RSAConference2019
San Francisco | March 4 – 8 | Moscone Center

SESSION ID: TECH-F03

Passwords and Patching: The Forgotten Building Blocks of Enterprise Security

Andrea Fisher

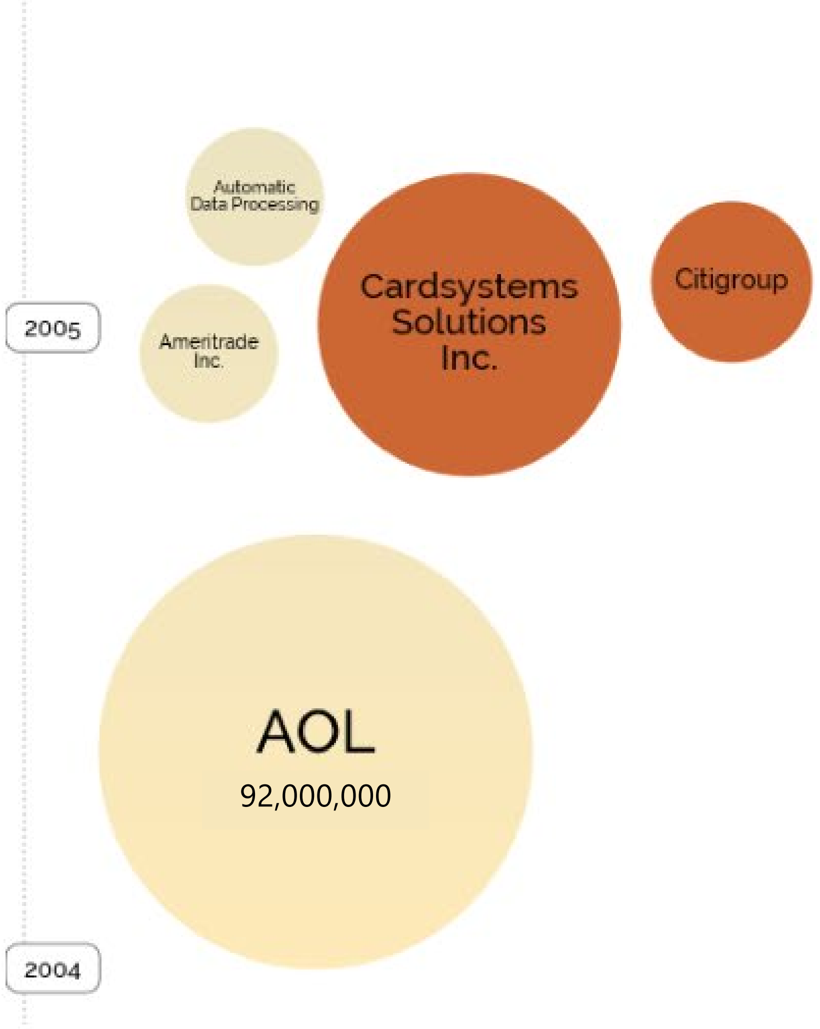
Security Specialist
Microsoft
@andreatfisher

Jon Wojan

Cloud Technical Architect
Microsoft
http://www.linkedin.com/in/wojan
@wojan

#RSAC

Brief History of Breaches



The problem with passwords…

Azure Active Directory

Bro

Over 85% of attacks come from people getting tricked out of their passwords.

problem

Password Demo: How big is the problem?

What can we do?

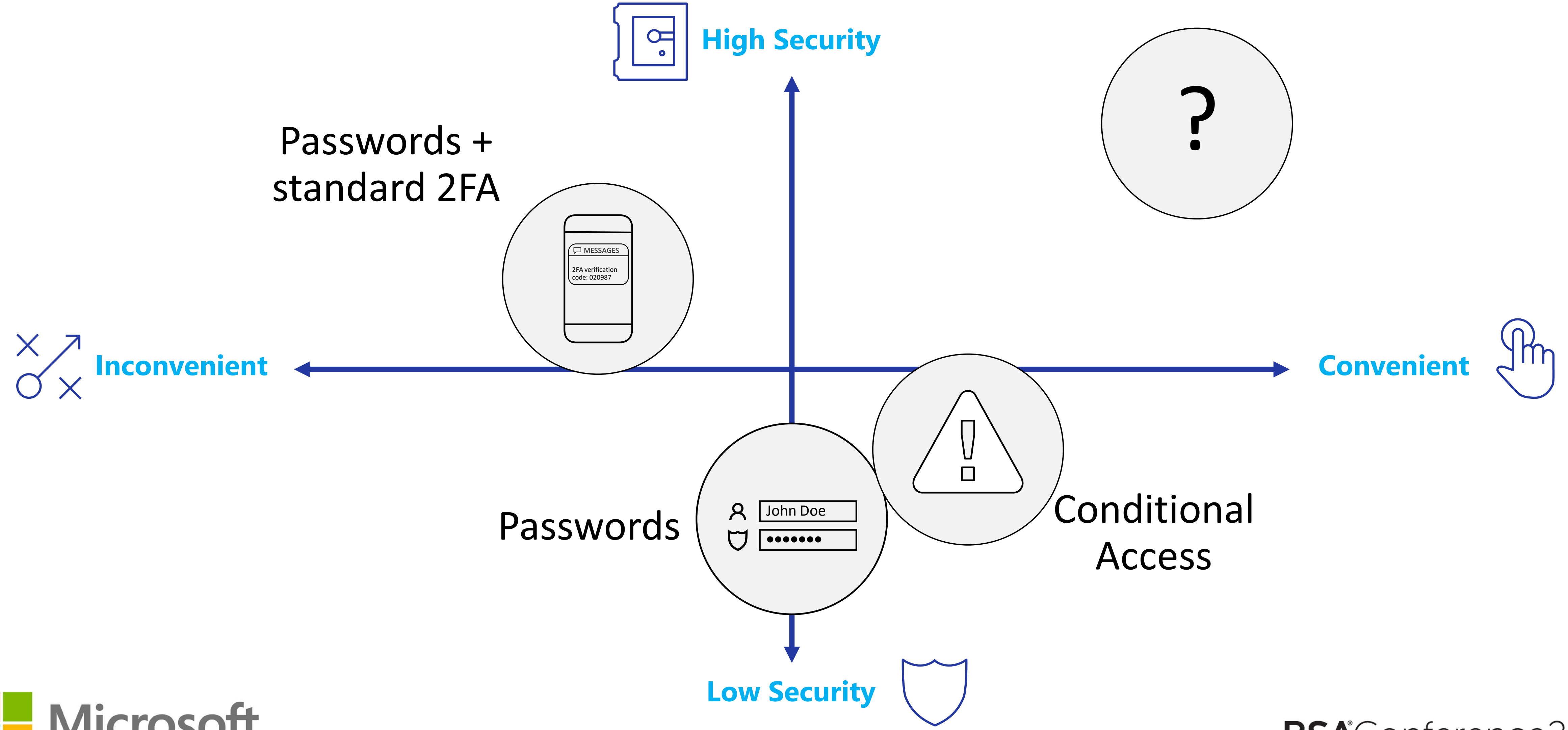
Replace the password

The Dream…

End-users should never have to deal with passwords in their day-to-day lives

User credentials will improve so that they cannot be cracked, breached, or phished

The search for better



User acceptance to non-traditional authentication

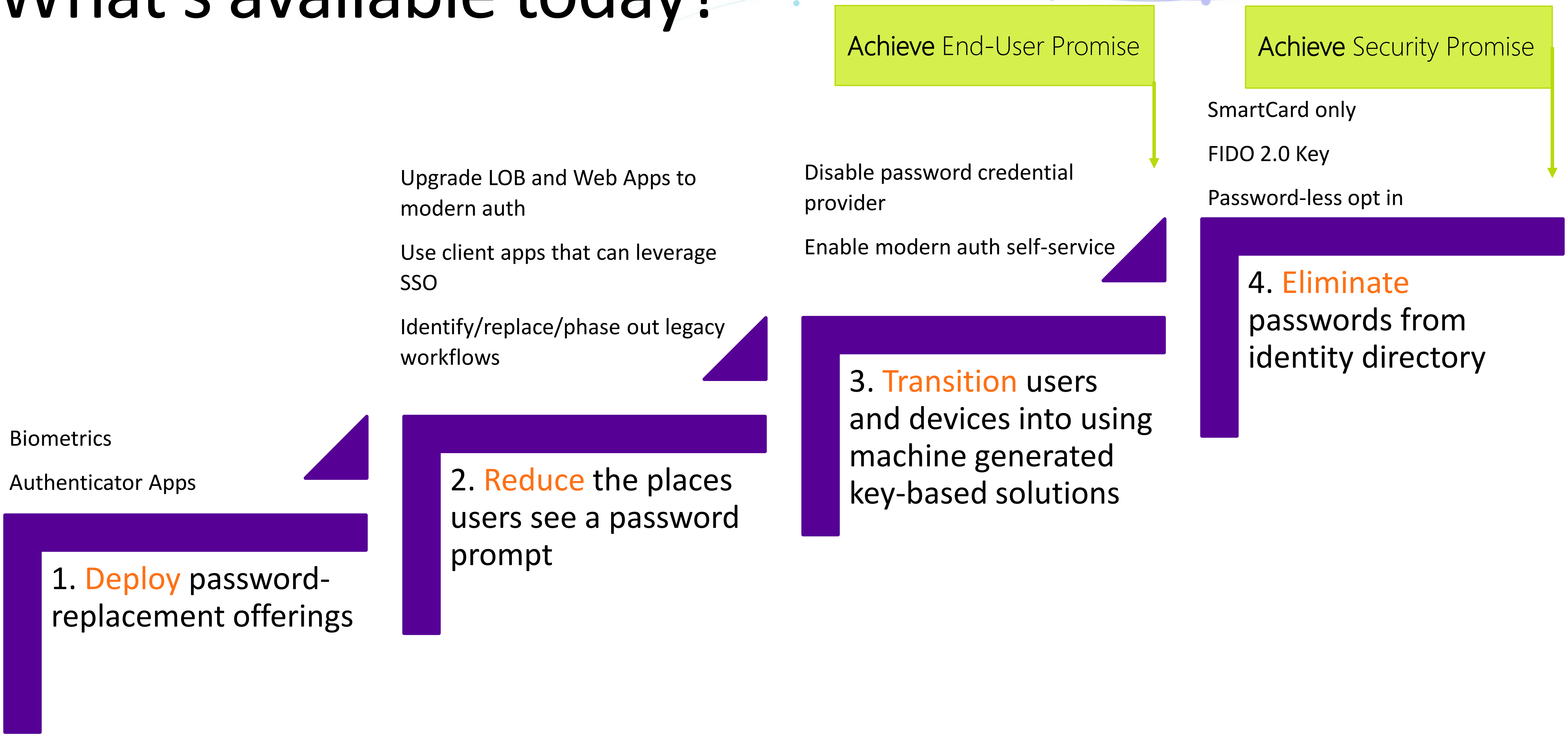
	Not welcomed	Welcomed	Welcomed completely	Neither
Biometric Verification	**15%**	**30%**	**32%**	23%
Conditional Access	**21%**	**23%**	**27%**	30%
Multifactor	**27%**	**19%**	**21%**	32%

62% of respondents would welcome biometric verification
Half (50%) would welcome geolocations
40% would welcome dual device access

However, just 15% would not welcome biometric verification, 21% wouldn't welcome geolocation, and 27% wouldn't welcome multifactor– highlighting that there is relatively low resistance to their introduction

Source: Amárach Research 1/2019

What’s available today?



Biometrics

Authenticator Apps

1. Deploy password-replacement offerings

Upgrade LOB and Web Apps to modern auth

Use client apps that can leverage SSO

Identify/replace/phase out legacy workflows

2. Reduce the places users see a password prompt

Achieve End-User Promise

Disable password credential provider

Enable modern auth self-service

3. Transition users and devices into using machine generated key-based solutions

Achieve Security Promise

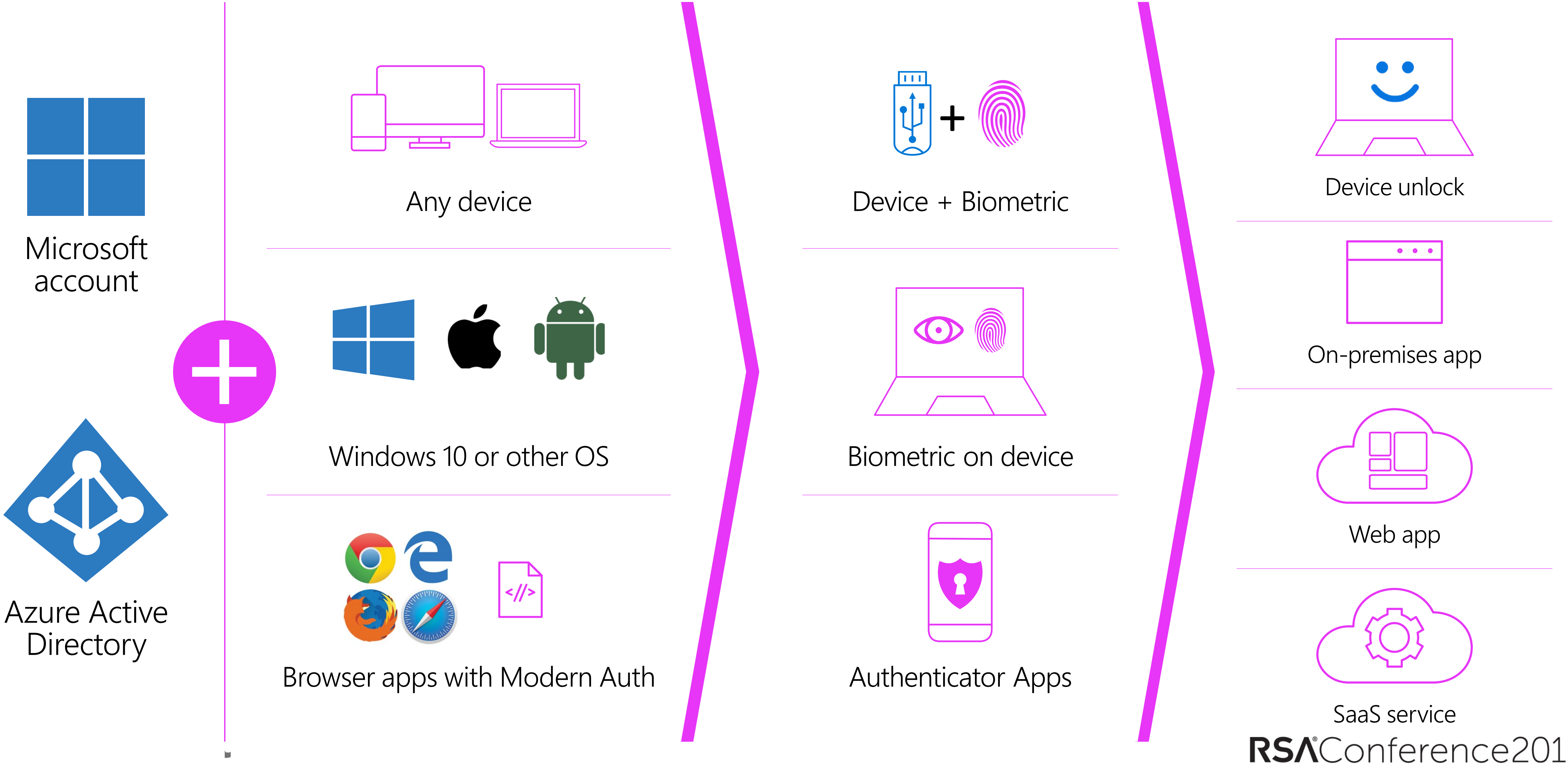
SmartCard only

FIDO 2.0 Key

Password-less opt in

4. Eliminate passwords from identity directory

The roadmap to no more passwords



Microsoft account

Azure Active Directory

Any device

Windows 10 or other OS

Browser apps with Modern Auth

Device + Biometric

Biometric on device

Authenticator Apps

Device unlock

On-premises app

Web app

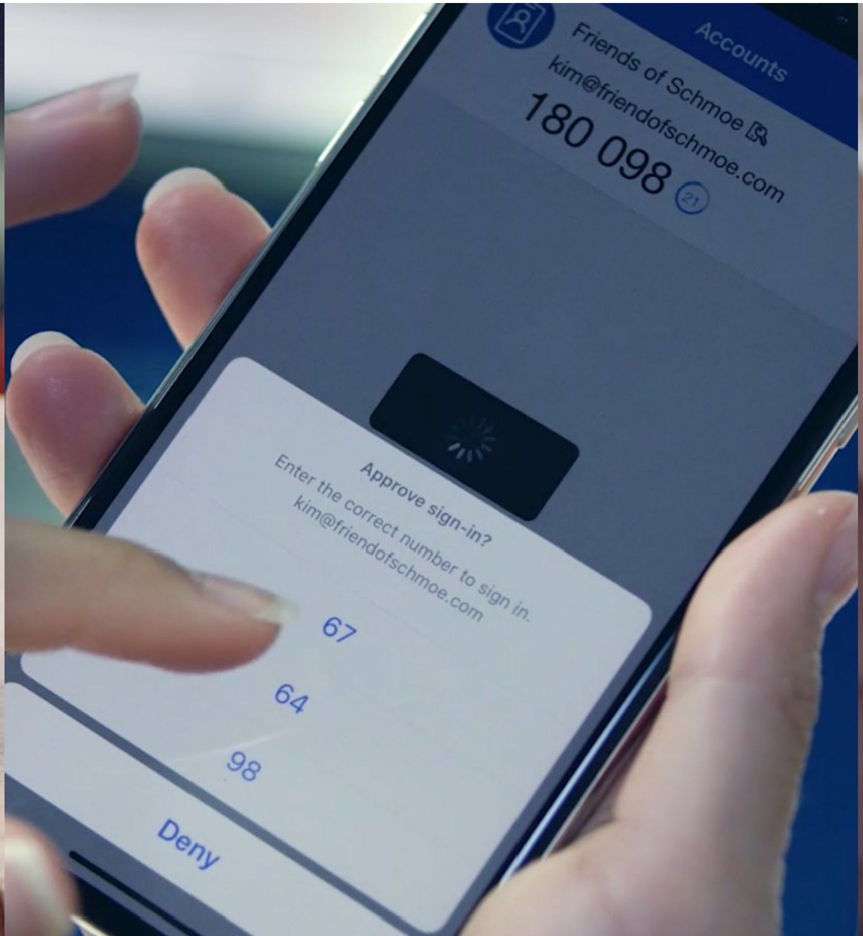
SaaS service

Getting to a world without passwords

High security, convenient methods of strong authentication

Biometric

Second Factor

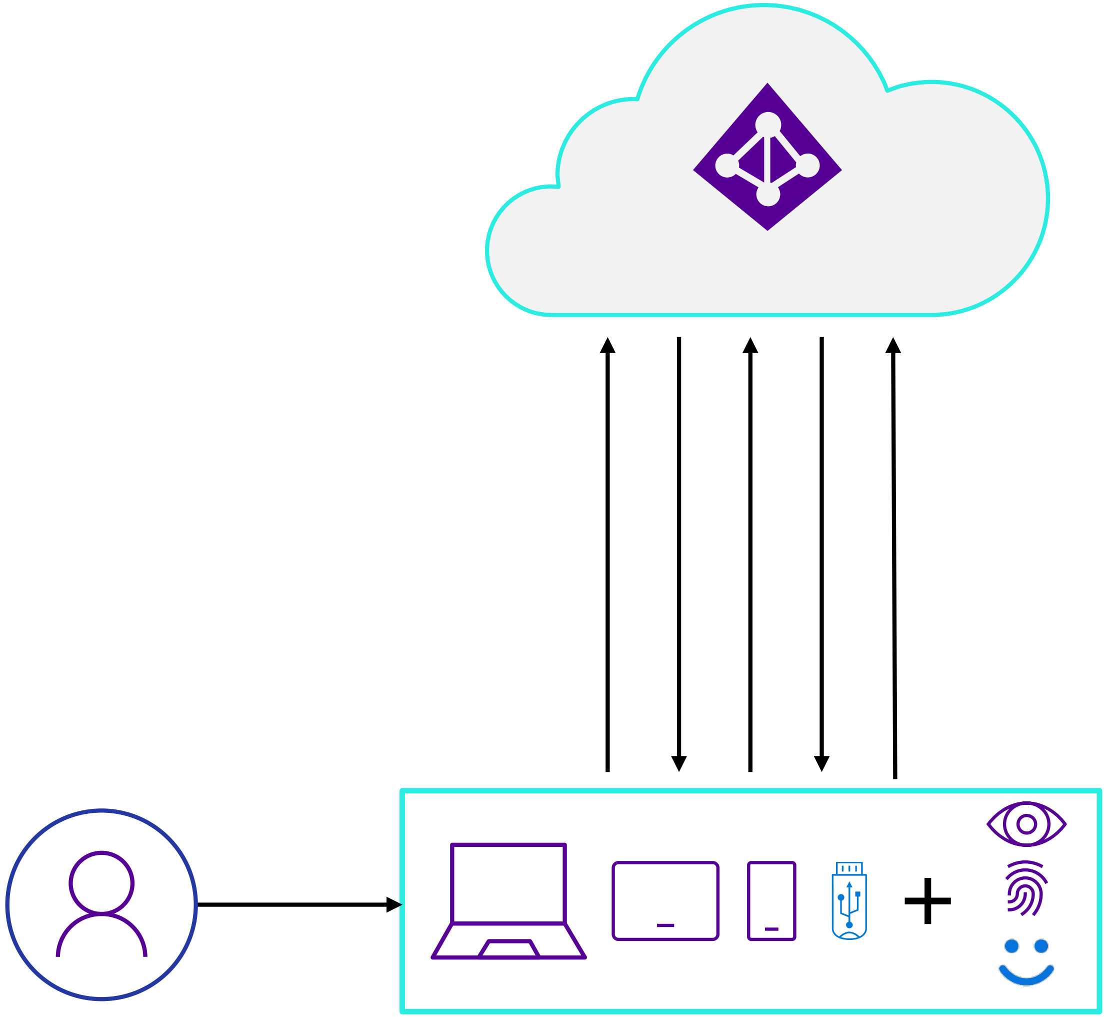


FIDO2 Security Keys

Secure Authentication Flow

A simple, common architecture

- Based on public-key technology
- Private-keys are securely stored on the device
- Requires a local gesture (e.g., biometric, PIN)
- Private-keys are bound to a single device and never shared



Next Steps

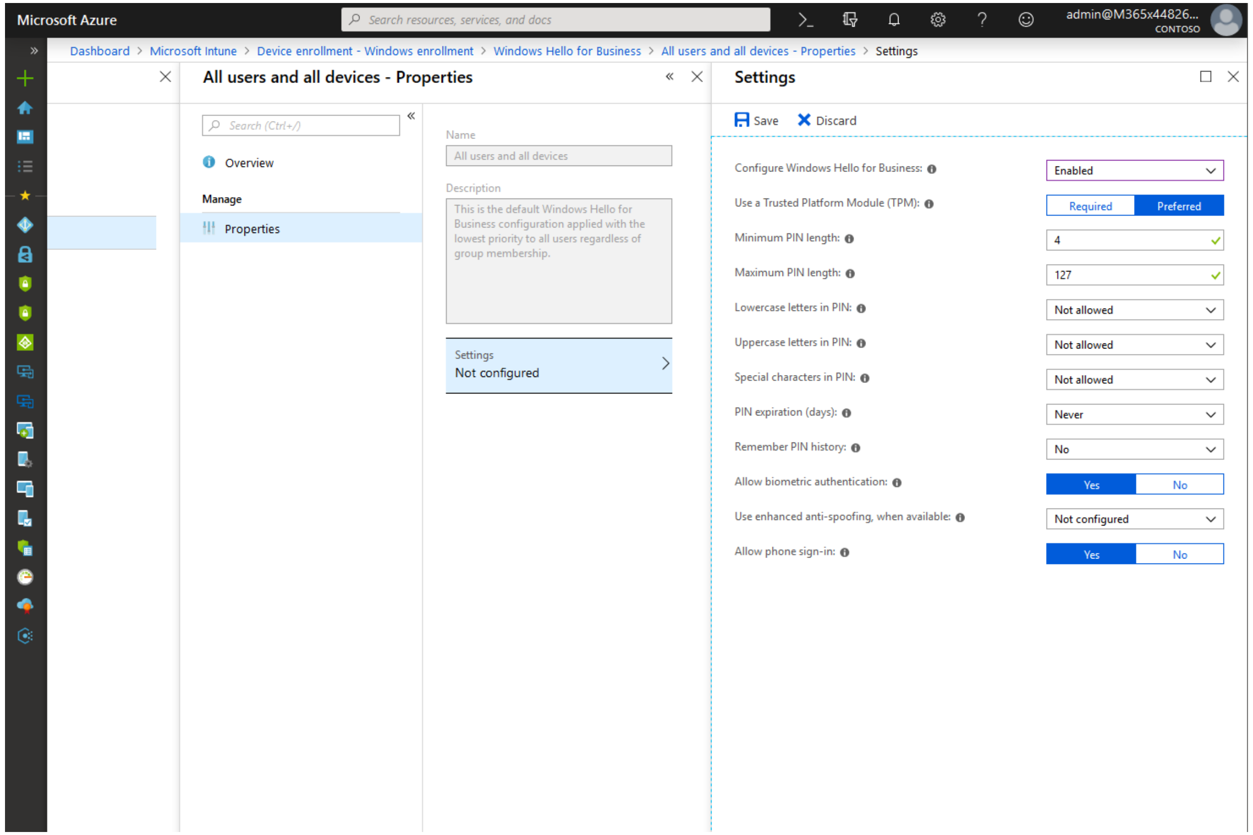
- Going password-less is a long-term strategy to reduce risk. Start with a plan.

1. Enabling Cloud based Identities (eg: Azure Active Directory)
2. Multi-Factor Authentication and Self-Service Password Reset for all users
3. Identify and update apps to allow AAD authentication
4. Start with a Pilot
   - Deploy a Windows Hello roll-out for Windows 10 users
   - Try Microsoft Authenticator phone sign-in for added mobility
   - Prepare for FIDO2 security keys with a pilot for desk-less or kiosk workers

- Try it yourself!

Enterprise enable Hello for Business

Intune (Modern Workplace Join)


Microsoft Azure
Search resources, services, and docs
admin@M365x44826...
CONTOSO
Dashboard > Microsoft Intune > Device enrollment - Windows enrollment > Windows Hello for Business > All users and all devices - Properties > Settings
All users and all devices - Properties
Search (Ctrl+/)
Overview
Manage
Properties
Settings
Save
Discard

Name: All users and all devices

Description: This is the default Windows Hello for Business configuration applied with the lowest priority to all users regardless of group membership.

Settings: Not configured

Configure Windows Hello for Business: Enabled

Use a Trusted Platform Module (TPM): Required [✓ Preferred]

Minimum PIN length: 4

Maximum PIN length: 127

Lowercase letters in PIN: Not allowed

Uppercase letters in PIN: Not allowed

Special characters in PIN: Not allowed

PIN expiration (days): Never

Remember PIN history: No

Allow biometric authentication: [✓ Yes] No

Use enhanced anti-spoofing, when available: Not configured

Allow phone sign-in: [✓ Yes] No

Federation Services (Hybrid Scenario)

1. Sign into ADFS Server as Domain Admin
2. Open a Powershell Prompt
3. Run command:

Set-AdfsCertificateAuthority -EnrollmentAgent -EnrollmentAgentCertificateTemplate WHFBEnrollmentAgent -WindowsHelloCertificateTemplate WHFBAuthentication

Demo: FIDO 2.0 Scenarios

The problem with patching…

The NSA says…

- The DOD's unclassified network hasn't been targeted with a 0day attack in two years
- Network defenses aren’t robust enough to make attackers rely on 0day exploits. It’s easier to exploit systems that are "not compliant with hardware and software best practices.”

Gartner says…

- The exploitation of known, but unmitigated, vulnerabilities is the primary method of compromise for most threats. Meanwhile, "zero days" are only approximately 0.4% of vulnerabilities during the past decade, but their risk to most companies is out of balance with the attention they get.
- Through 2021, 99% of vulnerabilities exploited will continue to be ones known by security and IT professionals for at least one year.
- Through 2021, the single most impactful enterprise activity to improve security will be patching.

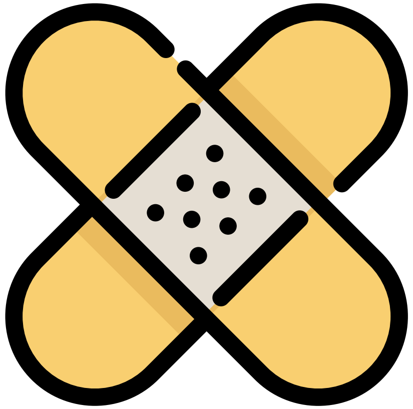
The problem with patching

The Tools Suuuuck

The Methodology Suuuucks

What we need is….

The tools suck…

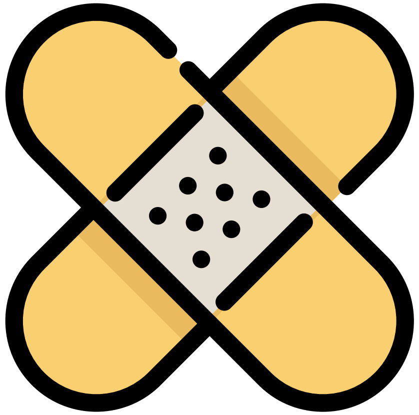


No single capability to inventory status across all layers of an environment

- Network hardware
- Network software
- Server hardware
- Server software
- Workstation hardware
- Workstation software

Applying patches across this diversity of needs is fragile/difficult

Tools suck: What can we do?



Transfer risk so you can focus on patching what is left

Responsibility	SaaS	PaaS	IaaS	On-prem
Information and Data	🟪	🟪	🟪	🟪
Devices (Mobile and PCs)	🟪	🟪	🟪	🟪
Accounts and Identities	🟪	🟪	🟪	🟪
Identity and directory infrastructure	🟦🟪	🟦🟪	🟪	🟪
Applications	🟦	🟦🟪	🟪	🟪
Network Controls	🟦	🟦🟪	🟪	🟪
Operating system	🟦	🟦	🟪	🟪
Physical hosts	🟦	🟦	🟦	🟪
Physical network	🟦	🟦	🟦	🟪
Physical datacenter	🟦	🟦	🟦	🟪

🟦 Cloud Provider 🟪 Tenant Owner

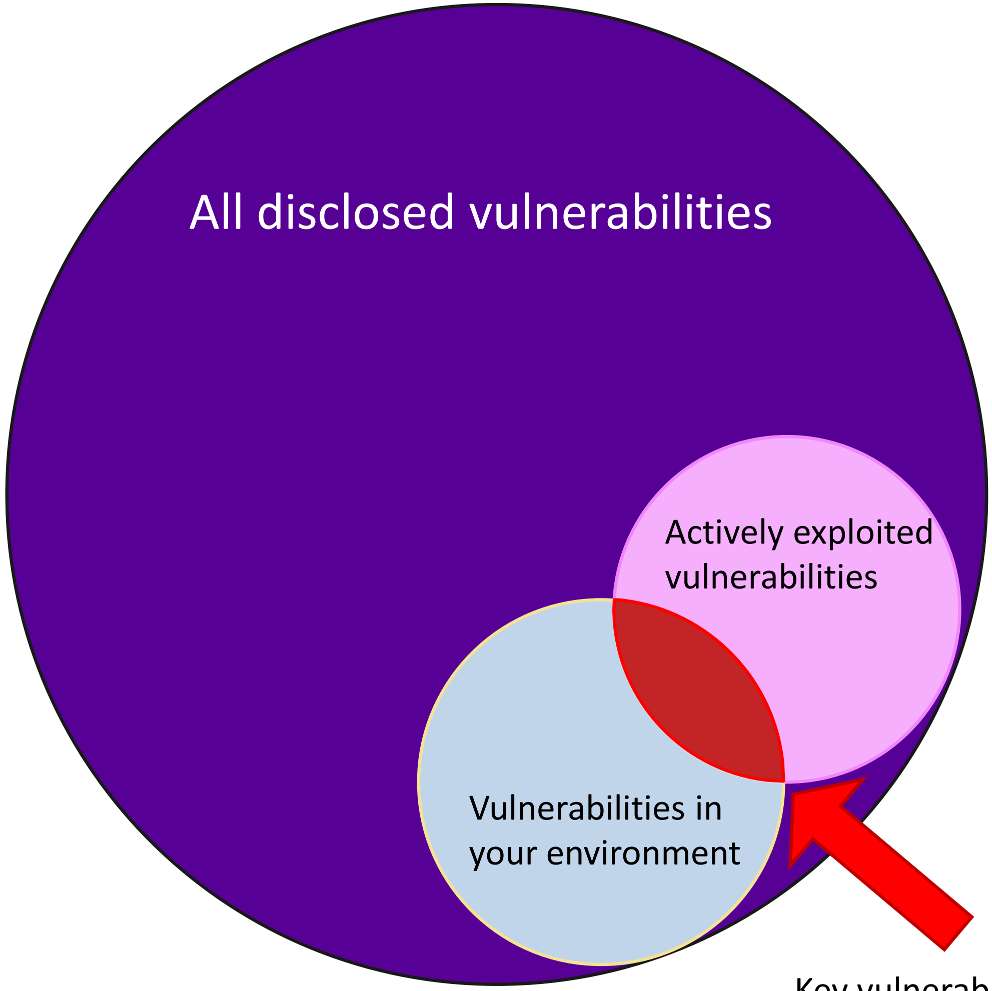
Secure/update what is left

Transfer responsibility to Provider

Establish an intelligent edge

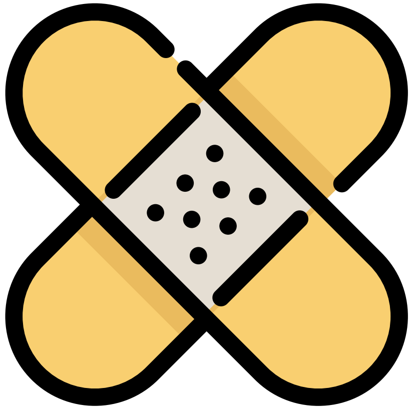
Methodology sucks

- 23% of published vulnerabilities have associated exploit code.
- 2% of published vulnerabilities have observed exploits in the wild.
- How do you keep up with the weaponization to stay on pace tomorrow?


All disclosed vulnerabilities
Actively exploited vulnerabilities
Vulnerabilities in your environment

Key vulnerabilities to be worried about RIGHT NOW

Methodology sucks: What can we do?



- First, focus on the basics
- “Patch everything, all the time, everywhere” doesn’t work.
- Focus on the vulnerabilities being exploited in the wild*
- Employ mitigation controls (compartmentalization/detection)

> Einstein's adage that, "The definition of insanity is to keep doing the same things but expect different results" has rarely seen a more definitive example than the way in which vulnerability management is being pursued in enterprises.

*On average, only about 12.5 percent of all vulnerabilities in the last decade have gone on to be exploited in the wild.

RSAConference2019

Developing a Predictive Model for Patching…

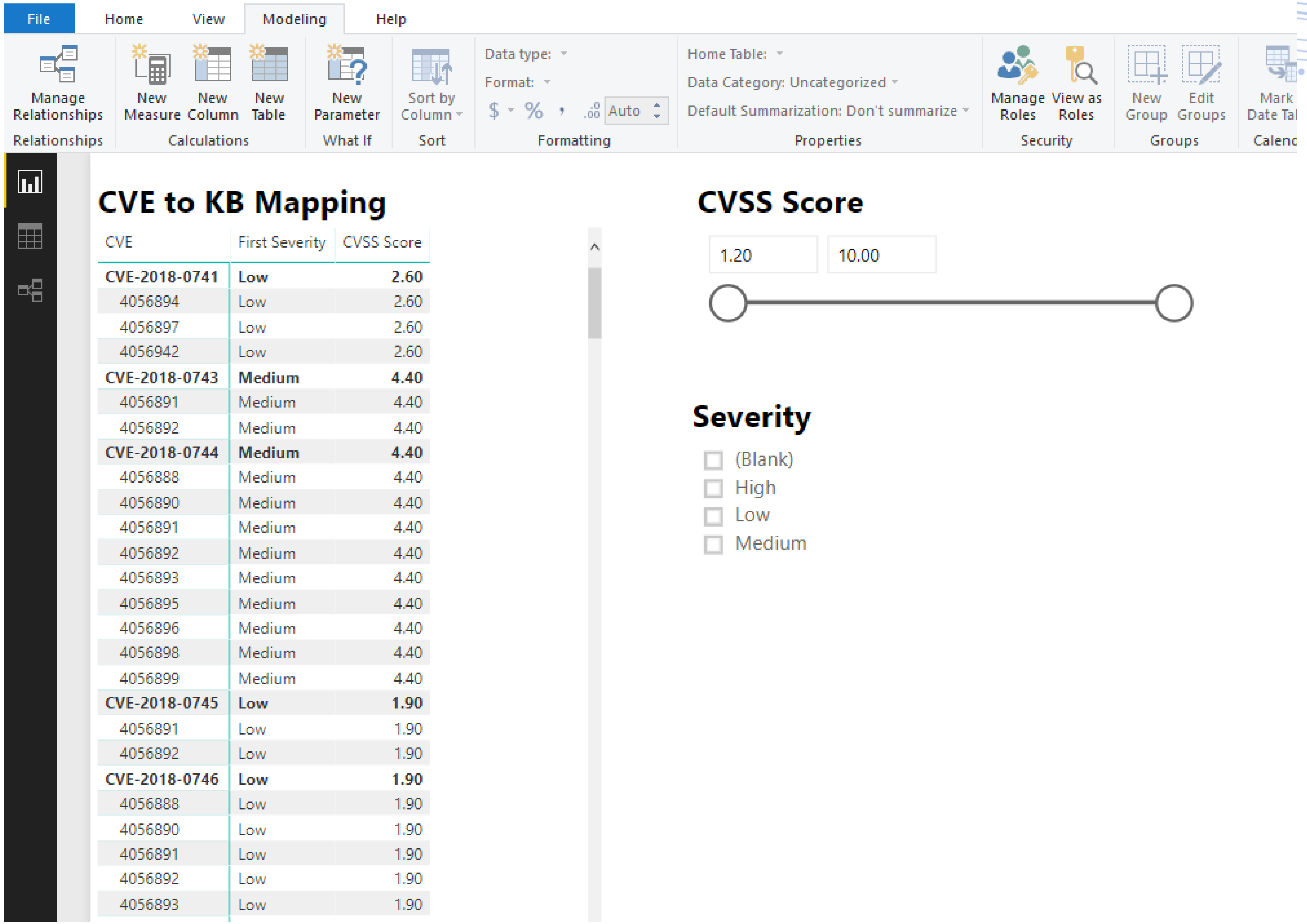
Top vulnerabilities used by cybercriminals*

CVE Number	Company	CVSS
CVE-2017-0199	Microsoft	9.3
CVE-2016-0189	Microsoft	7.6
CVE-2017-0022	Microsoft	4.3
CVE-2015-8651	Adobe	9.3
CVE-2014-6332	Microsoft	9.3
CVE-2016-4117	Adobe	10
CVE-2016-1019	Adobe	10
CVE-2017-0037	Microsoft	7.6

*https://go.recordedfuture.com/hubfs/reports/cta-2018-0327.pdf?utm_source=SecurityWeek

RSA®Conference2019

Demo: Minding the Gap



CVE to KB Mapping

CVE	First Severity	CVSS Score
CVE-2018-0741	**Low**	**2.60**
4056894	Low	2.60
4056897	Low	2.60
4056942	Low	2.60
CVE-2018-0743	**Medium**	**4.40**
4056891	Medium	4.40
4056892	Medium	4.40
CVE-2018-0744	**Medium**	**4.40**
4056888	Medium	4.40
4056890	Medium	4.40
4056891	Medium	4.40
4056892	Medium	4.40
4056893	Medium	4.40
4056895	Medium	4.40
4056896	Medium	4.40
4056898	Medium	4.40
4056899	Medium	4.40
CVE-2018-0745	**Low**	**1.90**
4056891	Low	1.90
4056892	Low	1.90
CVE-2018-0746	**Low**	**1.90**
4056888	Low	1.90
4056890	Low	1.90
4056891	Low	1.90
4056892	Low	1.90
4056893	Low	1.90

CVSS Score

1.20 10.00

Severity

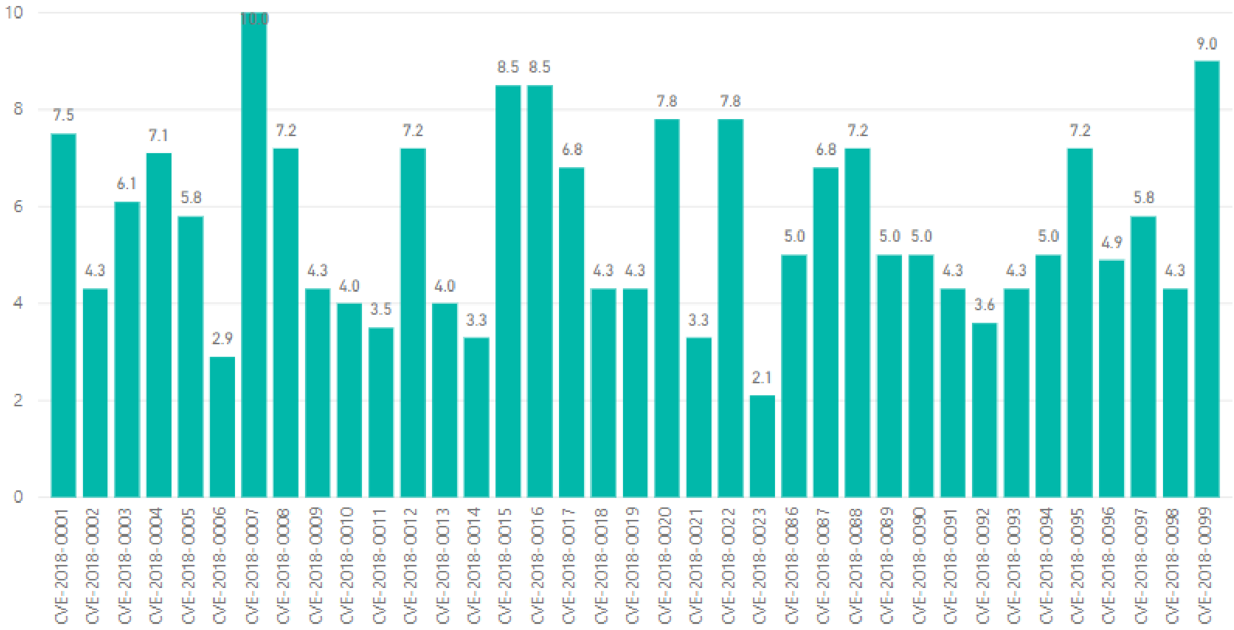
- □ (Blank)
- □ High
- □ Low
- □ Medium

Search CVS Score Score

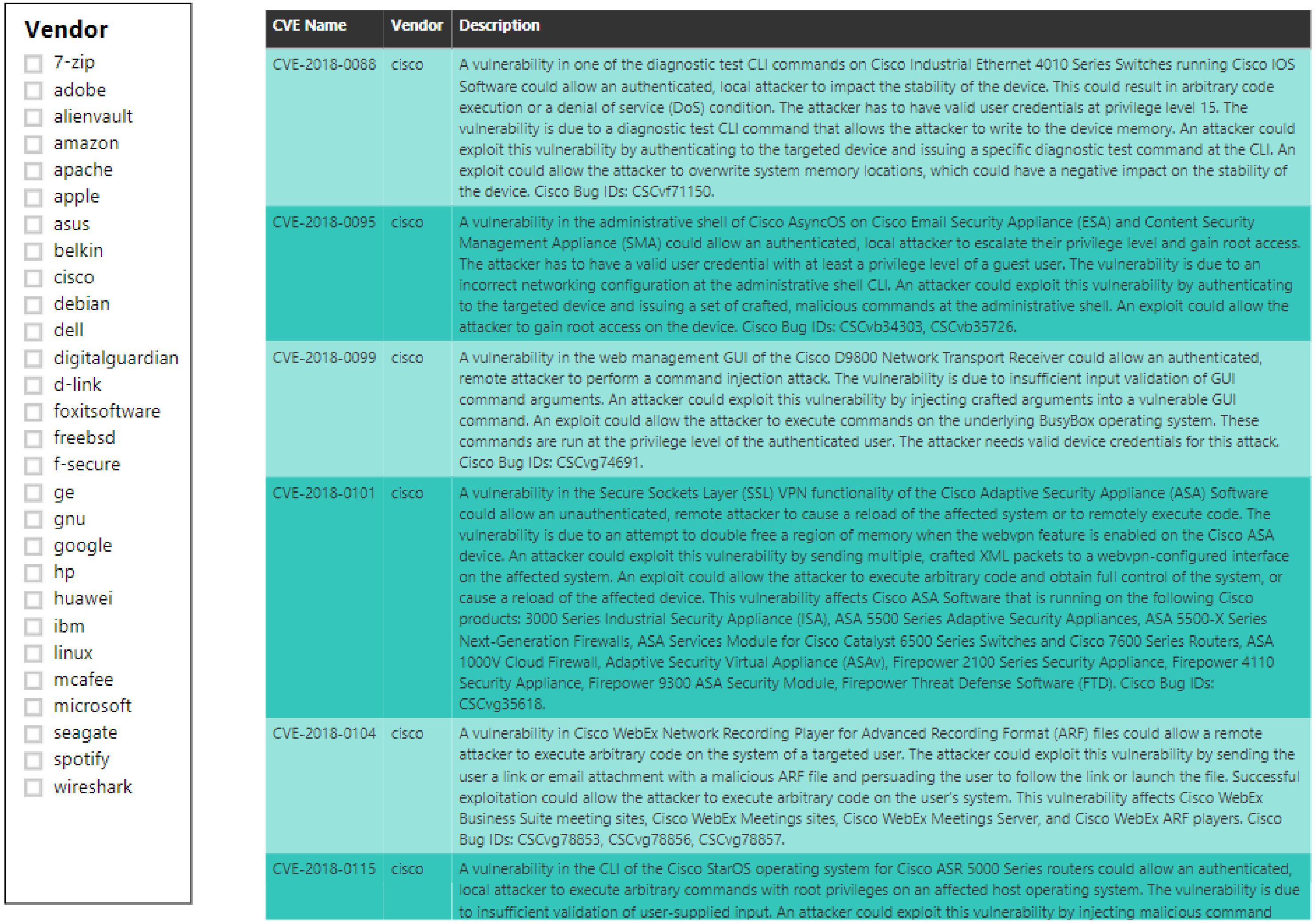
CVS Score

1.20 10.00

CVSS Score by CVE Name



Search for Vulnerabilities by Vendor

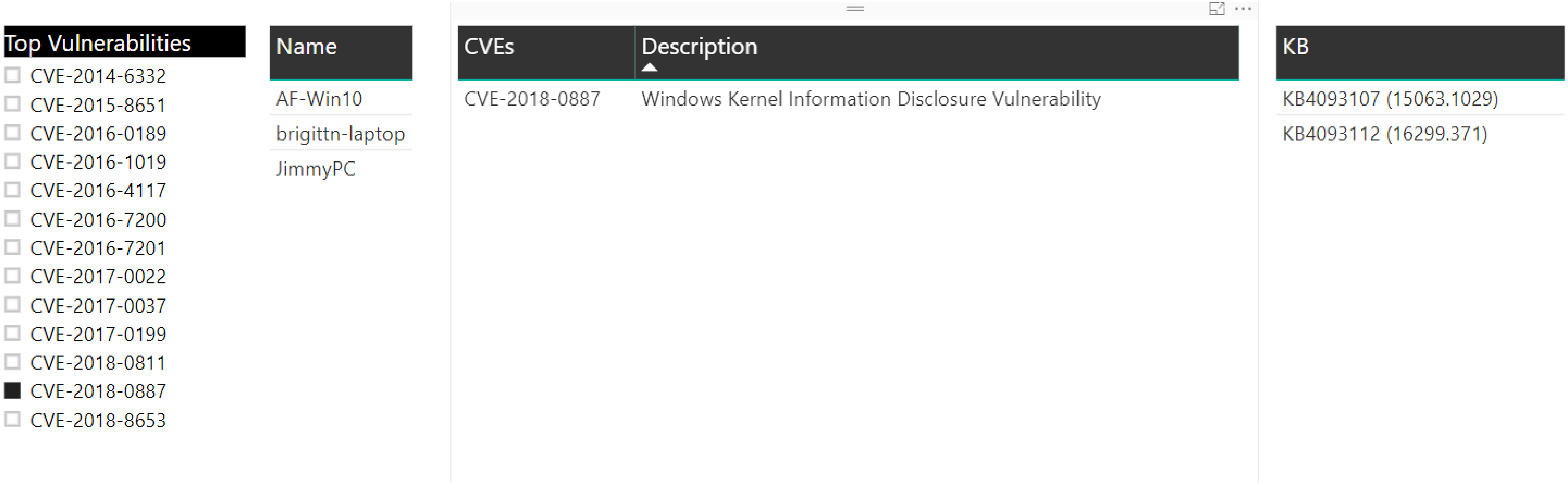


Vendor

- □ 7-zip
- □ adobe
- □ alienvault
- □ amazon
- □ apache
- □ apple
- □ asus
- □ belkin
- □ cisco
- □ debian
- □ dell
- □ digitalguardian
- □ d-link
- □ foxitsoftware
- □ freebsd
- □ f-secure
- □ ge
- □ gnu
- □ google
- □ hp
- □ huawei
- □ ibm
- □ linux
- □ mcafee
- □ microsoft
- □ seagate
- □ spotify
- □ wireshark

CVE Name	Vendor	Description
CVE-2018-0088	cisco	A vulnerability in one of the diagnostic test CLI commands on Cisco Industrial Ethernet 4010 Series Switches running Cisco IOS Software could allow an authenticated, local attacker to impact the stability of the device. This could result in arbitrary code execution or a denial of service (DoS) condition. The attacker has to have valid user credentials at privilege level 15. The vulnerability is due to a diagnostic test CLI command that allows the attacker to write to the device memory. An attacker could exploit this vulnerability by authenticating to the targeted device and issuing a specific diagnostic test command at the CLI. An exploit could allow the attacker to overwrite system memory locations, which could have a negative impact on the stability of the device. Cisco Bug IDs: CSCvf71150.
CVE-2018-0095	cisco	A vulnerability in the administrative shell of Cisco AsyncOS on Cisco Email Security Appliance (ESA) and Content Security Management Appliance (SMA) could allow an authenticated, local attacker to escalate their privilege level and gain root access. The attacker has to have a valid user credential with at least a privilege level of a guest user. The vulnerability is due to an incorrect networking configuration at the administrative shell CLI. An attacker could exploit this vulnerability by authenticating to the targeted device and issuing a set of crafted, malicious commands at the administrative shell. An exploit could allow the attacker to gain root access on the device. Cisco Bug IDs: CSCvb34303, CSCvb35726.
CVE-2018-0099	cisco	A vulnerability in the web management GUI of the Cisco D9800 Network Transport Receiver could allow an authenticated, remote attacker to perform a command injection attack. The vulnerability is due to insufficient input validation of GUI command arguments. An attacker could exploit this vulnerability by injecting crafted arguments into a vulnerable GUI command. An exploit could allow the attacker to execute commands on the underlying BusyBox operating system. These commands are run at the privilege level of the authenticated user. The attacker needs valid device credentials for this attack. Cisco Bug IDs: CSCvg74691.
CVE-2018-0101	cisco	A vulnerability in the Secure Sockets Layer (SSL) VPN functionality of the Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to cause a reload of the affected system or to remotely execute code. The vulnerability is due to an attempt to double free a region of memory when the webvpn feature is enabled on the Cisco ASA device. An attacker could exploit this vulnerability by sending multiple, crafted XML packets to a webvpn-configured interface on the affected system. An exploit could allow the attacker to execute arbitrary code and obtain full control of the system, or cause a reload of the affected device. This vulnerability affects Cisco ASA Software that is running on the following Cisco products: 3000 Series Industrial Security Appliance (ISA), ASA 5500 Series Adaptive Security Appliances, ASA 5500-X Series Next-Generation Firewalls, ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers, ASA 1000V Cloud Firewall, Adaptive Security Virtual Appliance (ASAv), Firepower 2100 Series Security Appliance, Firepower 4110 Security Appliance, Firepower 9300 ASA Security Module, Firepower Threat Defense Software (FTD). Cisco Bug IDs: CSCvg35618.
CVE-2018-0104	cisco	A vulnerability in Cisco WebEx Network Recording Player for Advanced Recording Format (ARF) files could allow a remote attacker to execute arbitrary code on the system of a targeted user. The attacker could exploit this vulnerability by sending the user a link or email attachment with a malicious ARF file and persuading the user to follow the link or launch the file. Successful exploitation could allow the attacker to execute arbitrary code on the user's system. This vulnerability affects Cisco WebEx Business Suite meeting sites, Cisco WebEx Meetings sites, Cisco WebEx Meetings Server, and Cisco WebEx ARF players. Cisco Bug IDs: CSCvg78853, CSCvg78856, CSCvg78857.
CVE-2018-0115	cisco	A vulnerability in the CLI of the Cisco StarOS operating system for Cisco ASR 5000 Series routers could allow an authenticated, local attacker to execute arbitrary commands with root privileges on an affected host operating system. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by injecting malicious command

Search for Top Vulnerabilities in your environment



Top Vulnerabilities

- ☐ CVE-2014-6332
- ☐ CVE-2015-8651
- ☐ CVE-2016-0189
- ☐ CVE-2016-1019
- ☐ CVE-2016-4117
- ☐ CVE-2016-7200
- ☐ CVE-2016-7201
- ☐ CVE-2017-0022
- ☐ CVE-2017-0037
- ☐ CVE-2017-0199
- ☐ CVE-2018-0811
- ■ CVE-2018-0887
- ☐ CVE-2018-8653

Name
AF-Win10
brigittn-laptop
JimmyPC

CVEs	Description
CVE-2018-0887	Windows Kernel Information Disclosure Vulnerability

KB
KB4093107 (15063.1029)
KB4093112 (16299.371)

Apply What You Have Learned Today

- Next week:
  - Start to inventory **ALL** your environment (software, hardware, appliances)
  - Turn on MFA for all Admin Accounts (Azure makes this easy)
  - Start a project to determine how to move from passwords to an alternative
- In the next three months:
  - Develop a “Threat Feed” to cross-reference CVEs against your inventory
  - Build the team to “Mind the Gap” on closing the patching gap
  - Begin pilot phase of the password alternative rollout
  - Develop communication strategy for broader rollout to the organization
- Within six months you should:
  - Build on your patching success to expand beyond “The Gap”
  - Investigate additional capabilities such as Conditional Access

References & Resources

RSAConference2019

Questions?