% of users infected through phishing from 11.253% in the first half of 2018

Coming behind was **Indonesia** with 14.316% from 10.719% in previous year,

→

Thailand at 11.972% from 10.9% and

Vietnam followed closely at 11.703% from 9.481%.

→

Singapore recorded 5% this year compared to 4.142% posted previous year.

Source: https://securitybrief.asia/story/southeast-asia-a-hotbed-for-phishing-attacks

Attacks are paying off

- Escalating Ransom demands
- Double extortion
- Significant profits

Ryuk ransomware Bitcoin wallets point to $150 million operation (bleepingcomputer.com)

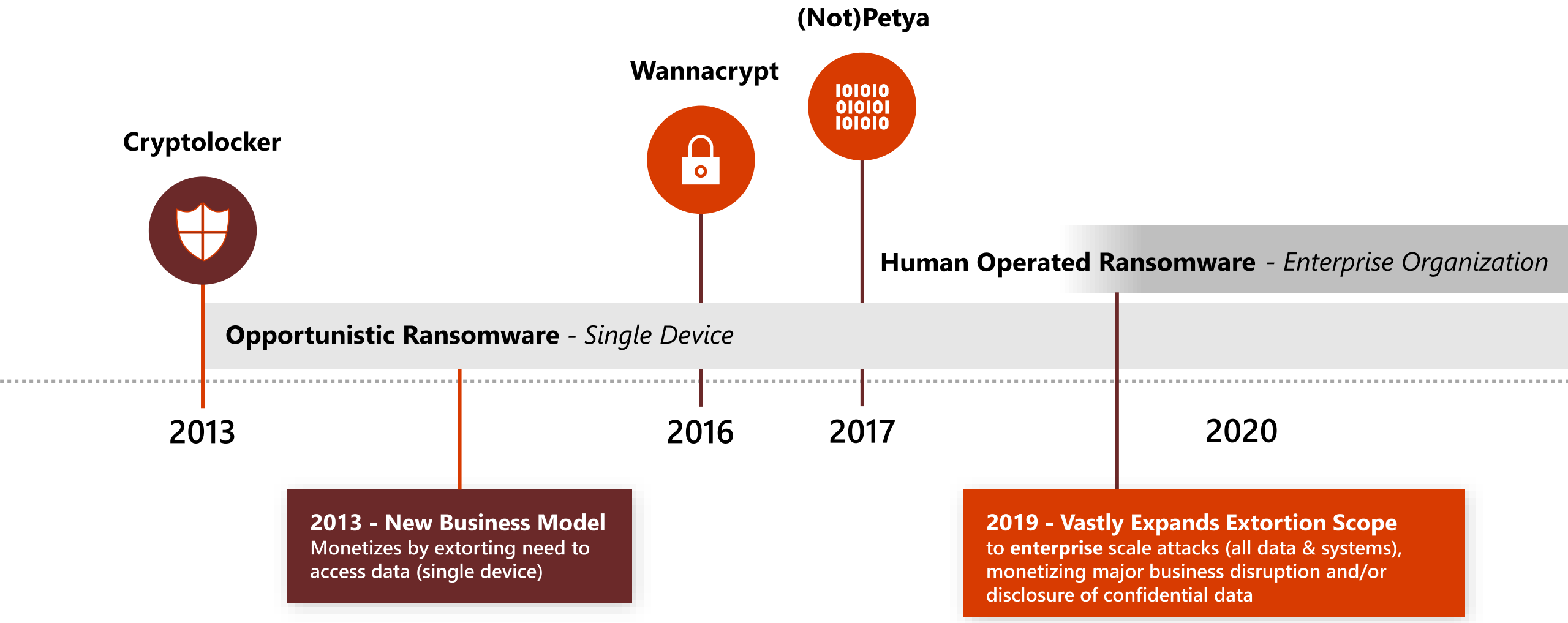
Ryuk ransomware Bitcoin wallets point to $150 million operation

By Ionut Ilascu

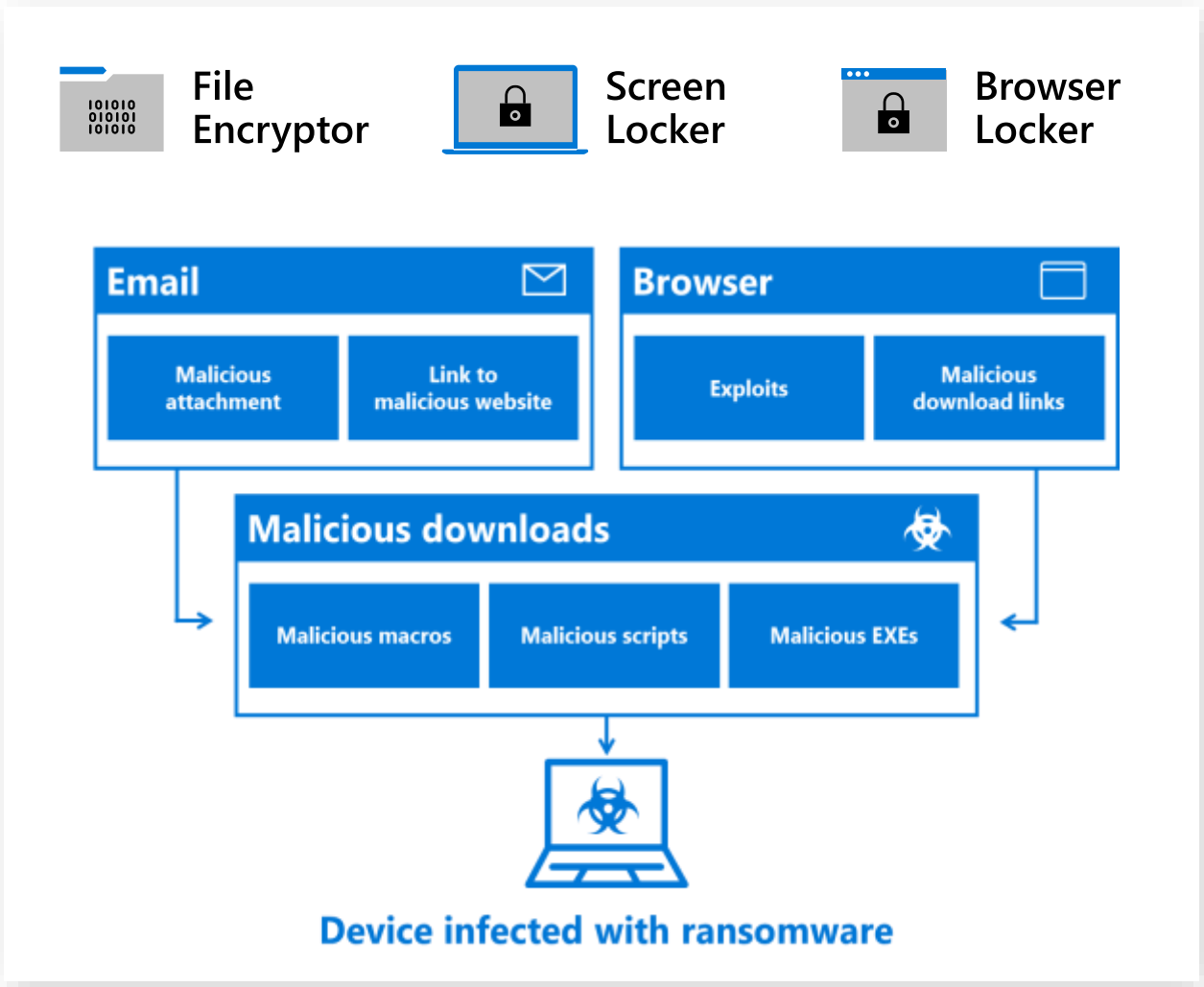
January 7, 2021 07:17 PM 0

Security researchers following the money circuit from Ryuk ransomware victims into the threat actor's pockets estimate that the criminal organization made at least $150 million.

Evolution of ransomware models



Commodity Ransomware



Commodity typical infection chain

Exposure

- Spam email or URL with malicious JS, HTM, VBS, Office Docs etc.

Infection

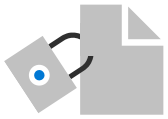
- Script Downloader
- Downloads ransom Malware

Dynamics

- Install Process
  Dump a copy install to appdata folder
- Autostart creation
  Creates auto start registry
- Inject Malicious Code
  Rename process, restart initiates MW

Clean up

- Encrypt User Files
  Begin encryption once restarts are complete
- Display Ransom Note
- Delete Shadow Copies
- Uninstalls itself



Human Operated Ransomware - high impact & growing

Not another background security risk

What's different?

High Business impact

Extortion must disrupt business operations to motivate payment

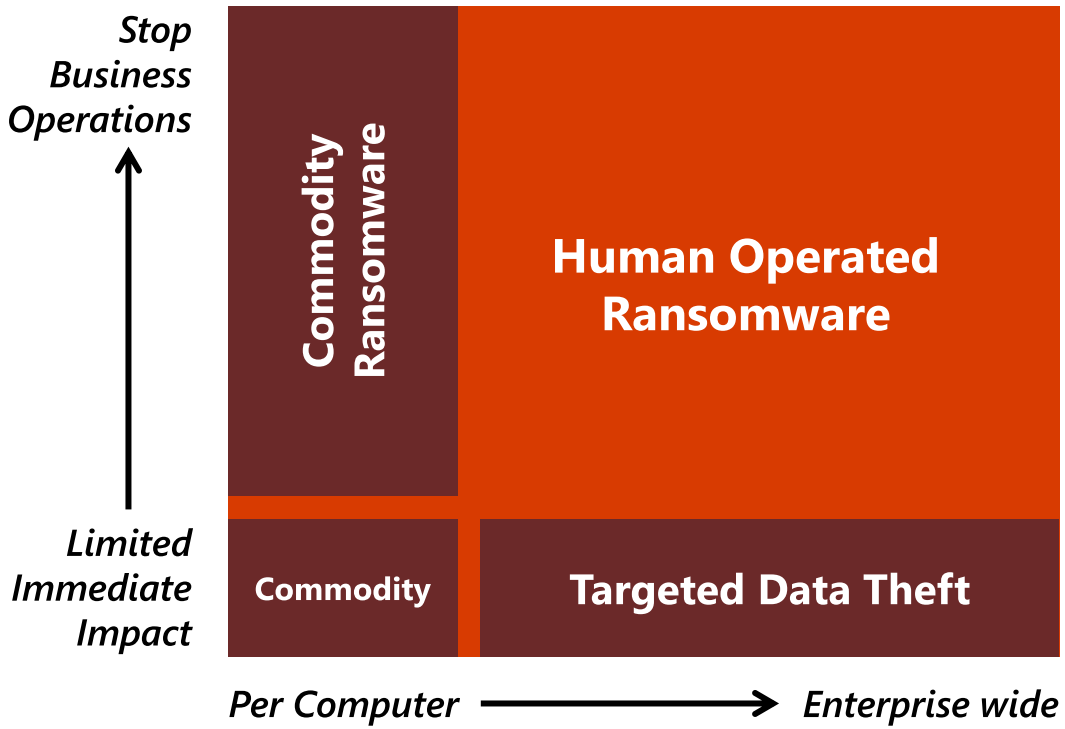
Profitable for Attackers

Economic incentive to continue growing

Room to Grow

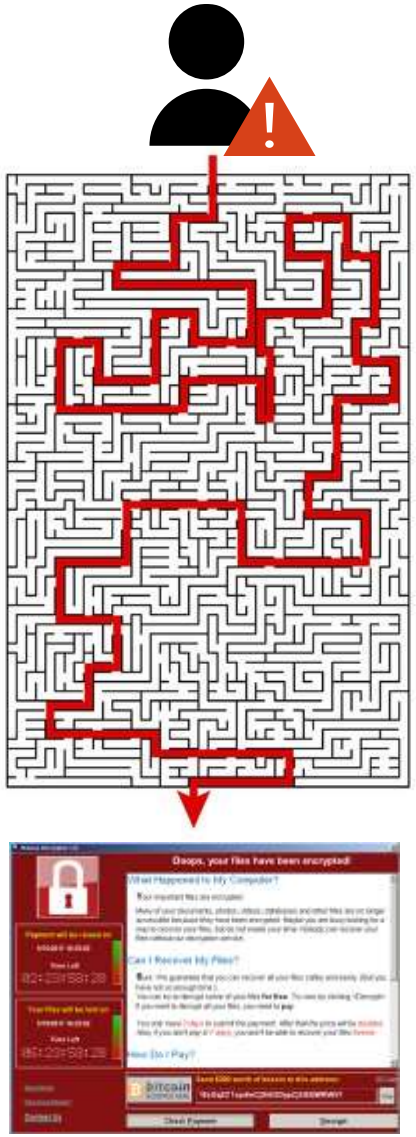
Attackers can monetize security maintenance gaps at most enterprises:

- **Apply security updates** consistently to all computers
- **Securely configure all resources** using manufacturer best practices
- **Mitigate credential theft** attacks for privileged users



What makes Human Operated Ransomware different?

- **Human Operated Ransomware**
  - Trojan
  - Disable AV
  - Credential theft
  - Cobalt Strike
  - Network recon
  - Additional backdoors
  - Clear logs
  - Exfiltrating data
  - Ransoming device



Human Operated Ransomware **attacks are not pre-programed** and adjust as needed

Paying the ransom doesn't remove the attacker

COVID-19 Outbreaks saw Human Operated Ransomware **target critical systems** and frontline workers

Open-sourcing new COVID-19 threat intelligence - Microsoft Security

Ransomware adversaries are evolving strategies to 10x their business too

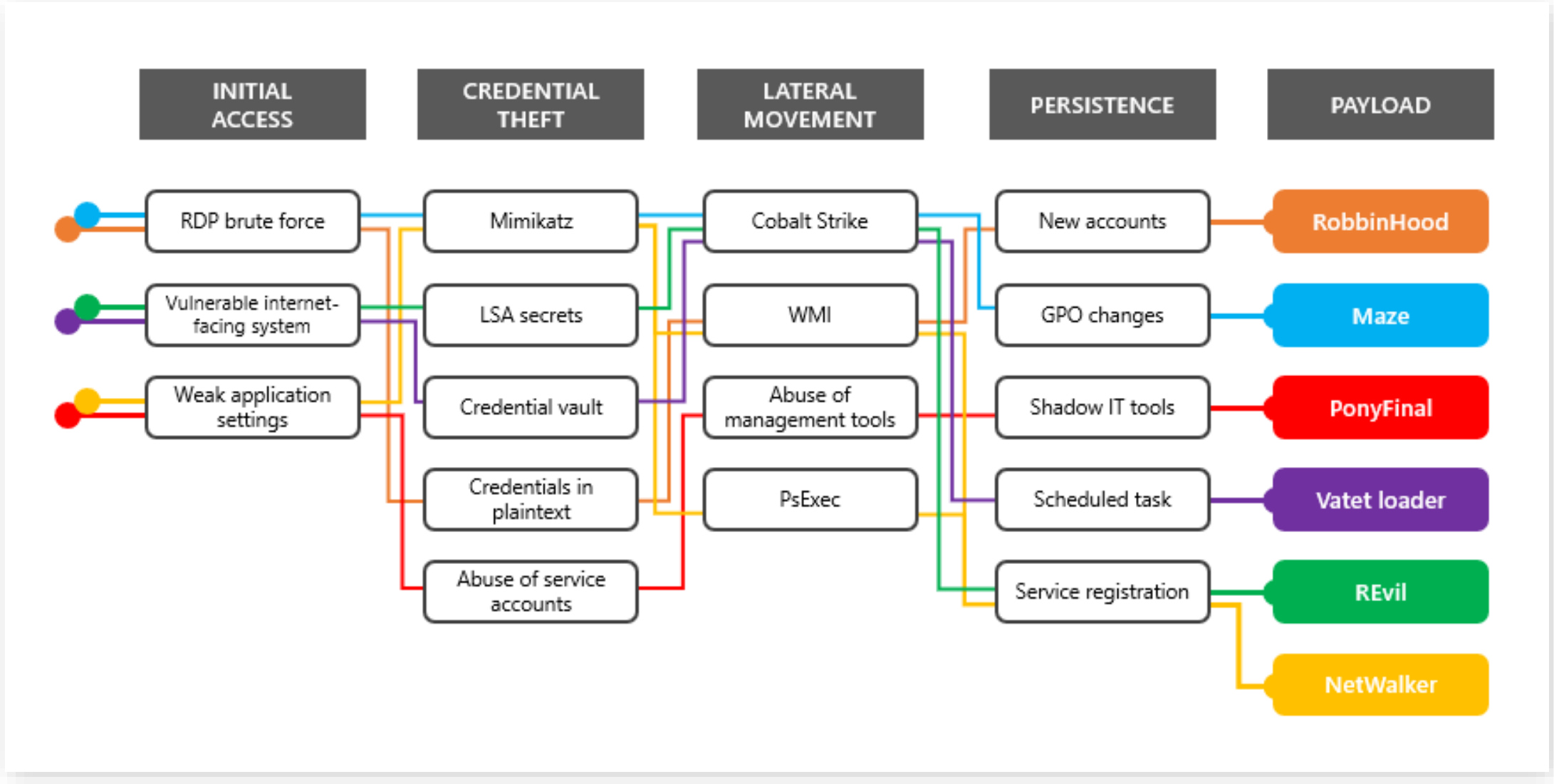
Commodity Ransomware

- Targets **individual**
- **Pre-programed attacks** that are best-effort
- **Opportunistic** data encryption
- Unlikely to cause catastrophic business disruption
- Successful defense is **malware remediation**

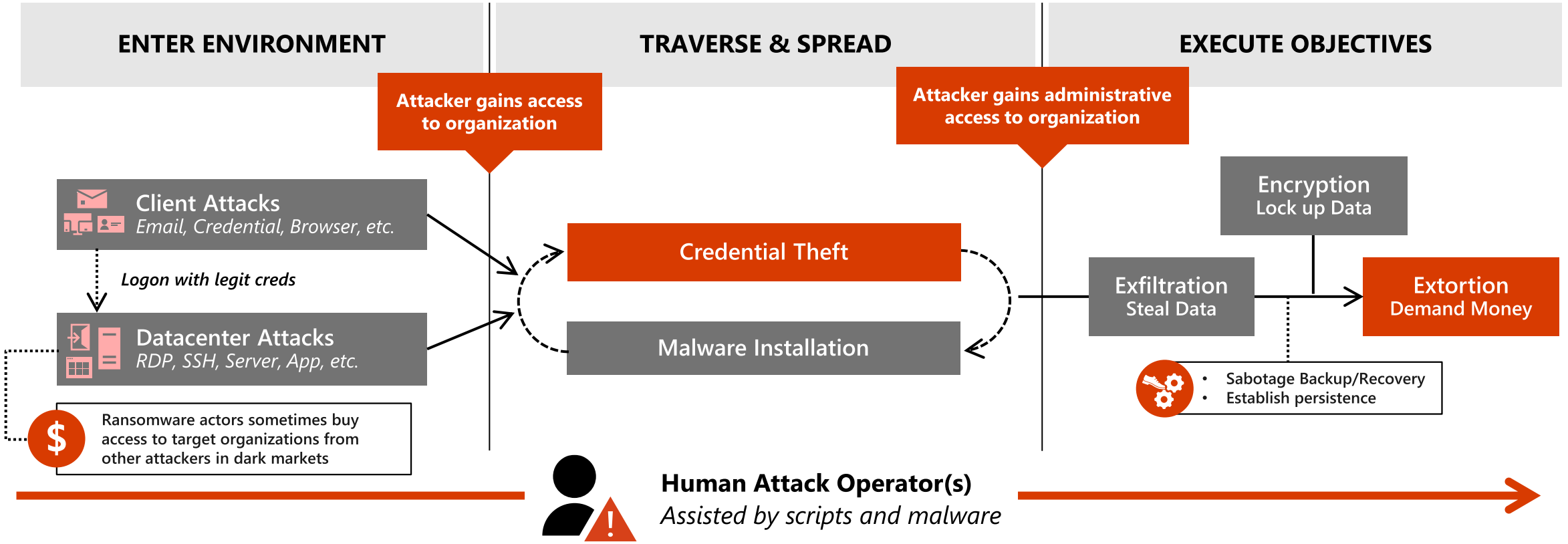
Human Operated Ransomware

- Targets **entire company**
- Customized attacks driven by **determined human intelligence**
- **Calculated** data encryption / data exfil
- Guaranteed to cause **catastrophic** and **visible** business disruption
- Successful defense is **adversary eviction**

Human Operated Ransomware – Mode of operation



Pattern – Human Operated Ransomware



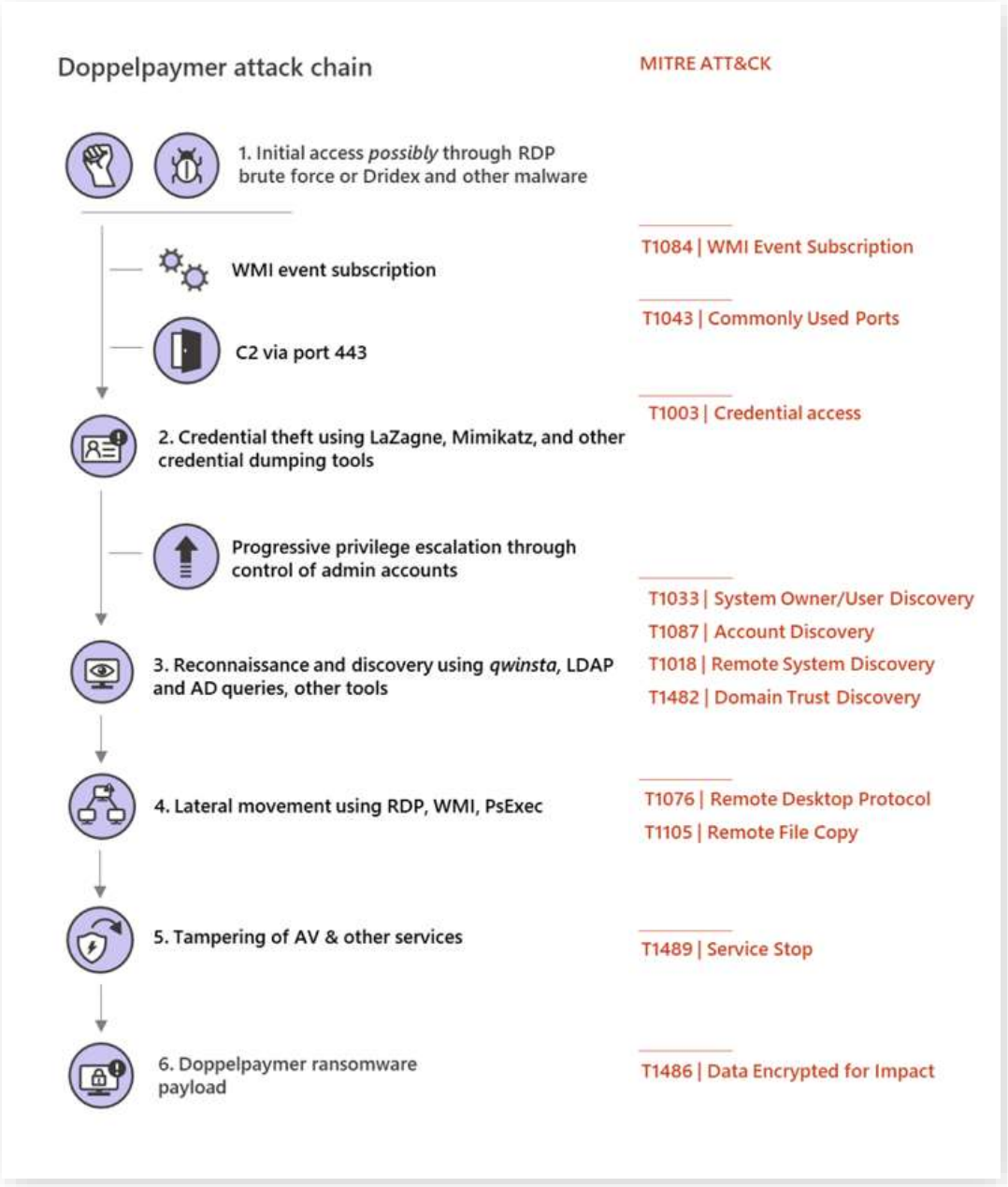
Ryuk example (Email)

Wadhrama example (RDP)

Comparison to traditional ransomware

Example:

Human operated ransomware kill chain with prevention controls



The Colonial Pipeline Ransomware Attack

Colonial Pipeline incident overview

6th May 2021

Malicious actors launch an attack, stealing data, locking computers, and requesting a ransom.

7th May 2021

Colonial Pipeline pays the ransom.

8th May 2021

Colonial Pipeline publicly announces attack, then shuts off servers and some pipelines.

9th May 2021

Colonial Pipeline makes a second public announcement, discussing its system restart plans.

10th May 2021

The FBI confirms DarkSide ransomware caused the attack, and Colonial Pipeline releases two more statements around its restoration process.

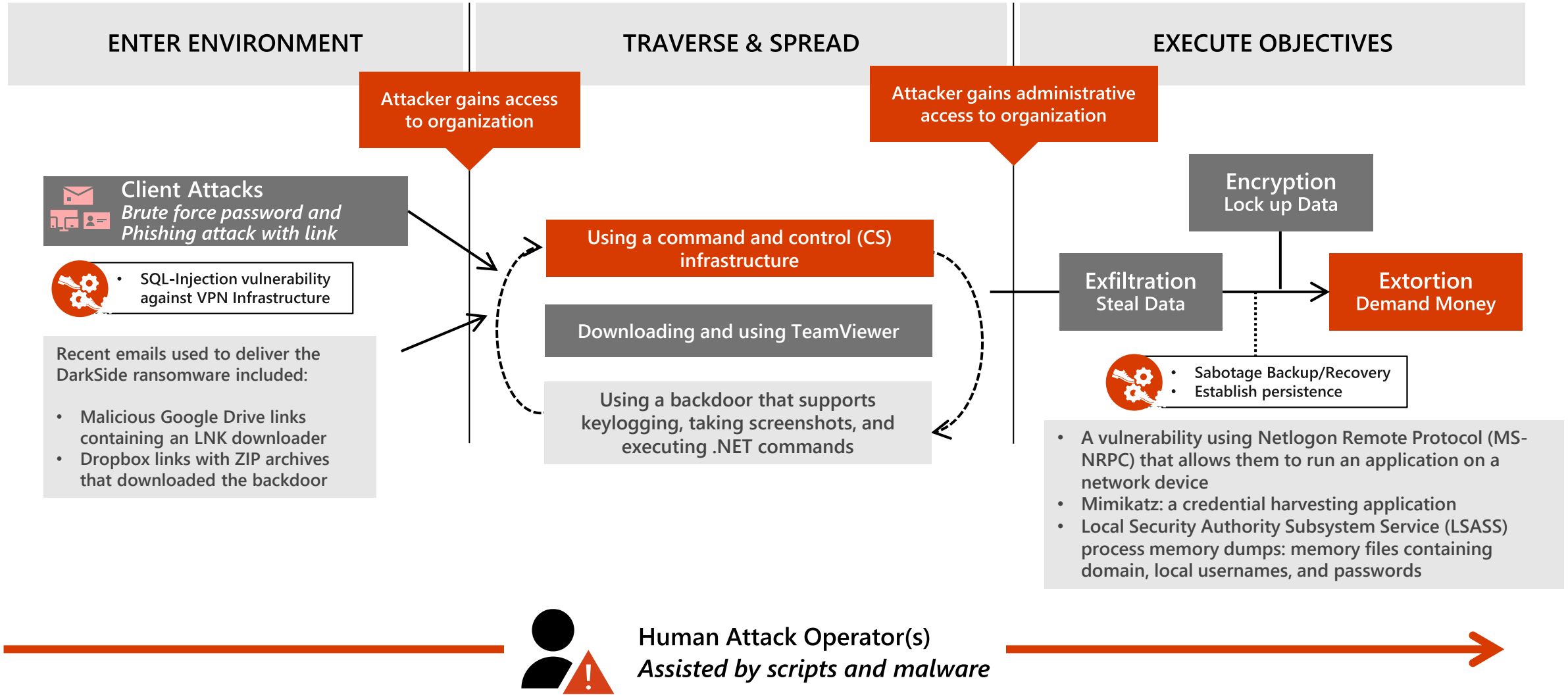
11th May 2021

Federal agencies release an advisory describing DarkSide ransomware and mitigation strategies while Colonial Pipelines releases a statement around fuel shipping.

12th May 2021

Colonial Pipeline restores operations and announces fuel delivery timelines, amidst people “panic buying” gasoline.

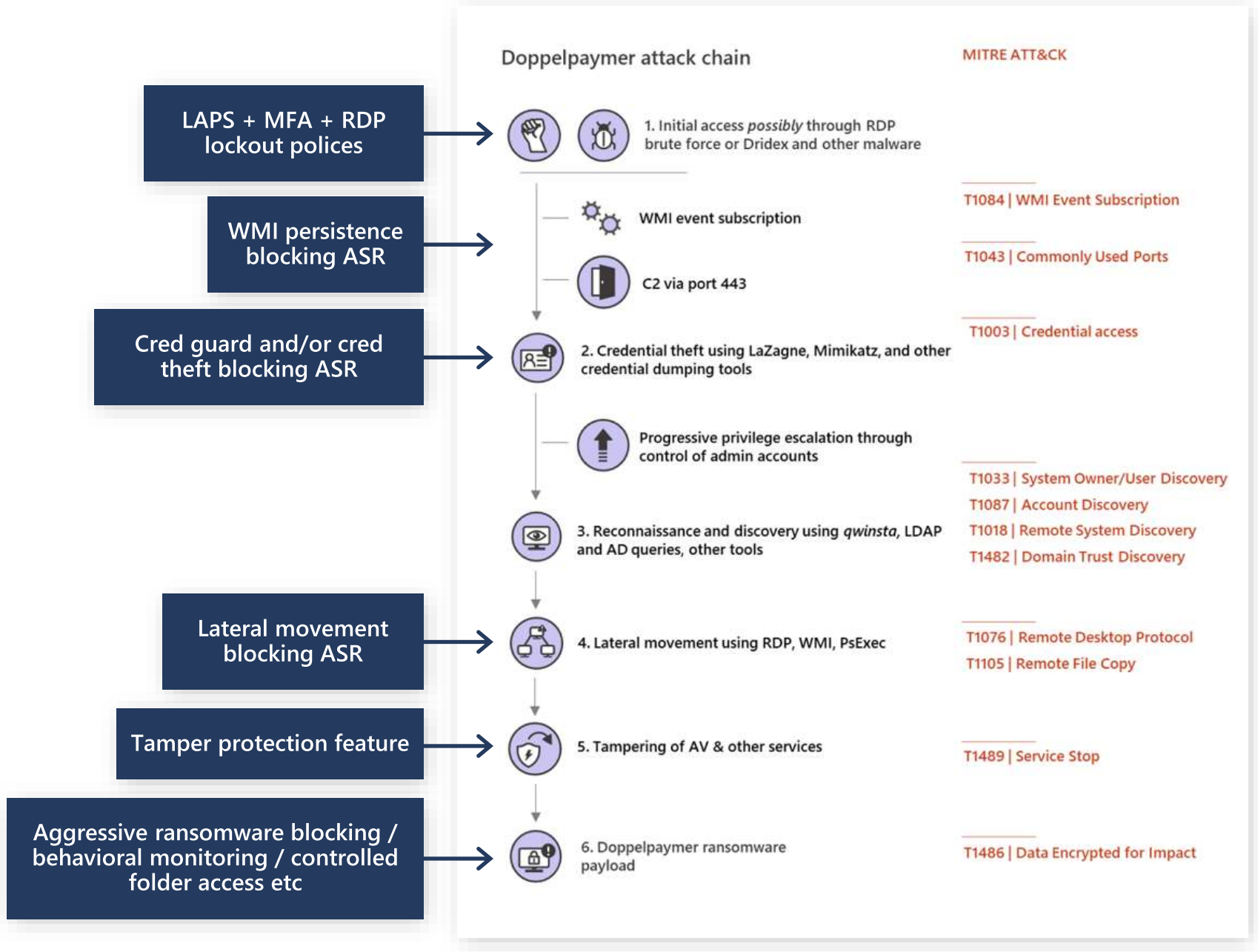
DarkSide Ransomware – How it worked



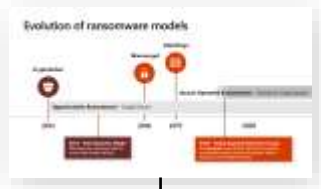
Attack surface Reduction (ASR)

Mapping rules to Human Operated Ransomware (HumOR)

[Use attack surface reduction rules to prevent malware infection]



Key Takeaways



Stakes have changed with evolved threat

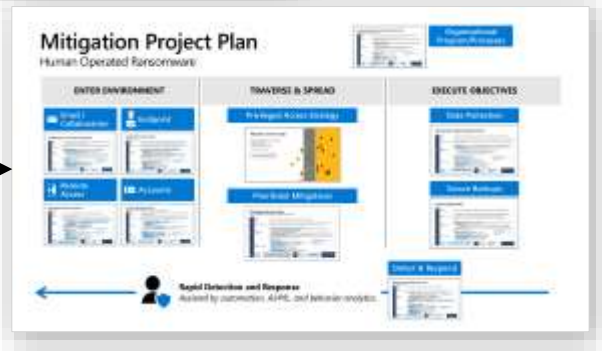
New attacker business model changes the impact and likelihood of attacks

No End in Sight – potential explosive growth trajectory from

- ***Attacker Profitability*** to fund and incent future attacks
- ***Lack of resistance*** to growth from legal or technical obstacles

Attacks have Weaknesses – efficient extortion relies on

- ***Getting asset access*** – rapidly via admin privielges
- ***Denying recovery*** – via backups and recovery processes



Urgently Follow Mitigation Plan – for critical defenses

1. ***Rapidly and securely restore*** critical business operations
2. ***Protect Admins*** to strengthen privielged access security
3. ***Clean up common/cheap entry points*** to continually increase attacker cost and friction

Mitigation Project Plan

Human Operated Ransomware

Organizational Program/Processes

ENTER ENVIRONMENT

Email / Collaboration

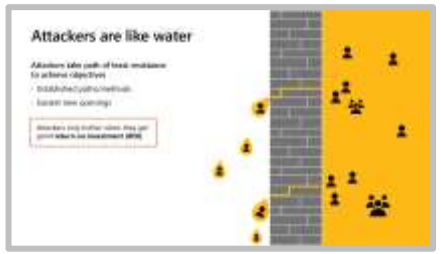
Endpoint

Remote Access

Accounts

TRAVERSE & SPREAD

Privileged Access Strategy



Prioritized Mitigations

EXECUTE OBJECTIVES

Data Protection

Secure Backups

Detect & Respond

Rapid Detection and Response

Assisted by automation, AI/ML, and behavior analytics

The cybersecurity bell curve:

Basic security hygiene still protects against 98% of attacks

Enable multifactor authentication

Make it harder for bad actors to utilize stolen or phished credentials by enabling multifactor authentication. Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.

Apply least privilege access

Prevent attackers from spreading across the network by applying least privilege access principles, which limits user access with just-in-time and just-enough-access (JIT/JEA), risk-based adaptive polices, and data protection to help secure both data and productivity.

Keep up to date

Mitigate the risk of software vulnerabilities by ensuring your organization's devices, infrastructure, and applications are kept up to date and correctly configured. Endpoint management solutions allow policies to be pushed to machines for correct configuration and ensure systems are running the latest versions.

Utilize antimalware

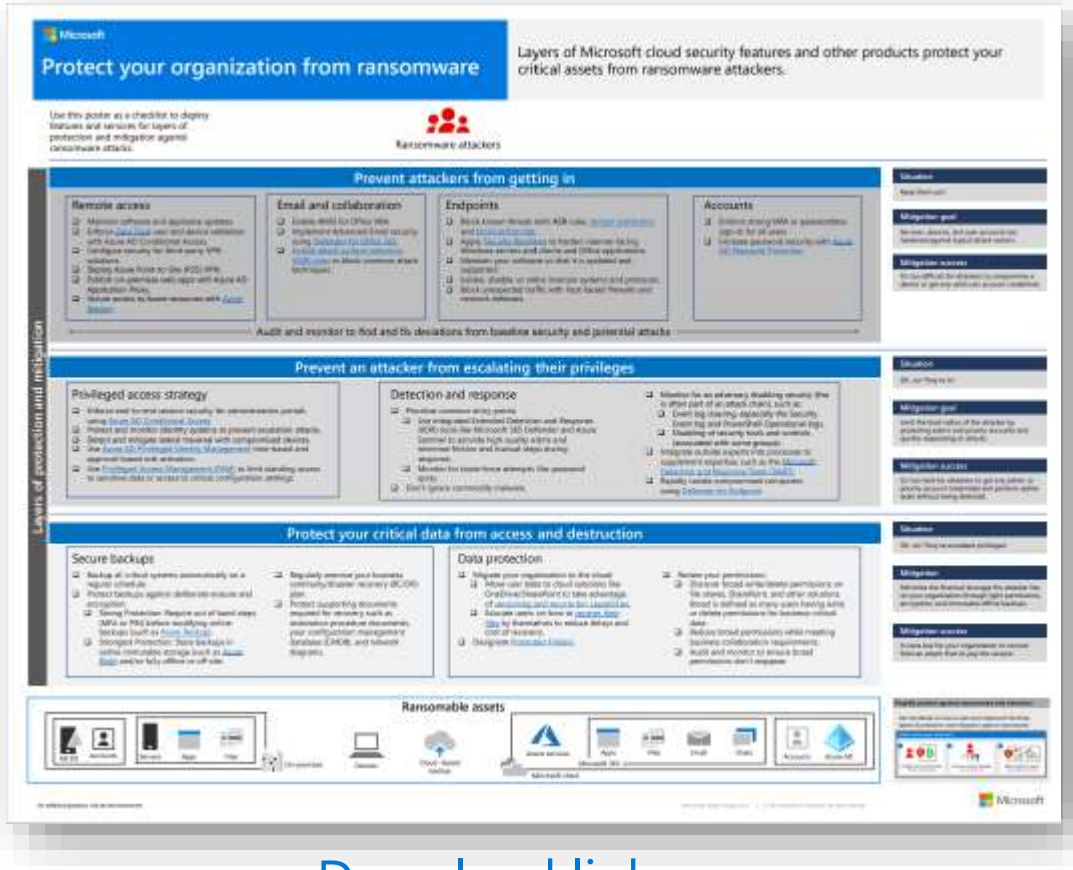
Stop malware attacks from executing by installing and enabling antimalware solutions on endpoints and devices. Utilize cloud-connected antimalware services for the most current and accurate detection capabilities.

Protect data

Know where your sensitive data is stored and who has access. Implement information protection best practices such as applying sensitivity labels and data loss prevention policies. If a breach does occur, it's critical that security teams know where the most sensitive data is stored and accessed.

Resources and blogs link

- [Human-operated ransomware | Microsoft Docs]
- [Human-operated ransomware attacks: A preventable disaster - Microsoft Security Blog]
- [Rapidly protect against ransomware and extortion | Microsoft Docs]
- [Azure backup and restore plan to protect against ransomware | Microsoft Docs]
- [A guide to combatting human-operated ransomware: Part 1 - Microsoft Security Blog]
- [How cyberattacks are changing according to new Microsoft Digital Defense Report - Microsoft Security Blog]
- [Microsoft Digital Defense Report – Microsoft Security]



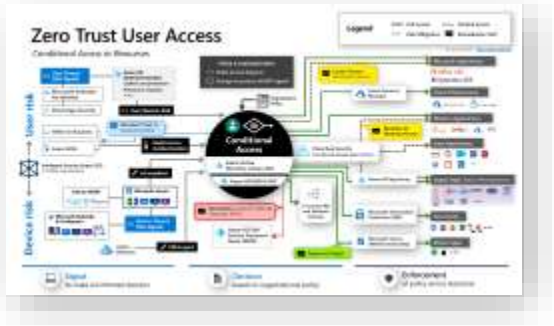
[Download link]

Q&A

Additional Information

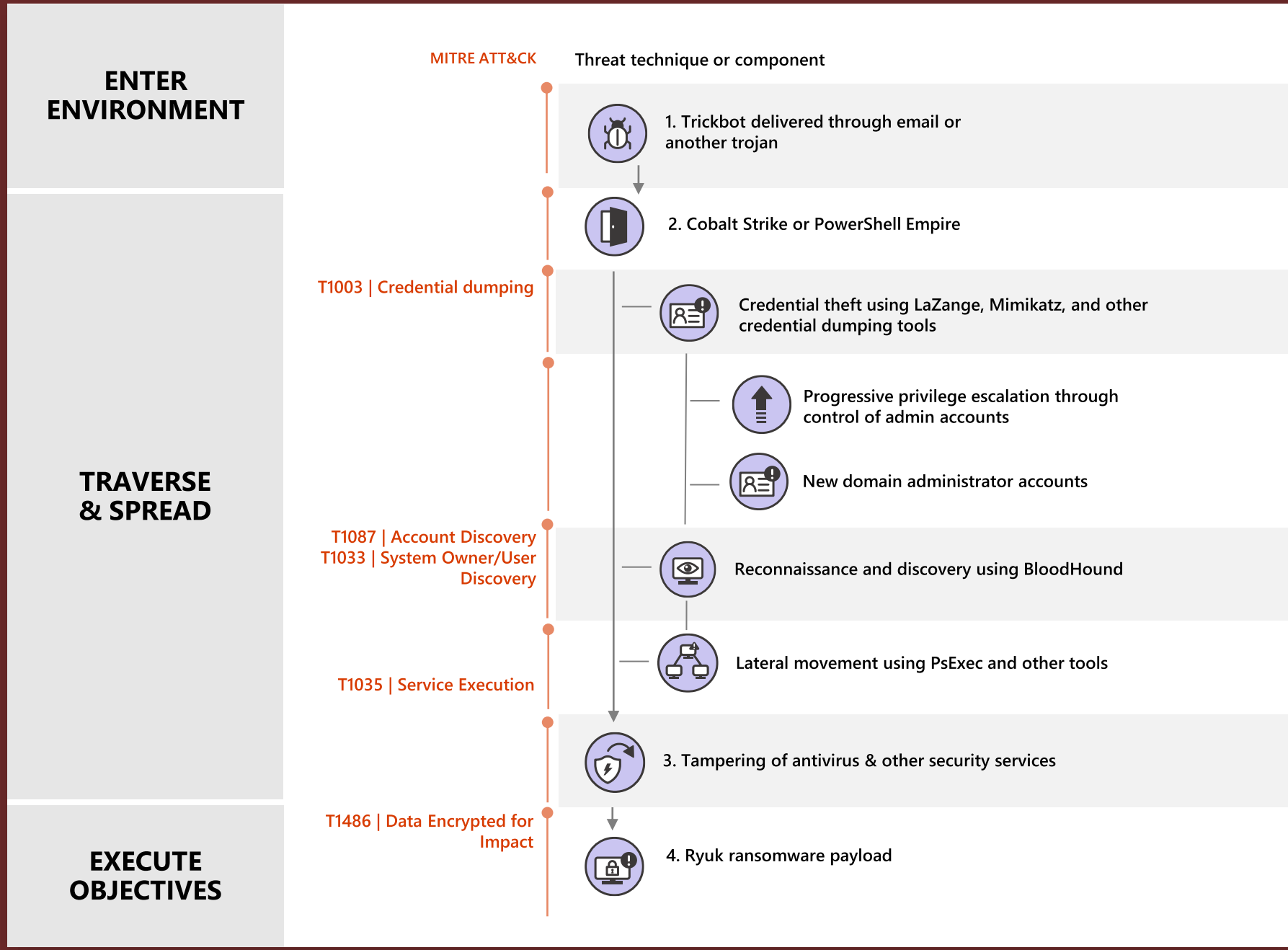
Windows Platform Protections

Attack Surface Reduction (ASR)



Zero Trust User Access

Ryuk Ransomware



Wadhrama Ransomware

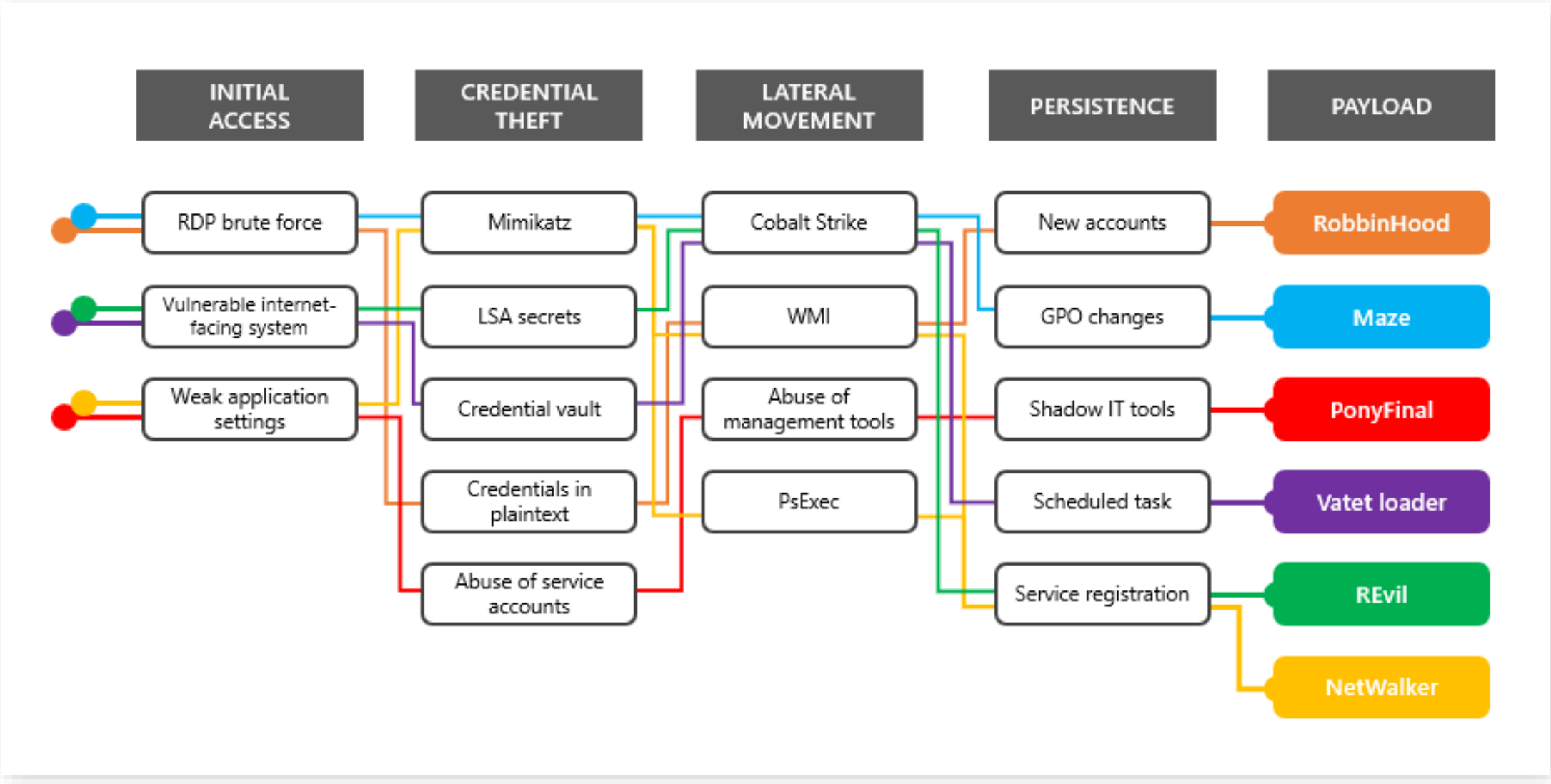
ENTER ENVIRONMENT

TRAVERSE & SPREAD

EXECUTE OBJECTIVES

MITRE ATT&CK	Threat technique or component
T1076 | Remote Desktop Protocol T1110 | Brute Force	1. RDP brute force
	2. Scan for connectivity and performance
	RDP brute force against new targets
T1089 | Disabling Security Tools	3. Turn off security controls
T1046 | Network Service Scanning	4. Network recon
	Lateral movement
T1003 | Credential Dumping	5. Credential theft
T1136 | Create Account T1219 | Remote Access Tools T1060 | Registry Run Keys / Startup Folder	6. Backdoor & persistence
	7. Coin miner, spammer
T1486 | Data Encrypted for Impact	8. Ransomware

Human Operated Ransomware



Collaboration and Email Security Plan

What Objective	**Implement best practices for email and collaboration solutions to make it more difficult for attackers to abuse them, while allowing internal users to easily and safely access external content.**
Why Importance and benefits	Attackers frequently enter the environment by transferring malicious content in with authorized collaboration tools such as email and file sharing and convincing users to run it. Microsoft has invested in enhanced mitigations that vastly increase protection for these attack vectors.
How Implementation Instructions	❑ **Enable** **AMSI for Office VBA** to detect Office macro attacks with endpoint tools like Defender for Endpoint ❑ **Implement Advanced Email security** using Defender for Office 365 or a similar solution ❑ **Enable attack surface reduction (ASR) rules** to block common attack techniques including ○ **Endpoint Abuse -** Credential theft, ransomware activity, and suspicious use of PsExec and WMI ○ **Weaponized Office document** activity including advanced macro activity, executable content, process creation, and process injection initiated by Office applications. ***Note:*** Deploy these rules in ***audit*** mode first, then ***assess*** any negative impact, and then deploy them in ***block*** mode. ❑ **Audit and Monitor –** to find and fix deviations from baseline and potential attacks (see *Detection and Response Plan*)
Who Assign Accountability	**Sponsorship –** CISO or CIO **Project Leadership –** Security Architecture **IT Architecture –** Prioritize components +integrate into architectures **Cloud Productivity / End User Team –** Enable Defender for Office 365, ASR, AMSI **Security Architecture / Infrastructure + Endpoint** – Configuration assistance **User Education Team** – update any guidance on workflow changes **Security Policy and Standards –** Update standards and policy documents **Security Compliance Management** – Monitor to ensure compliance

Enter Names for the Team
Sponsor - Jane Smith
Lead – John Doe

Measure Key Results	**% of computers with all protections enabled**	**When** To Complete	**Typically within 30 days**	**##-##-2021**

Endpoint Protection Plan

Clients + Servers + Browsers

What
Objective

Implement relevant security features and rigorously follow software maintenance best practices for computers and applications, prioritizing applications and server/client operating systems directly exposed to internet traffic and content

Why
Importance and benefits

Internet exposed endpoints are a common entry vector that provide attackers access to the organization's assets.
Prioritize blocking common OS and application with preventive controls to slow or stop them from executing the next stages.

How
Implementation Instructions

Apply these best practices to all Windows, Linux, MacOS, Android, iOS, and other endpoints (as available):

- ❑ **Block known threats –** with Attack surface reduction rules, tamper protection, and block at first site
- ❑ **Apply Security Baselines -** to harden internet-facing Windows Servers, Windows Clients, and Office Applications
- ❑ **Maintain Software –** to avoid missing/neglecting manufacturer protections
  - ❑ **Updated -** Rapidly deploy critical security updates for OS, browser, & email
  - ❑ **Supported –** Update operating systems and software to currently support versions

  Isolate, disable, or retire insecure systems and protocols – including unsupported operating systems and legacy protocols
- ❑ **Block unexpected traffic –** using host-based firewall and network defenses
- ❑ **Audit and Monitor –** to find and fix deviations from baseline and potential attacks (see *Detection and Response Plan*)

Who
Assign Accountability

Executive Sponsor (Maintenance) - Business Leadership accountable for business impact of both downtime and attack damage
Executive Sponsor (Others) - *Central IT Operations or CIO*
Project Leadership - Central IT Infrastructure Team
IT + Security Architecture – Prioritize components +integrate into architecture
Central IT Operations – Implement changes to environment
Cloud Productivity / End User Team – Enable attack surface reduction
Workload/App Owners – Identify maintenance windows for changes
Security Policy and Standards – Update standards and policy documents
Security Compliance Management – Monitor to ensure compliance

Enter Names for the Team
Sponsor - Jane Smith
Lead – John Doe

Measure
Key Results

% of endpoints meeting security standards

When
To Complete

Typically within 30-60 days

##-##-2021

Remote Access Security Plan

RDP, VPN, VDI, etc.

★	**What** Objective	**Follow zero trust security best practices for remote access solutions to internal organizational resources**
?	**Why** Importance and benefits	Attackers frequently use the organization's remote access solutions for the initial entry into the environment and for ongoing operations to damage internal resources.

⚙	**How**
	Implementation Instructions
		❑ **Maintain Software/Appliance –** to avoid missing/neglecting manufacturer protections (security updates, supported status)
		❑ **Configure Azure AD** – for existing remote access, including enforcing zero trust user + device validation with Conditional Access (so that infected remote machines and compromised user accounts cannot communicate with the corporate network)
		  ❑ **Existing 3rd party VPN –** 3rd party VPNs (Cisco AnyConnect, Palo Alto Networks GlobalProtect & Captive Portal, Fortinet FortiGate SSL VPN, Citrix NetScaler, Zscaler Private Access (ZPA), and more)
		  ❑ **Azure VPN gateway**
		❑ **Publish Remote Desktop** with Azure Active Directory Application Proxy
		❑ **Move Beyond VPN** by publishing apps with Azure AD Application Proxy
		❑ **Secure Access to Azure resources -** using Azure Bastion
		❑ **Audit and Monitor –** to find and fix deviations from baseline and potential attacks (see *Detection and Response Plan*)

👥	**Who** Assign Accountability	**Executive Sponsor –** *CIO or CISO* **Project Leadership -** Central IT Infrastructure/Network Team **IT + Security Architecture –** Prioritize components +integrate into architectures **Central IT Identity Team** – Configure Azure AD and conditional access policies **Central IT Operations** – Implement changes to environment **Workload Owners** – Assist with RBAC permissions for app publishing **Security Policy and Standards –** Update standards and policy documents **Security Compliance Management** – Monitor to ensure compliance **User Education Team** – update any guidance on workflow changes

Enter Names for the Team
Sponsor - Jane Smith
Lead – John Doe

📶	**Measure** Key Results	**% of remote access connections using zero trust validation** **% of applications published to internet** **# of VPN connections per month (target is zero)**	📅	**When** To Complete	**Typically within 30-60 days**	**##-##-2021**

Account Protection Plan

Passwordless / Multi-Factor Authentication, Password Security, Detection, and more

What
Desired Outcome

Starting with critical impact admins, rigorously follow best practices for account security including using passwordless or multi-factor authentication (MFA).

Why
Importance and benefits

Just as antique 'skeleton keys' won't protect a house against a modern-day burglar, passwords cannot protect accounts against common attacks we see today. While MFA was once a burdensome extra step, Passwordless approaches today improve the logon experience using biometric approaches that don't require you to remember or type a password. Additionally, zero trust approaches remember trusted devices, which reduce prompting for annoying out of band MFA actions.

How
Implementation Instructions

- ❑ **Enforce Strong MFA or Passwordless logon –** for all users starting with administrators using one or more of:
  - **Passwordless Authentication** with Windows Hello or Authenticator App
  - **Azure Multi-Factor Authentication (MFA)**
  - **Third-party MFA** solution
- ❑ **Increase password security**
  - ❑ **Azure AD Accounts** – Use Azure AD Identity Protection to prevent and detect attacks and extend blocking of known weak passwords to on-premises Active Directory.
  - ❑ **On-Premises AD** - Extend Azure AD Password Protection to on-premises active directory
- ❑ **Audit and Monitor –** to find and fix deviations from baseline and potential attacks (see *Detection and Response Plan*)

Who
Assign Accountability

Executive Sponsor - CISO, CIO, or Identity Director
Lead: Identity and Key Management and/or Security Architecture.

- **IT and Security Architects –** Prioritize components integrate into architectures
- **Identity and Key Management or Central IT Operations** to implement change
- **User Education Team** – update any password guidance
- **Security Policy and Standards –** Update standards and policy documents
- **Security Compliance Management** – Monitor to ensure compliance

Enter Names for the Team
Sponsor - Jane Smith
Lead – John Doe

Measure
Key Results

100% of employees actively using MFA
100% deployment of password security

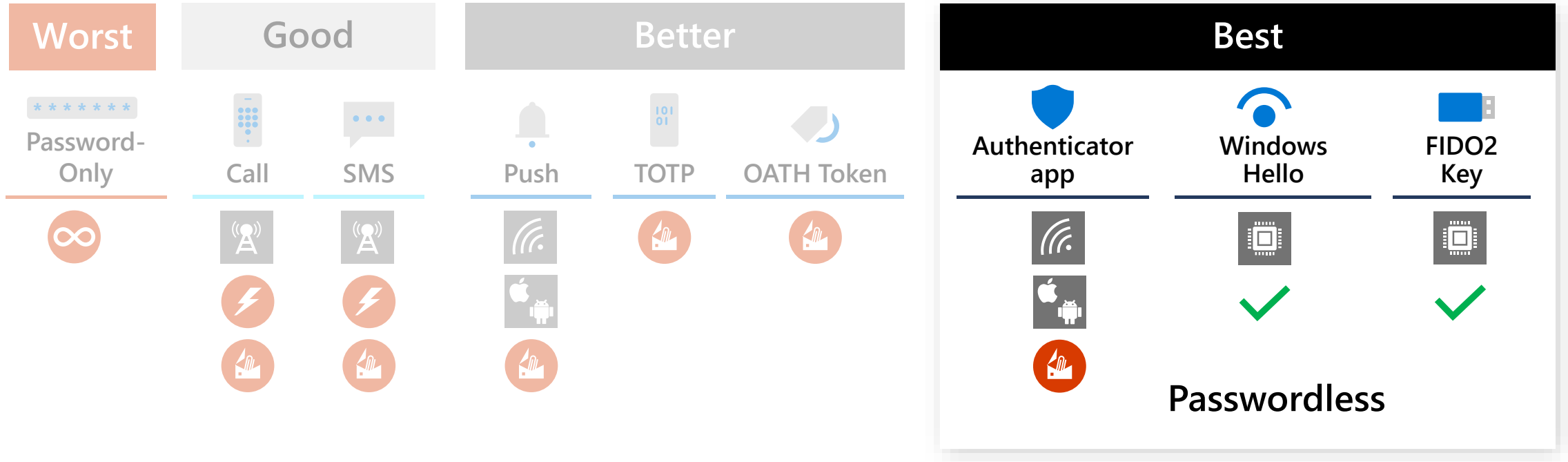
When
To Complete

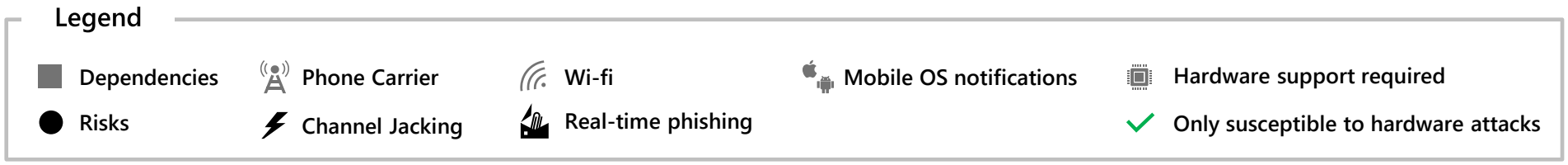
Typically within 30 days

##-##-2021

Strong Multi-Factor Authentication

The best options aren't that difficult





Privileged Access Plan

Strong protection for administrative rights and business critical users

★	**What** Objective	**Implement a comprehensive strategy to reduce risk of privileged access compromise**
?	**Why** Importance and benefits	All other security controls can easily be invalidated by an attacker with privileged access in your environment. Ransomware attack operators use privileged access as a quick path to control all critical assets in the organization for their extortion.
⚙	**How** Implementation Instructions	Build a multi-part strategy using the guidance at https://aka.ms/SPA including: ❑ **A. Enforce End-to-end Session Security –** to explicitly validate trust of users and workstations before allowing access to administrative interfaces (using Azure AD Conditional Access). ❑ **B. Protect & Monitor Identity Systems** against privilege escalation attacks including Directories, Identity Management, Admin Accounts and groups, Consent grant configuration. ❑ **C. Mitigate Lateral Traversal** to ensure that compromising a single device will not immediately lead to control of many or all other devices using local account passwords, service account passwords, or other secrets ❑ **D. Ensure Rapid Threat Response** to limit adversary access and time in the environment. See *Detection and Response Plan* for more
👥	**Who** Assign Accountability	**Executive Sponsor** - This is typically sponsored by CISO and CIO **Lead:** Security Architect(s) • **IT and Security Architects –** Prioritize components integrate into architectures • **Identity and Key Management** to implement identity changes • **Central IT Productivity / End User Team** – Implement changes to Devices and Office 365 tenant • **Policy and standards team** establish clear requirements • **User Education Team** – update any password guidance • **Security Policy and Standards –** Update standards and policy documents • **Security Compliance Management** – Monitor to ensure compliance

Enter Names for the Team
Sponsor - Jane Smith
Lead – John Doe

📶	**Measure** Key Results	• **100% of admins required to use secure workstations** • **100% local workstation/server passwords randomized** • **100% deployment of privilege escalation mitigations**	📅	**When** To Complete	**Multiple deliverables spanning 30-90 days** **##-##-2021**

Ransomware Data Protection Plan

What
Objective

Implement data protection to ensure rapid and reliable recovery from a ransomware attack + block some techniques

Why
Importance and benefits

Ransomware extortion (and destructive attacks) only work when all legitimate access to data and systems is lost. Ensuring that attackers cannot remove your ability to resume operations without payment will protect your business and undermine the monetary incentive for attacking your organization.

How
Implementation Instructions

- ❑ **Migrate to cloud -** move user data to cloud solutions like OneDrive/SharePoint to take advantage of versioning and recycle bin capabilities. Educate users on how to recover their files by themselves to reduce delays and cost of recovery.
- ❑ **Designate Protected Folders** – to make it more difficult for unauthorized applications to modify the data in these folders.
- ❑ **Review Permissions –** to reduce risk from broad access enabling ransomware
  - ❑ **Discover broad write/delete permissions** on fileshares, SharePoint, and other solutions
    Broad is defined as many users having write/delete to business-critical data
  - ❑ **Reduce broad permissions** while meeting business collaboration requirements
  - ❑ **Audit and monitor** to ensure broad permissions don't reappear

Who
Assign Accountability

Sponsorship - *Central IT Operations or CIO*
Project Leadership - Data Security Team
Central IT Productivity / End User Team – Implement changes to Microsoft 365 tenant for OneDrive / Protected Folders
Business / Application Teams - Identify business critical assets
Security Policy and Standards – Update data protection standards and policy
Security Compliance Management – Monitor to ensure compliance
User Education Team – Ensure guidance for users reflects policy updates
Security Architecture – Review security configuration for cloud migration

Enter Names for the Team
Sponsor - Jane Smith
Lead – John Doe

Measure
Key Results

- **% of users with data protection solutions**
- **% of devices with data protection solutions**

When
To Complete

Typically within 30-90 days

##-##-2021

Secure Backup Plan

What
Desired Outcome

Ensure critical systems are backed up and backups are protected against deliberate attacker erasure/encryption.

Why
Importance and benefits

These attacks focus on crippling your organization's ability to respond without paying, frequently targeting backups and key documentation required for recovery (e.g. SolarWinds diagrams) to force organizations into paying extortion demands. Most organizations don't protect backup and restoration procedures against this level of intentional targeting.

Note: This preparation also improves resilience to natural disasters and rapid attacks like WannaCry & (Not)Petya

How
Implementation Instructions

- ❑ **Backup** all critical systems automatically on a regular schedule
- ❑ **Ensure Rapid Recovery** of business operations by regularly exercising business continuity / disaster recovery (BC/DR) plan
- ❑ **Protect backups** against deliberate erasure and encryption
  - ❑ **Strong Protection –** Require out of band steps (MFA or PIN) before modifying online backups (e.g. Azure Backup)
  - ❑ **Strongest Protection –** Store backups in online immutable storage (Azure Blob info) and/or fully offline/off-site
- ❑ **Protect supporting documents** required for recovery such as restoration procedure documents, CMDB, and network diagrams

Who
Assign Accountability

Sponsorship - Central IT Operations CIO
Project Leadership - Central IT Infrastructure Team
Business / Application Teams - Identify Business Critical Assets
Central IT Infrastructure/Backup Team– Enable Infrastructure backup
Central IT Productivity / End User Team – Enable OneDrive Backup
Security Policy and Standards – Update standards and policy documents
Security Compliance Management – Monitor to ensure compliance
Security Architecture – Advise on configuration and standards

Enter Names for the Team
Sponsor - Jane Smith
Lead – John Doe

Measure
Key Results

Mean Time to Recover (MTTR) meets BC/DR goal
Measured during exercise and real-world operations

When
To Complete

Typically within 30 days

00-00-2021

Detection and Response Plan

Rapid eviction to mitigate risk

What Objective	**Ensure rapid detection and remediation of common attacks on endpoint, email, and identity**
Why Importance and benefits	***Minutes matter.*** Rapidly remediating common attack entry points to limit attacker's time to laterally traverse & do damage.

How
Implementation Instructions
	❑ **Prioritize Common Entry Points –** Ransomware (and other) operators favor Endpoint/Email/Identity + RDP
	  ❑ **Integrated XDR** - Use integrated Extended Detection and Response (XDR) tools like Microsoft 365 Defender to provide high quality alerts and minimize friction and manual steps during response
	  ❑ **Brute Force** - Monitor for brute-force attempts like password spray
	❑ **Monitor for Adversary Disabling Security –** as this is often part of HumOR attack chain
	  ❑ **Event Logs Clearing –** especially the Security Event log and PowerShell Operational logs
	  ❑ **Disabling of security tools**/controls (associated with some groups)
	❑ **Don't Ignore Commodity Malware -** Ransomware attackers regularly purchase access to target organizations from dark markets
	❑ **Integrate outside experts** – into processes to supplement expertise, such as Microsoft Detection and Response Team (DART)
	❑ **Rapidly isolate** compromised computers using Defender for Endpoint

Who Assign Accountability	**Sponsorship –** CISO **Project Leadership - Security Operations** Central IT **Infrastructure Team** – Implement client and server agents/features Security Operations – integrate any new tools into security operations processes Central IT **Productivity / End User Team** – Enable features for Defender for Endpoints, Defender for O365, Defender for Identity, and Cloud App Security Central IT **Identity Team** – Implement Azure AD security + Defender for Identity Security Policy and Standards **–** Update standards and policy documents Security Compliance Management – Monitor to ensure compliance Security Architecture – Advise on configuration, standards, and tooling

Enter Names for the Team
Sponsor - Jane Smith
Lead – John Doe

Measure Key Results	**Mean Time to Acknowledge (MTTA) Alerts** **Mean Time to Remediate (MTTR) Incidents**	**When** To Complete	**Typically within 30 days**	**##-##-2021**

Security Posture and Governance Plan

Sustain and increase improvements, ensure asset coverage

What
Objective

Actively discover and continuously improve the security posture of your environment

Why
Importance and benefits

Ransomware and other attackers are continuously looking for ways to monetize weaknesses in your security posture. Staying secure requires visibility to find and address these weaknesses (and validate that the mitigations have been implemented successfully)

How
Implementation Instructions

Sustaining and improving your security requires you to

- ❑ **Assign Responsibilities** – to ensure clear accountability for monitoring risk and remediating it by asset owners (see Microsoft recommendations on accountabilities)
- ❑ **Assess and Measure** security posture using Microsoft Secure Score
- ❑ **Apply recommended improvement** actions, guidance, and control
- ❑ **Audit and Monitor** resources for compliance using
  - ❑ Azure Security Center (ASC) Secure score and regulatory compliance dashboard
  - ❑ Microsoft Secure Score
  - ❑ Compliance manager

Who
Assign Accountability

Sponsorship – CISO
Project Leadership - Posture Management
IT + Security Architects – Prioritize components + integrate into architectures
IT or DevOps Resource Owners – Remediate security risks in their resources
Cloud Team / Central IT Infrastructure Team – grant permissions to security team. Configure/Deploy Azure Arc for on-prem, AWS, GCP, other clouds
Security Policy and Standards – identify which elements to audit and enforce
Security Compliance Management – Monitor to ensure compliance

Enter Names for the Team
Sponsor - Jane Smith
Lead – John Doe

Measure
Key Results

% Secure Score improvement (month over month)
% of assets with security visibility

When
To Complete

Typically within 15-30 days

##-##-2021

Organizational Program/Processes Plan

Build muscle memory and pave the road

What
Objective

Update organizational processes to manage major ransomware events and streamline outsourcing to avoid friction.

Why
Importance and benefits

Common weaknesses in organizational process weaknesses can significantly increase security

- **Business Continuity / Disaster Recovery** often doesn't include security incidents and/or human operated ransomware scenarios
- **IT outsourcing contracts** are typically designed for cost efficiency, which creates risk by impeding the organization's ability to rapidly respond to active security incidents.

How
Implementation Instructions

- ❑ **Exercise whole-enterprise recovery plans –** to build and strengthen organizational processes and muscle memory for this scenario
- ❑ **Update IT and security outsourcing contracts** *(if applicable)* – to ensure that service level agreements (SLAs) support rapid response actions for security incidents, including
  - ❑ Time to isolate individual workstations
  - ❑ Time to remediate accounts (disable accounts, reset credentials, expire authentication tokens, and related)
  - ❑ Time to remove malicious message from all mailboxes and block/register malicious senders
  - ❑ Time to fully remediate workstations (IT provided elements of removing malware and/or rebuild/reinstall)
  - ❑ Time to block malicious sites
  - ❑ Time to remove malware from cloud services, servers, fileshares, and sharepoint

Who
Assign Accountability

Sponsorship (Incident Preparation) – Business or Risk Leadership
Project Leadership – CISO
Legal, Security, Communications – Participate in building and validating process
Security Operations **and** **Architects**- Advise on scenarios and plans

Sponsorship (Outsourcing Contract) – Chief Financial Officer (CFO)
Project Leadership – Procurement leads and executes on changes
CISO and CIO Provide requirements, consulting, and advisory

Enter Names for the Team(s)
Sponsor - Jane Smith
Lead – John Doe

Measure
Key Results

- **Mean Time to Recover** (Whole enterprise)
- **Outsourced Service Provider SLAs** meet 100% of org requirements

When
To Complete

Typically within 15-30 days

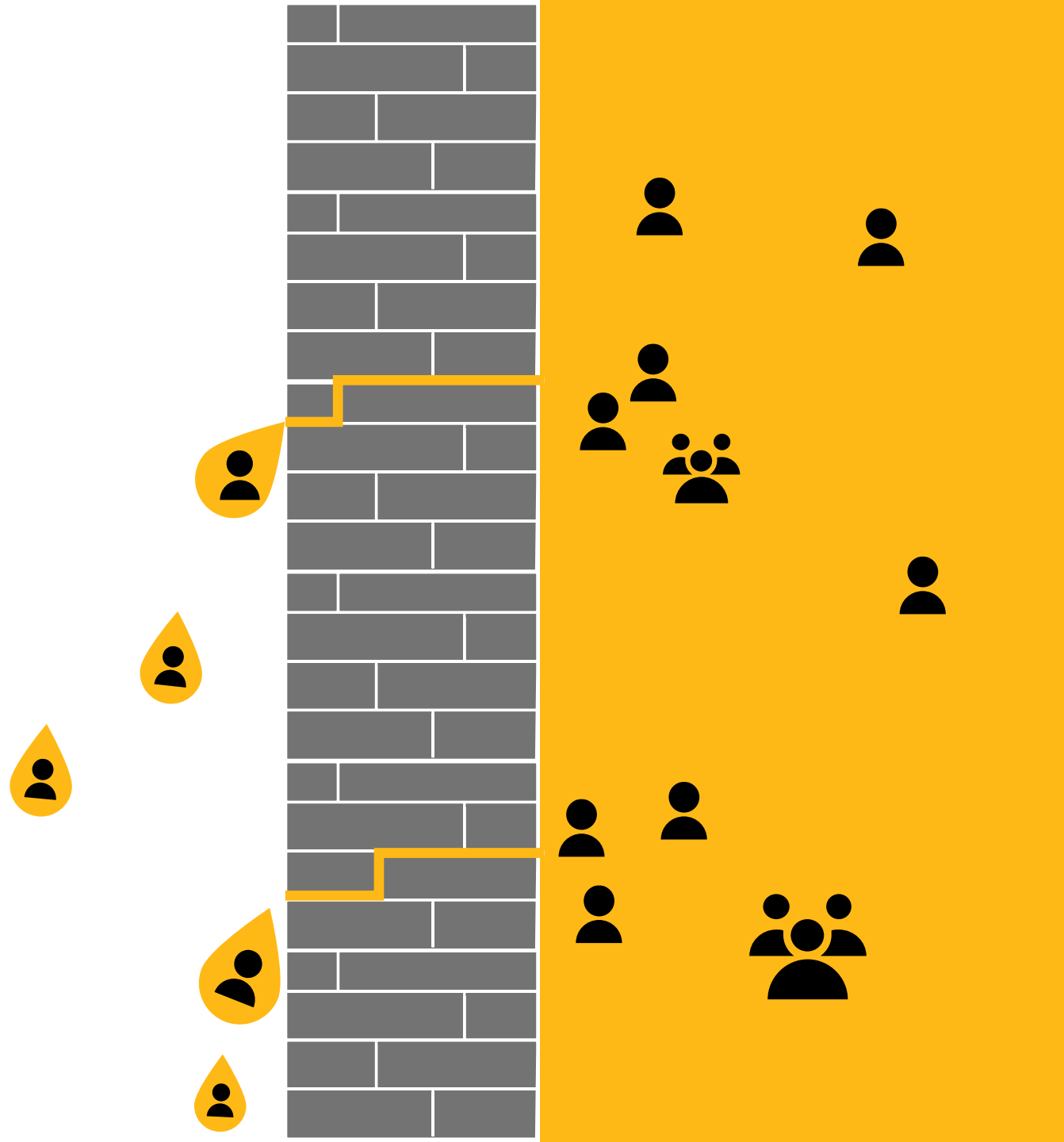
##-##-2021

Attackers are like water

Attackers take path of least resistance to achieve objectives

- Established paths/methods
- Easiest new openings

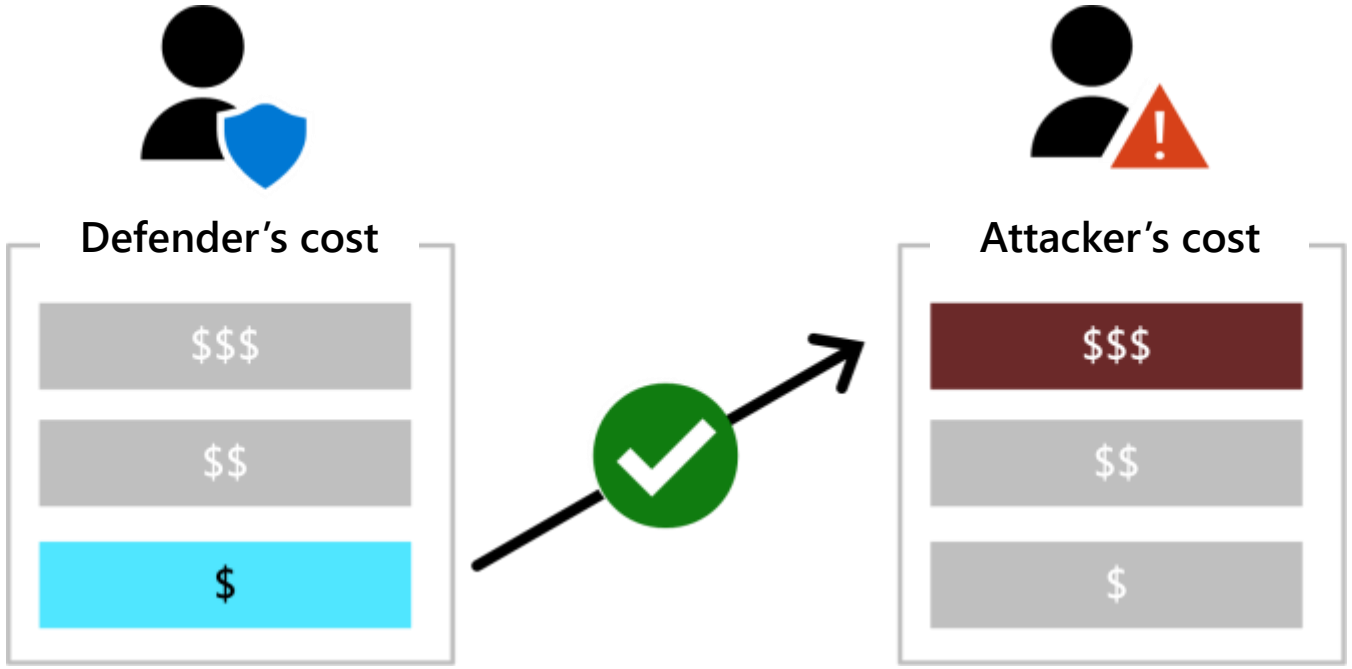
Attackers only bother when they get good ***return on investment (ROI)***



Security goal – Disrupt Attackers

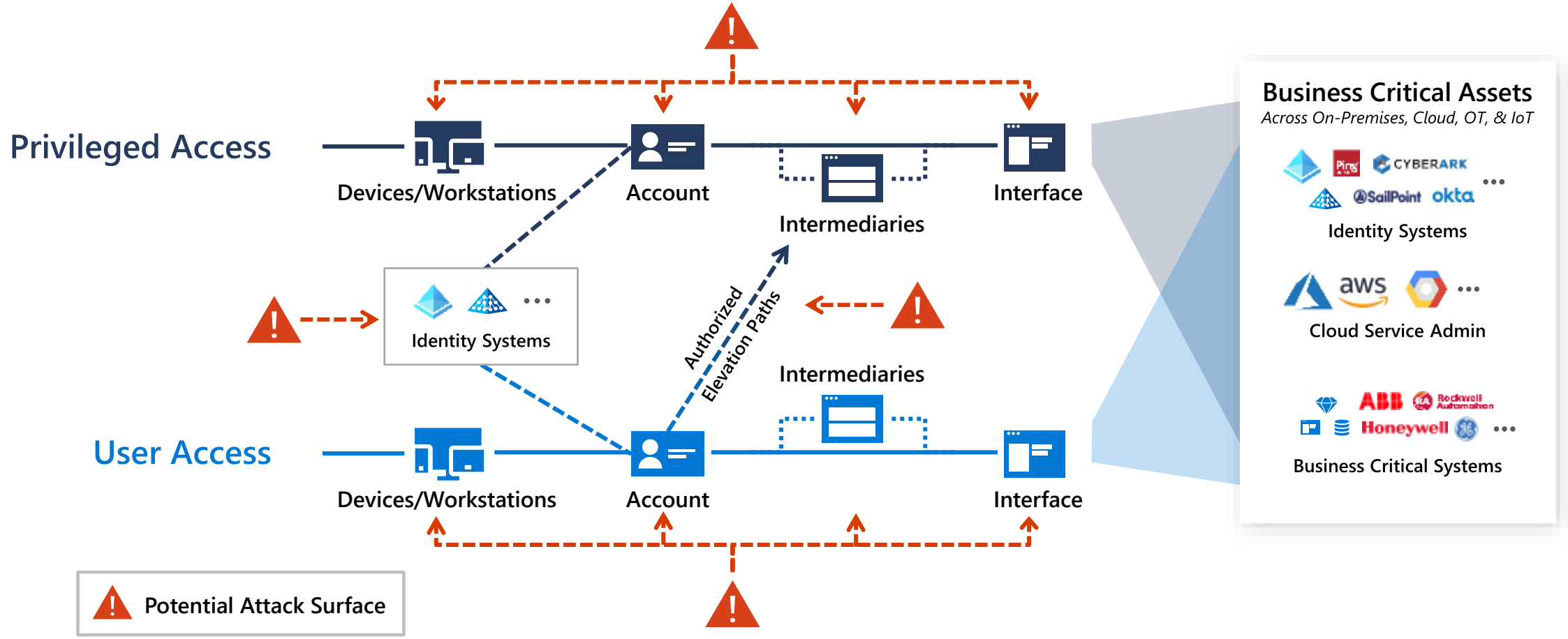
Slow (or occasionally stop) attackers by disrupting return on investment (ROI)

Seek efficient means to disrupt attacks
Increase attacker costs with the least amount of resource investment



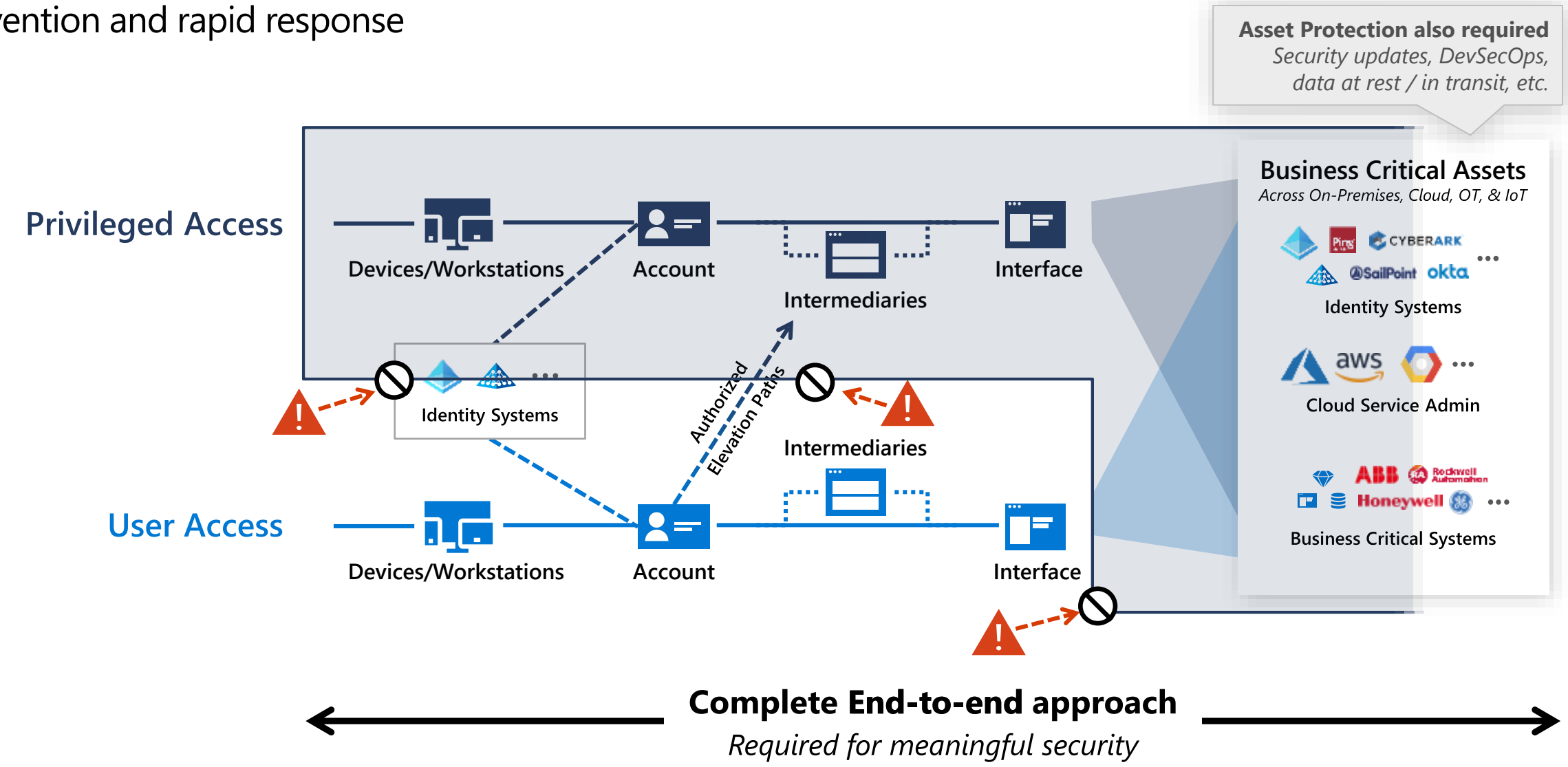
Attackers have options

to compromise privileged access



Limit and protect pathways to privileged access

Prevention and rapid response



Achieve goal with complementary initiatives

A. End-to-end Session Security

Explicit Zero Trust validation for

- ***Privileged Sessions***
  (including authorized elevation)
- ***User Sessions***

B. Protect & Monitor Identity Systems

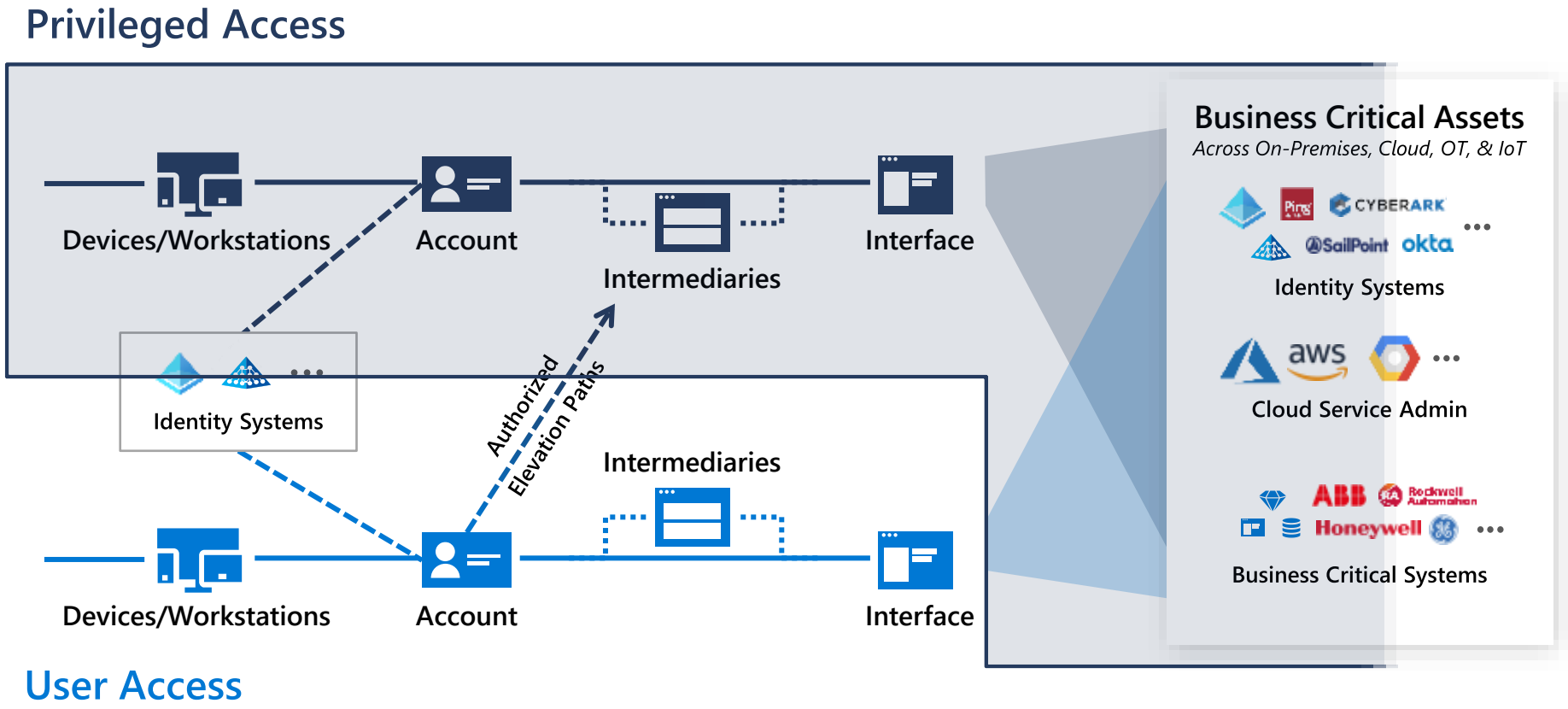
Secure Directories, Identity Management, Admin Accounts, Consent grants, and more

C. Mitigate Lateral Traversal

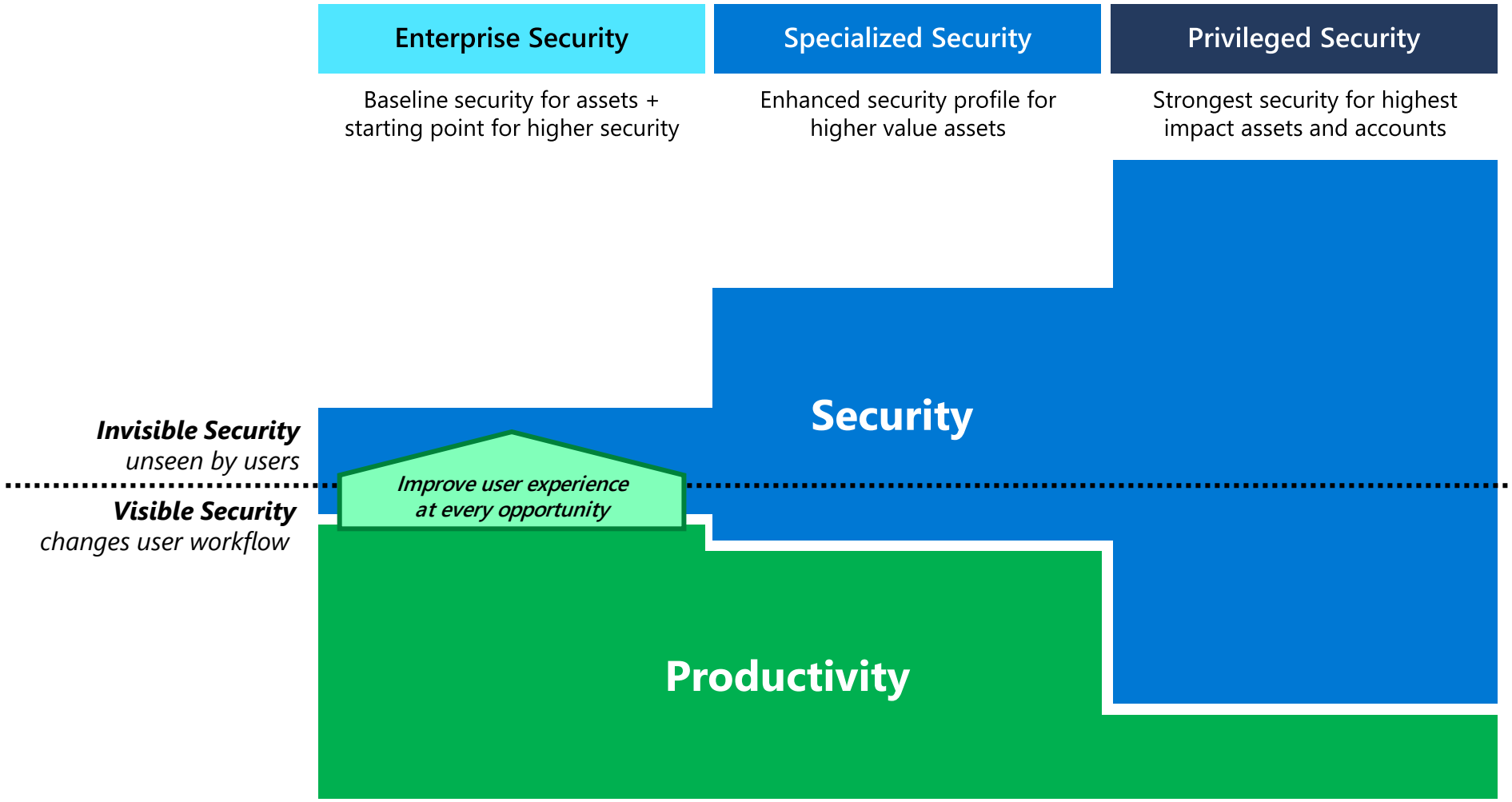
Using Local Accounts

D. Rapid Threat Response

Limit adversary access and time

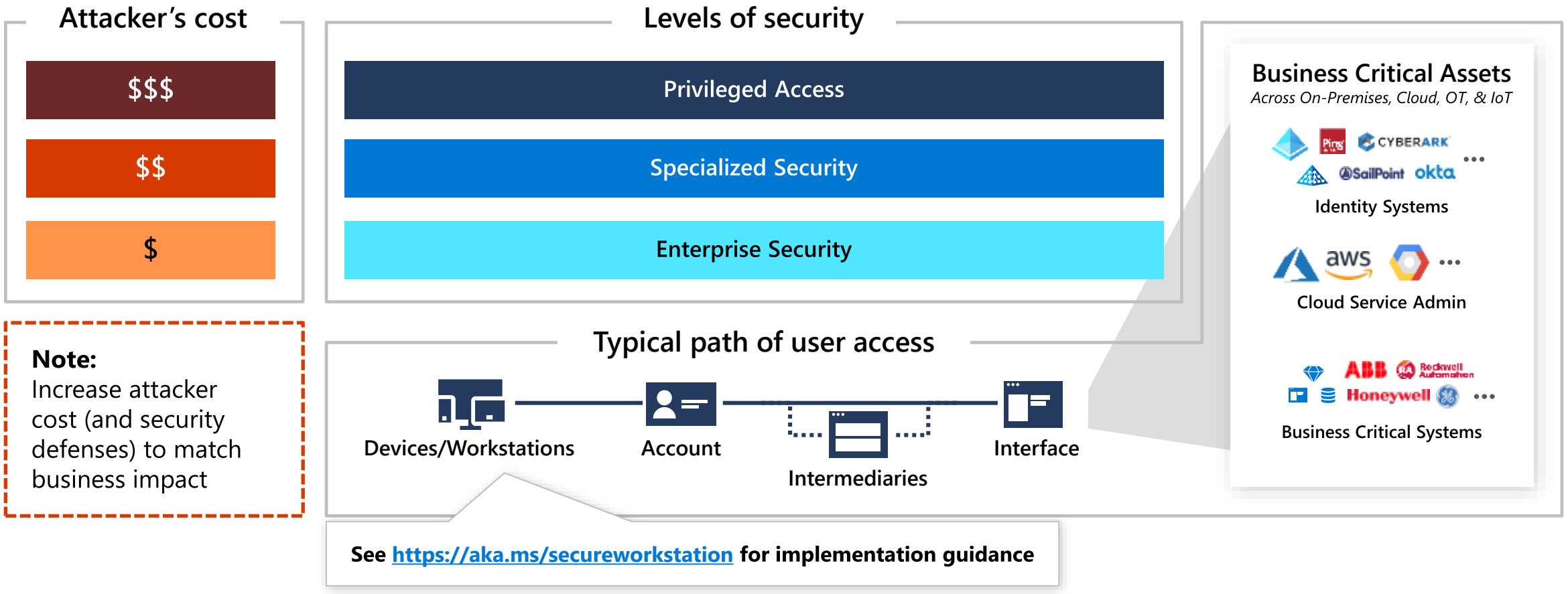


Security *and* Productivity

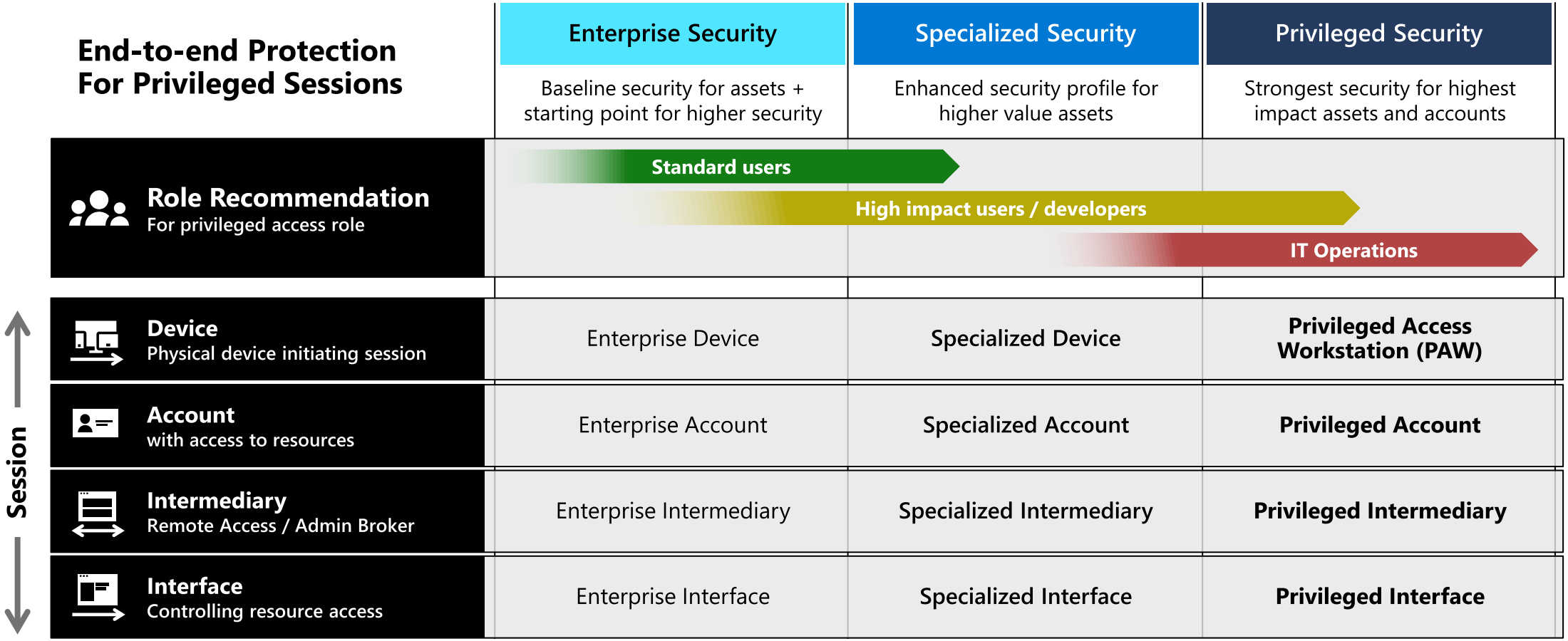


End-to-end approach to security

Increase the attacker's cost to gain access and reach business critical assets



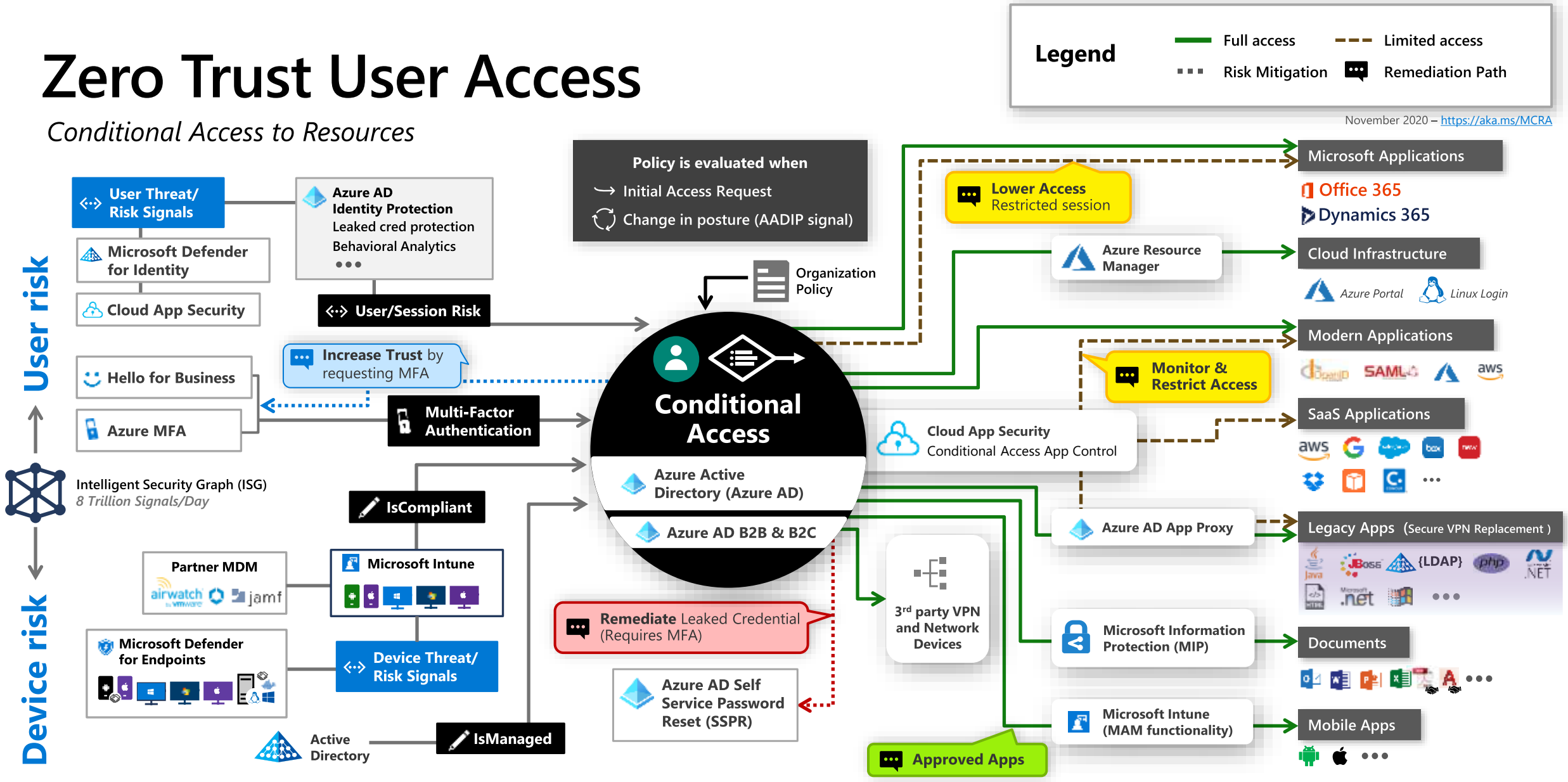
Security level drill down



- Guidelines apply to privileged access of all resources on-premises and in the cloud resources
- Cloud provides management and security for all privileged assets (when possible)

Zero Trust User Access

Conditional Access to Resources



Signal
to make an informed decision

Decision
based on organizational policy

Enforcement
of policy across resources

Ransomware Protection: Windows Platform Protections

Pre-breach → **Post-breach**

Off machine

Office 365 (Email)

- Reducing email attack vector
- Advanced sandbox detonation

Edge (Browser)

- Browser hardening
- Reduce script-based attack surface
- App container hardening
- Reputation based blocking for downloads
- SmartScreen

On machine

Locked Down Devices

- Windows 10S
- Application Control
- Credential Guard
- VSM

Attack Surface Reduction Rules

- Configurable attack surface

App Guard (Virtualized Security)

- App isolation

Controlled Folder Access

- Only allowed apps can alter user data

Exploit Protection

- Block specific Exploit Techniques

Network Protection

- Device level network filtering

Microsoft Defender for Endpoint / Pre breach (AV)

- Improved ML and heuristic protection
- Instantly protected with the cloud
- Enhanced Exploit Kit Detections

Microsoft Defender for Endpoint / Pre breach Behavioral Engine (Behavior Analysis)

- Enhanced behavioral and machine learning detection
- Memory scanning capabilities

Microsoft Defender for Endpoint / Post breach (Behavior Analysis)

- Process tree visualizations
- Artifact hunting capabilities
- Machine Isolation
- Automated incident response playbooks

Off machine

OneDrive (Cloud Storage)

- Reliable versioned file storage in the cloud
- Point in time file recovery

Attack surface Reduction (ASR)

Mapping rules to Human Operated Ransomware (HumOR)

[Use attack surface reduction rules to prevent malware infection]