HACC

HAWAI'I ANNUAL CODE CHALLENGE

HACC – Workshop 1

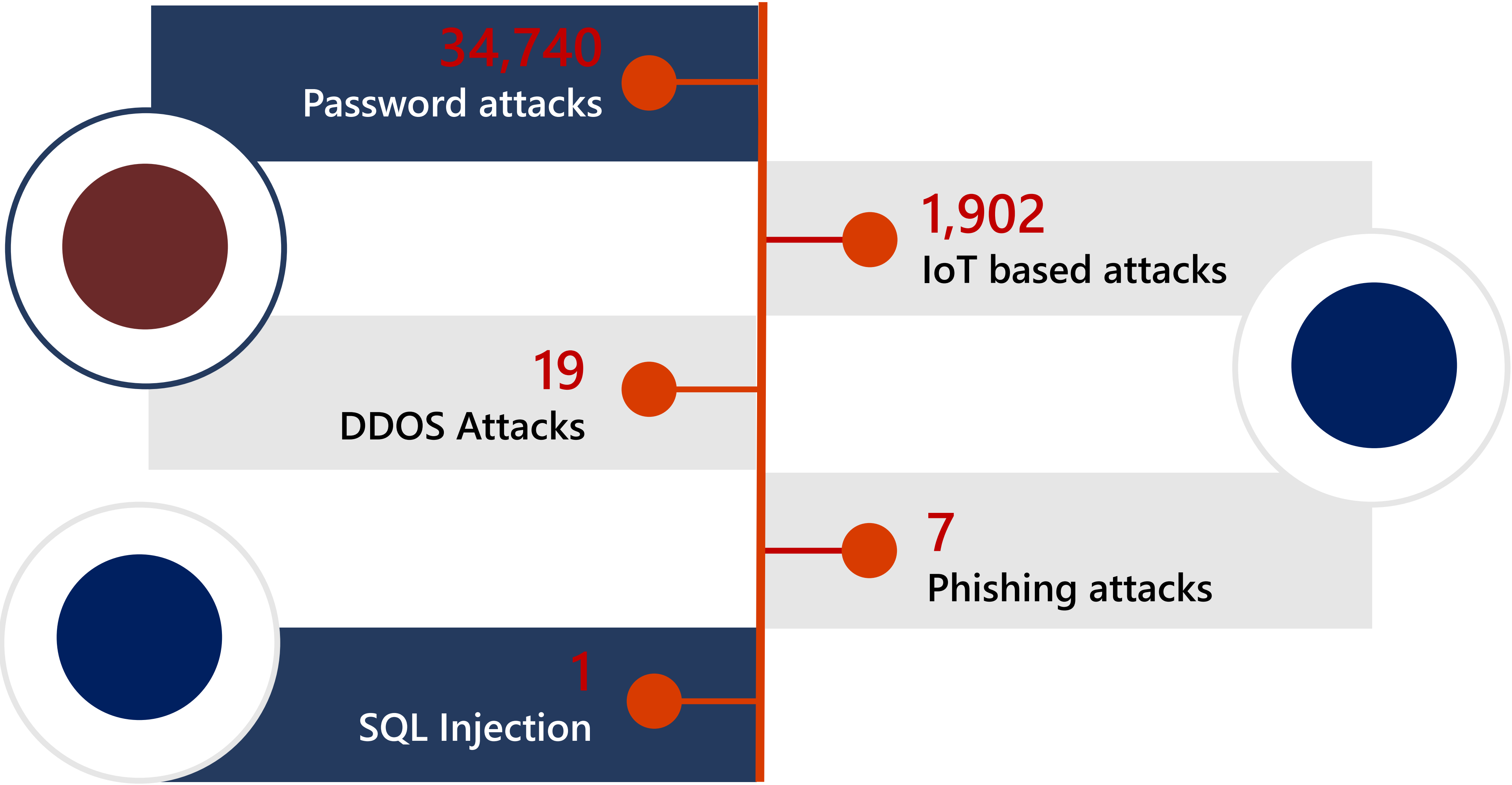
Security & Privacy Considerations in App Development

Richard Antonow
Security Technical Specialist

Microsoft

It only takes 1 minute

Volume of attacks



34,740
Password attacks

1,902
IoT based attacks

19
DDOS Attacks

7
Phishing attacks

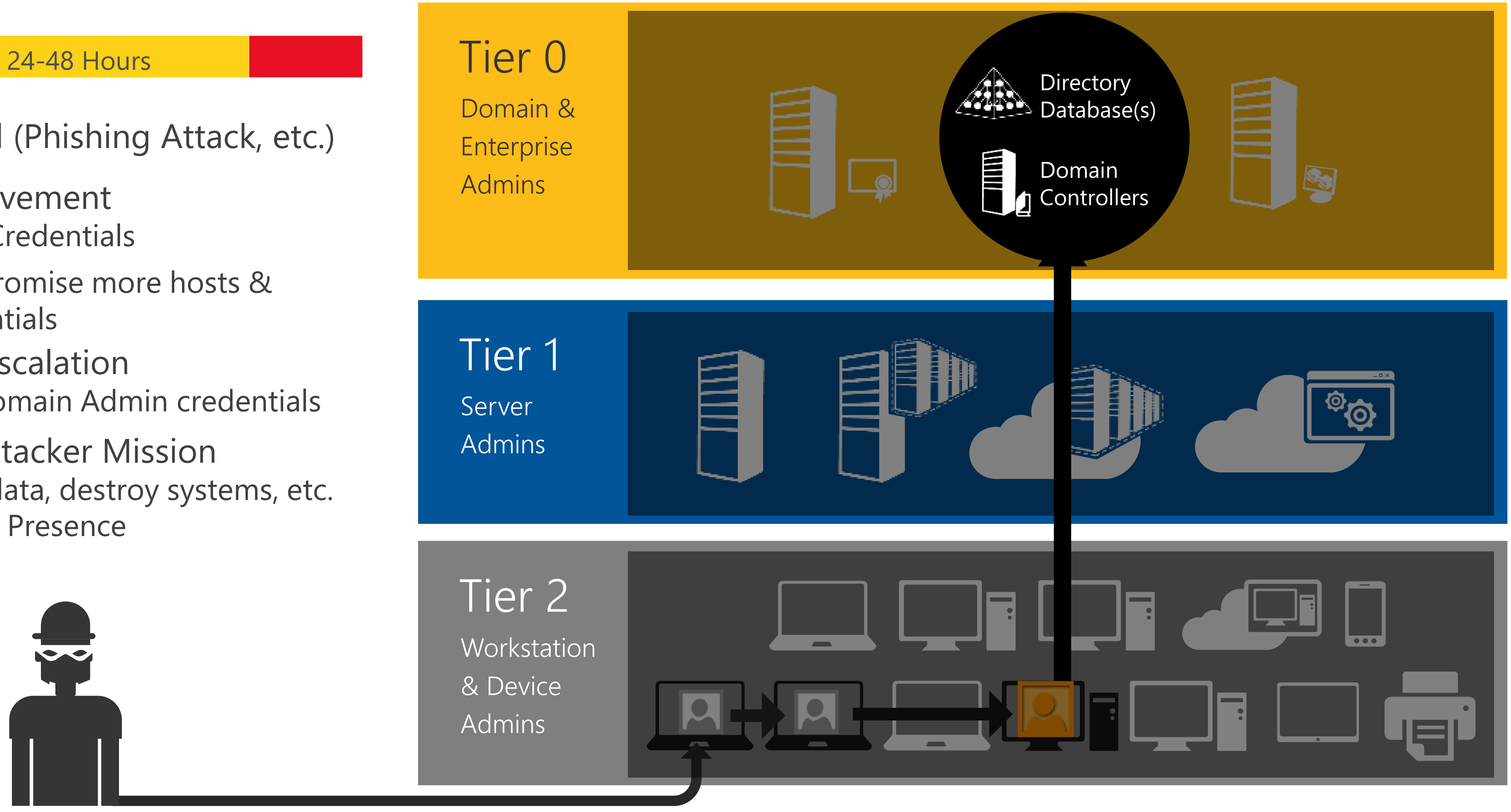
1
SQL Injection

What are hackers going after?

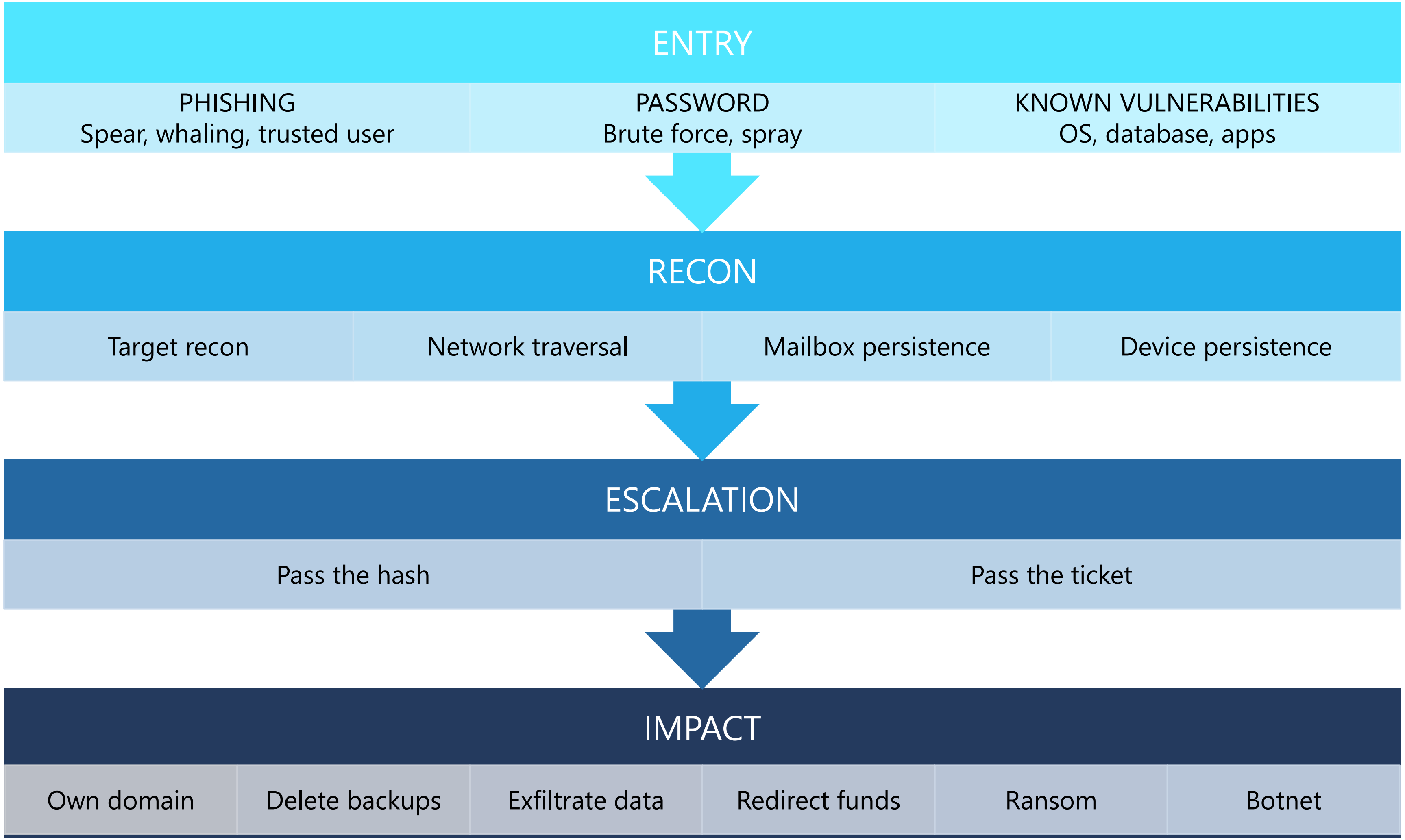
Utilizes identity to compromise systems and access data

24-48 Hours

1. Beachhead (Phishing Attack, etc.)
2. Lateral Movement
   a. Steal Credentials
   b. Compromise more hosts & credentials
3. Privilege Escalation
   a. Get Domain Admin credentials
4. Execute Attacker Mission
   a. Steal data, destroy systems, etc.
   b. Persist Presence



ANATOMY OF A BREACH...OR SEVERAL



ENTRY

- PHISHING
  Spear, whaling, trusted user
- PASSWORD
  Brute force, spray
- KNOWN VULNERABILITIES
  OS, database, apps

RECON

- Target recon
- Network traversal
- Mailbox persistence
- Device persistence

ESCALATION

- Pass the hash
- Pass the ticket

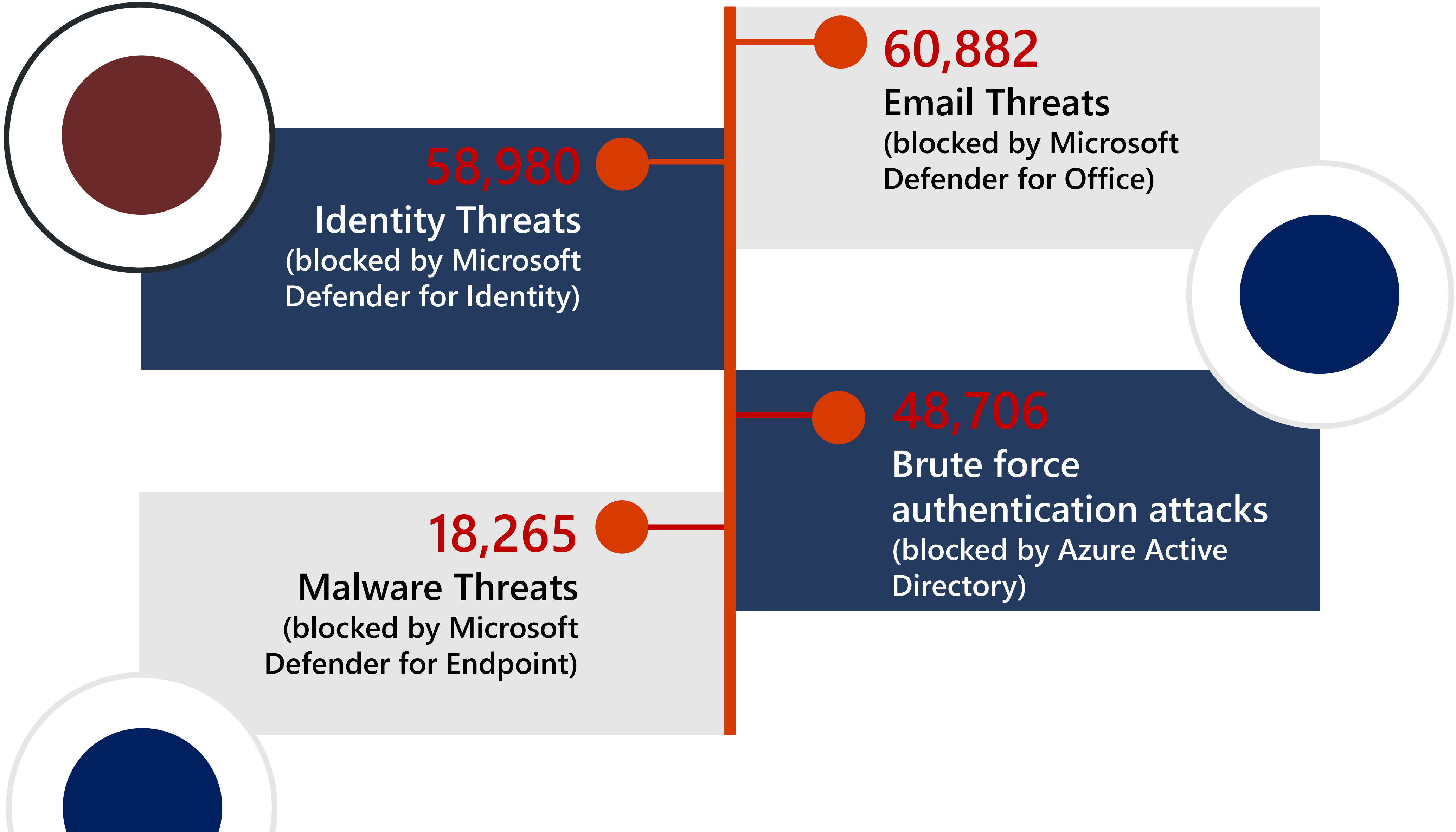
IMPACT

- Own domain
- Delete backups
- Exfiltrate data
- Redirect funds
- Ransom
- Botnet

Want to protect your account? - DON’T tell your password!

It only takes 1 minute

Attacks blocked by Microsoft



60,882

Email Threats

(blocked by Microsoft Defender for Office)

58,980

Identity Threats

(blocked by Microsoft Defender for Identity)

48,706

Brute force authentication attacks

(blocked by Azure Active Directory)

18,265

Malware Threats

(blocked by Microsoft Defender for Endpoint)

Phishing – The entry point

Phishing is an online scam where criminals send alluring emails to the organization, user, and more to collect sensitive information.

Email phishing

•The most common form of phishing, this type of attack uses tactics like phony hyperlinks to lure email recipients into sharing their personal information. Attackers often masquerade as a large account provider like Microsoft or Google, or even a coworker.

Malware phishing

•Another prevalent phishing approach, this type of attack involves planting malware disguised as a trustworthy attachment (such as a resume or bank statement) in an email. In some cases, opening a malware attachment can paralyze entire IT systems.

Spear phishing

•Where most phishing attacks cast a wide net, spear phishing targets specific individuals by exploiting information gathered through research into their jobs and social lives. These attacks are highly customized, making them particularly effective at bypassing basic cybersecurity.

Whaling

•When bad actors target a “big fish” like a business executive or celebrity, it’s called whaling. These scammers often conduct considerable research into their targets to find an opportune moment to steal login credentials or other sensitive information. If you have a lot to lose, whaling attackers have a lot to gain.

Smishing

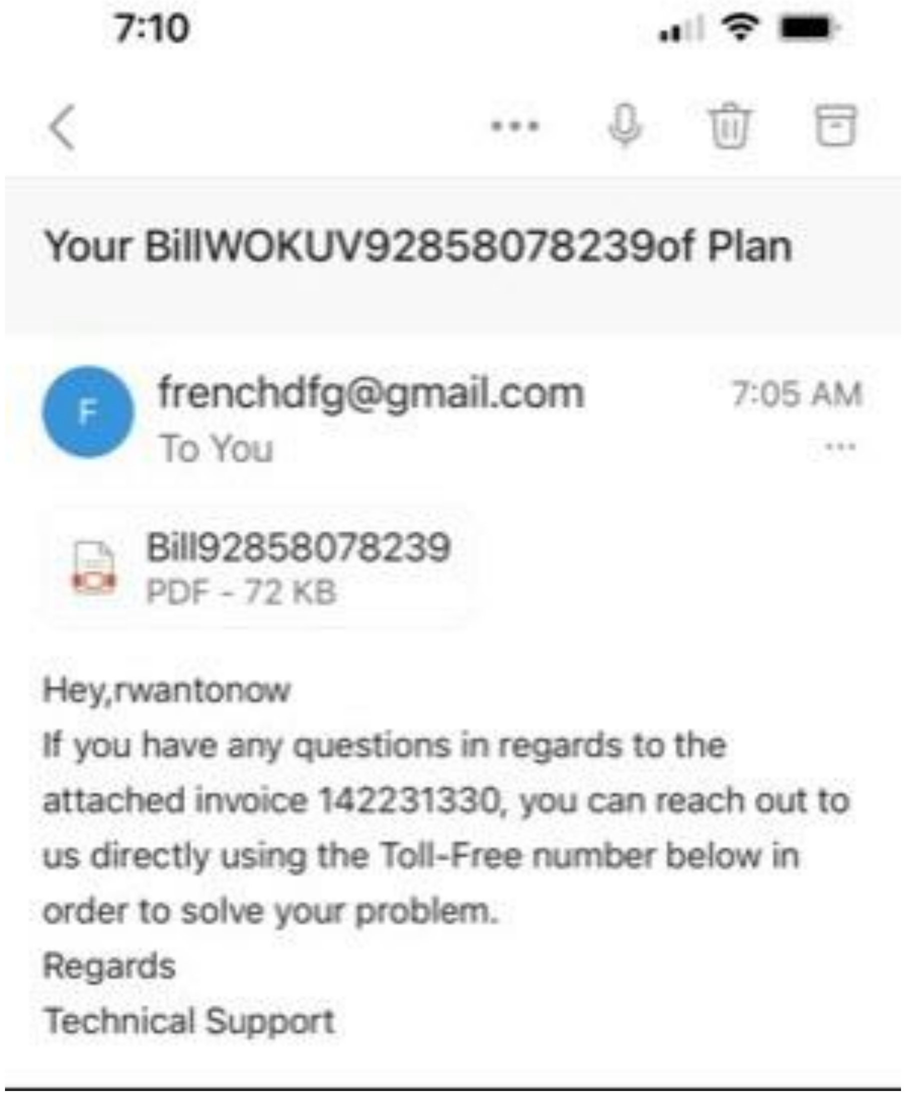
•A combination of the words “SMS” and “phishing,” smishing involves sending text messages disguised as trustworthy communications from businesses like Amazon or FedEx. People are particularly vulnerable to SMS scams, as text messages are delivered in plain text and come across as more personal.

Vishing

•In vishing campaigns, attackers in fraudulent call centers attempt to trick people into providing sensitive information over the phone. In many cases, these scams use social engineering to dupe victims into installing malware onto their devices in the form of an app.

Can you spot a Phishing attempt?

Can you spot 5 signs that this is a phishing email?



Your BillWOKUV92858078239of Plan

frenchdfg@gmail.com 7:05 AM

To You

Bill92858078239

PDF - 72 KB

Hey,rwantonow

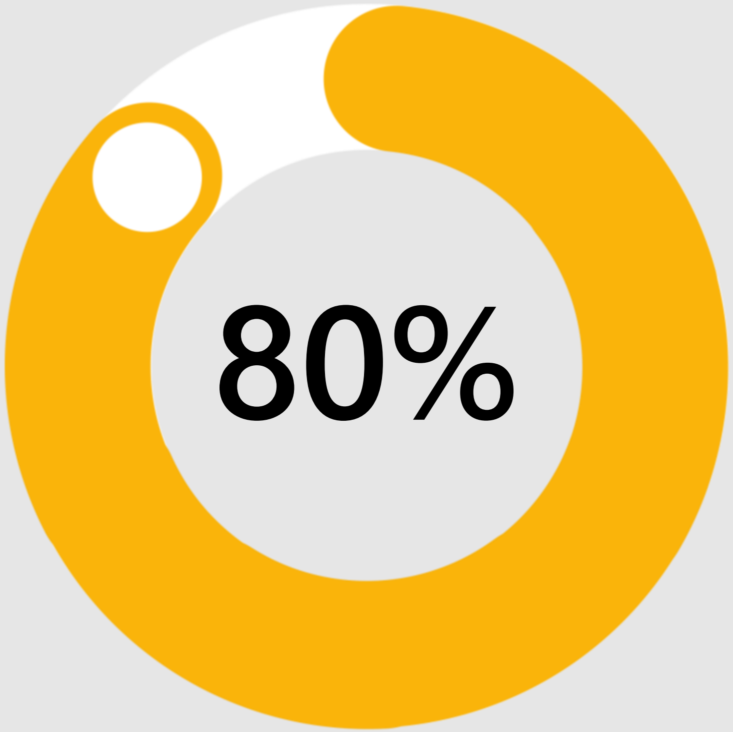
If you have any questions in regards to the attached invoice 142231330, you can reach out to us directly using the Toll-Free number below in order to solve your problem.

Regards

Technical Support

Ransomware

Ransomware's
new business model



Over 80 percent of ransomware attacks can be traced to common configuration errors in software and devices.[1]

● Ransomware attacks exploiting configuration errors

The Cost of Ransomware

“Ninety-four percent of respondents said the ransomware attack impacted their ability to operate and 90% of private sector healthcare organizations responded that the attack “caused them to lose business or revenue.”

“…the average cost for a healthcare organization to remediate the impact of a ransomware attack went up to $1.85 million in 2021, compared to $1.27 million in 2020. This was the second-highest average cost across all sectors.”

It took 44% of healthcare organizations “up to a week” to recover from a ransomware attack in 2021, and 25% took up to a month to recover. The average time for healthcare organizations to recover was one week.

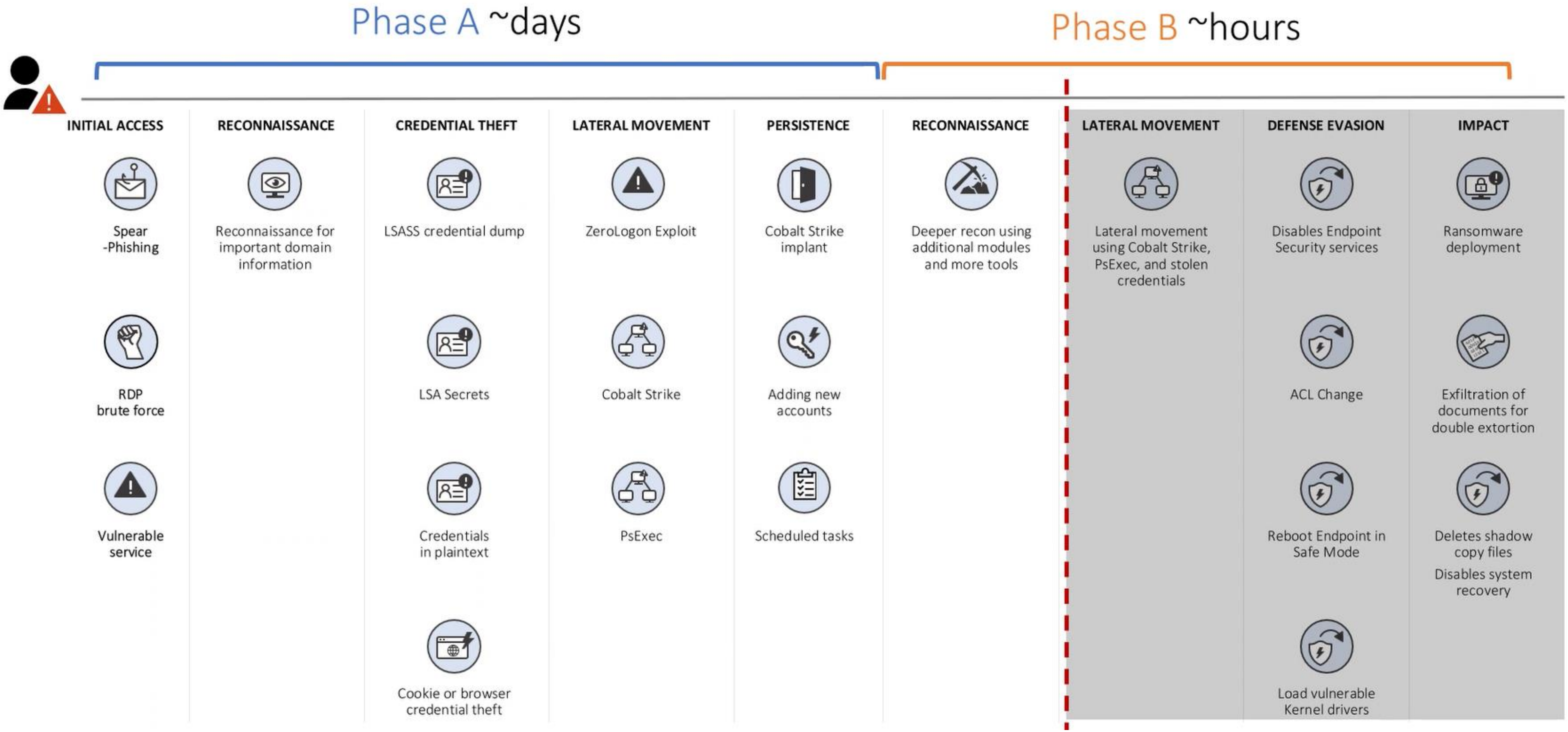
Source: Thomas Reuters July 5, 2022

Consider these statistics about ransomware in healthcare:

- ✓ 66% of healthcare organizations were struck by ransomware in 2021. This is almost **double** the number of the year before.
- ✓ 61% of these organizations will pay the ransom. This is the **highest figure** in all industries.
- ✓ $1.85 million is the average cost to recover from these ransomware attacks.

Source: CEI Digital Office, Ransomware in Healthcare Organizations and the State of the Industry in 2022

How fast does ransomware propagate?



Phase A ~days

Phase B ~hours

INITIAL ACCESS
- Spear -Phishing
- RDP brute force
- Vulnerable service

RECONNAISSANCE
- Reconnaissance for important domain information

CREDENTIAL THEFT
- LSASS credential dump
- LSA Secrets
- Credentials in plaintext
- Cookie or browser credential theft

LATERAL MOVEMENT
- ZeroLogon Exploit
- Cobalt Strike
- PsExec

PERSISTENCE
- Cobalt Strike implant
- Adding new accounts
- Scheduled tasks

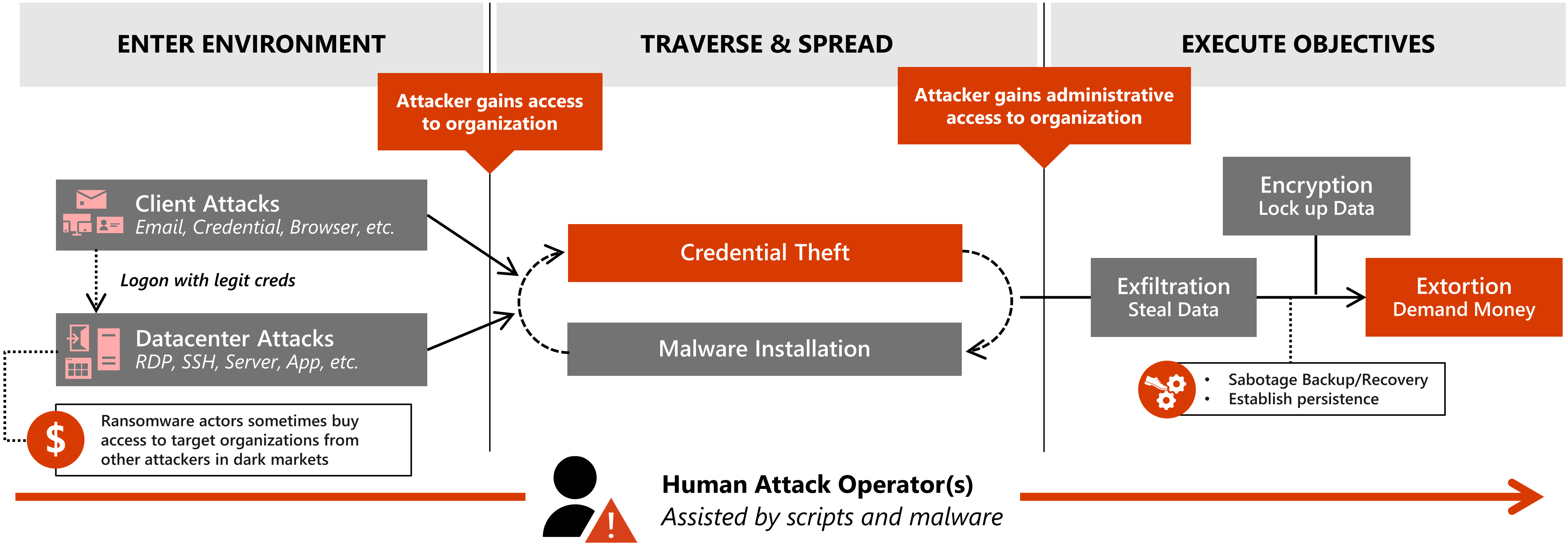
RECONNAISSANCE
- Deeper recon using additional modules and more tools

LATERAL MOVEMENT
- Lateral movement using Cobalt Strike, PsExec, and stolen credentials

DEFENSE EVASION
- Disables Endpoint Security services
- ACL Change
- Reboot Endpoint in Safe Mode
- Load vulnerable Kernel drivers

IMPACT
- Ransomware deployment
- Exfiltration of documents for double extortion
- Deletes shadow copy files
- Disables system recovery

Pattern – Human Operated Ransomware



ENTER ENVIRONMENT

TRAVERSE & SPREAD

EXECUTE OBJECTIVES

Attacker gains access to organization

Attacker gains administrative access to organization

Client Attacks
Email, Credential, Browser, etc.

Logon with legit creds

Datacenter Attacks
RDP, SSH, Server, App, etc.

Ransomware actors sometimes buy access to target organizations from other attackers in dark markets

Credential Theft

Malware Installation

Encryption
Lock up Data

Exfiltration
Steal Data

Extortion
Demand Money

- Sabotage Backup/Recovery
- Establish persistence

Human Attack Operator(s)
Assisted by scripts and malware

Ryuk example (Email)

Wadhrama example (RDP)

Actionable Insights

Comparison to traditional ransomware

GDPR – A Global Requirement

General Data Protection Regulation (GDPR). GDPR was put in effect in the European Union (EU) in 2018 and defines the collection, processing or storing of personal data of anyone within the EU.

But my application is in the US… why do I need to worry about GDPR? – because the physical location of the institution, organization or business is not as important in determining the need to comply with the GDPR as the physical location of the data subject – the individual whose data is being collected, processed or stored.

The GDPR places strict controls on data transferred to non-EU countries or international organizations. These are detailed in Chapter V of the Regulation. Data is allowed to be transferred only when the EU Commission has deemed that the transfer destination "ensures an adequate level of protection".

Source: HIPAA Journal, 2022

Take-away: when writing applications that collect personal data about an individual, you must provide a method for the user to opt out of storing that data and/or wiping all personal data when they leave that application

HIPAA Compliance

Health Insurance Portability and Accountability Act (HIPAA), which regulates healthcare information;

Under HIPAA, protected health information is considered to be individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations (PHI healthcare business uses).

Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information.

Source: HIPAA Journal, 2022

Take-away: Think about where and how data will be stored and protected. Care must be taken in securely protecting any Personally Identifiable Information (PII) relating to user healthcare

Secure Coding Guidelines

When designing and writing your code, you need to protect and limit the access that code has to resources, especially when using or invoking code of unknown origin. So, keep in mind the following techniques to ensure your code is secure:

- Do not use Code Access Security (CAS).
- Do not use partial trusted code.
- Do not use the AllowPartiallyTrustedCaller attribute (APTCA).
- Do not use .NET Remoting.
- Do not use Distributed Component Object Model (DCOM).
- Do not use binary formatters.

User data, which is any kind of input (data from a Web request or URL, input to controls of a Microsoft Windows Forms application, and so on), can adversely influence code because often that data is used directly as parameters to call other code. This situation is analogous to malicious code calling your code with strange parameters, and the same precautions should be taken. User input is actually harder to make safe because there is no stack frame to trace the presence of the potentially untrusted data.

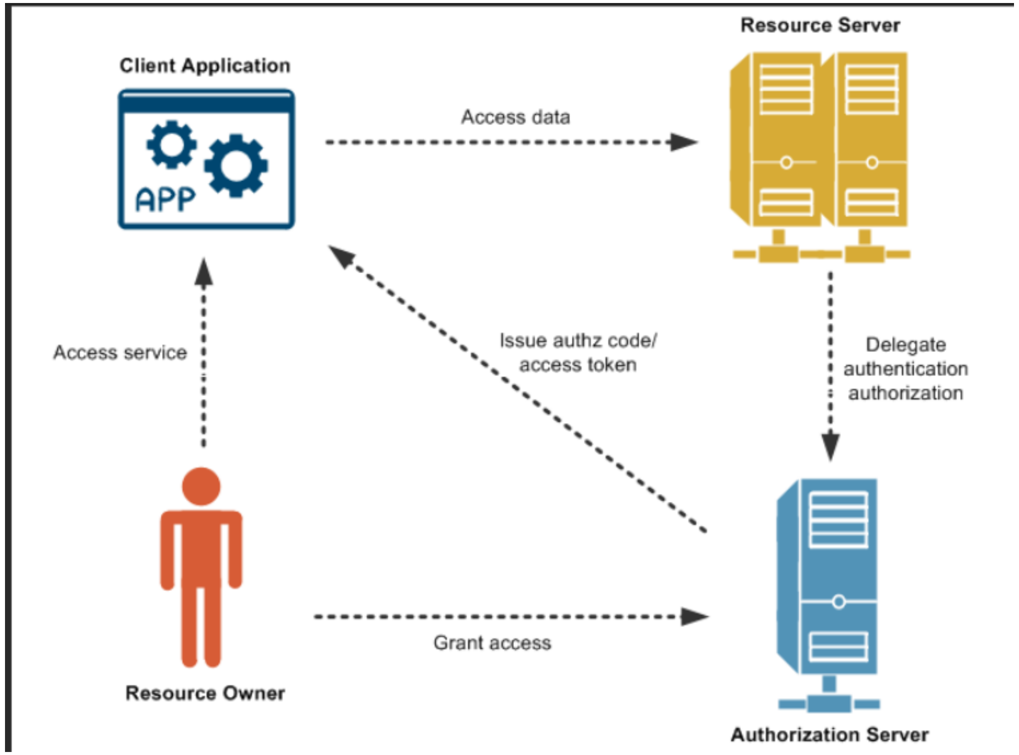
Secure coding guidelines for .NET | Microsoft Learn

OAuth2 for Secure Web and Mobile apps

"OAuth 2 is an authorization framework that enables applications — such as Facebook, GitHub, and DigitalOcean — to obtain limited access to user accounts on an HTTP service. It works by delegating user authentication to the service that hosts a user account and authorizing third-party applications to access that user account. OAuth 2 provides authorization flows for web and desktop applications, as well as mobile devices."

Source: Digital Ocean 2022

1) The *application* requests authorization to access service resources from the *user*
2) If the *user* authorized the request, the *application* receives an authorization grant
3) The *application* requests an access token from the *authorization server* (API) by presenting authentication of its own identity, and the authorization grant
4) If the application identity is authenticated and the authorization grant is valid, the *authorization server* (API) issues an access token to the application. Authorization is complete.
5) The *application* requests the resource from the *resource server* (API) and presents the access token for authentication
6) If the access token is valid, the *resource server* (API) serves the resource to the *application*

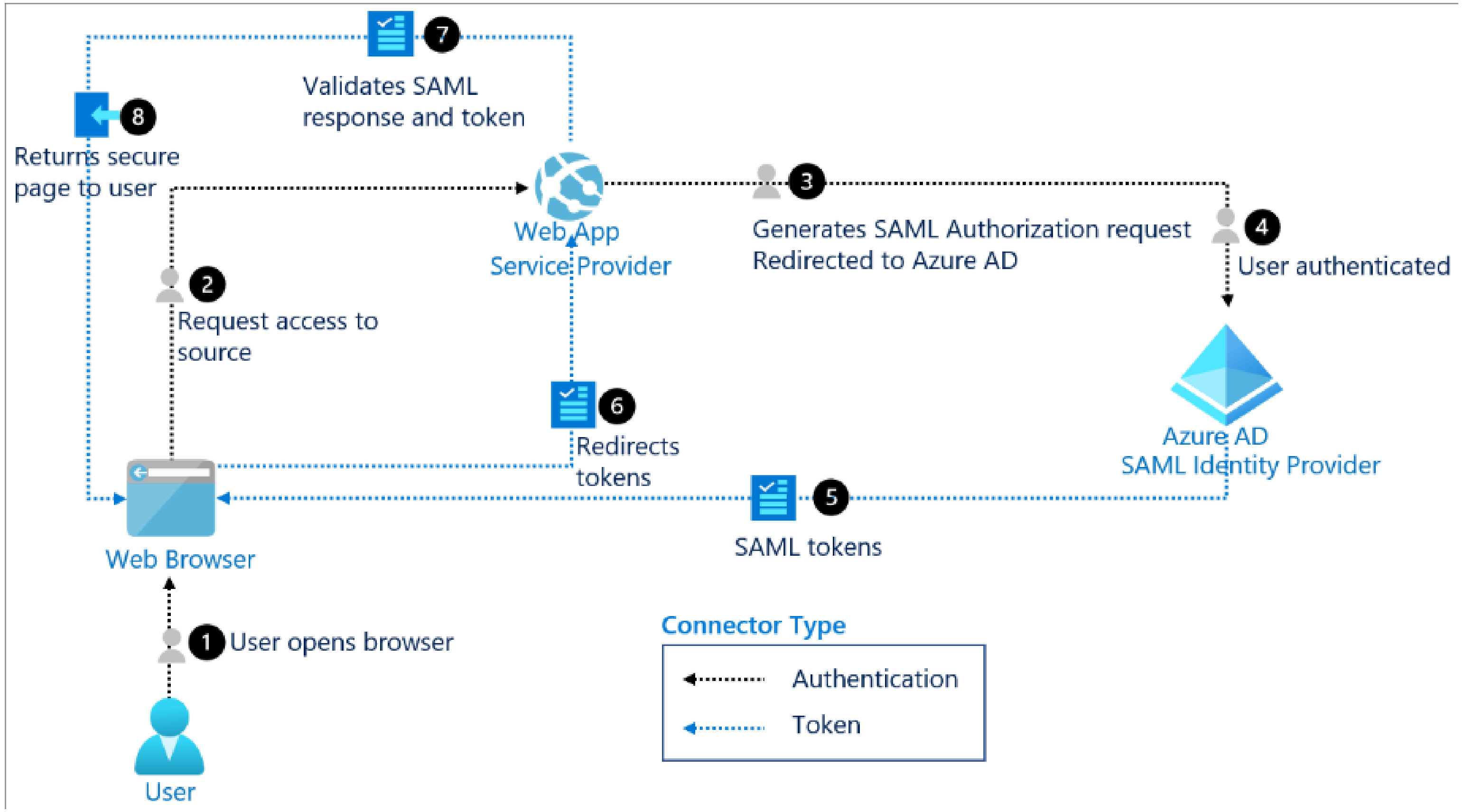


SAML for Secure Single Sign-On

Security Assertion Markup Language (SAML) is an open standard for exchanging authentication and authorization data between an identity provider and a service provider. SAML is an XML-based markup language for security assertions, which are statements that service providers use to make access-control decisions.

The SAML specification defines three roles:

- The principal, generally a user
- The identity provider (IdP)
- The service provider (SP)



[SAML authentication with Azure Active Directory - Microsoft Entra | Microsoft Learn]

Should I use OAuth2 or SAML for my apps?

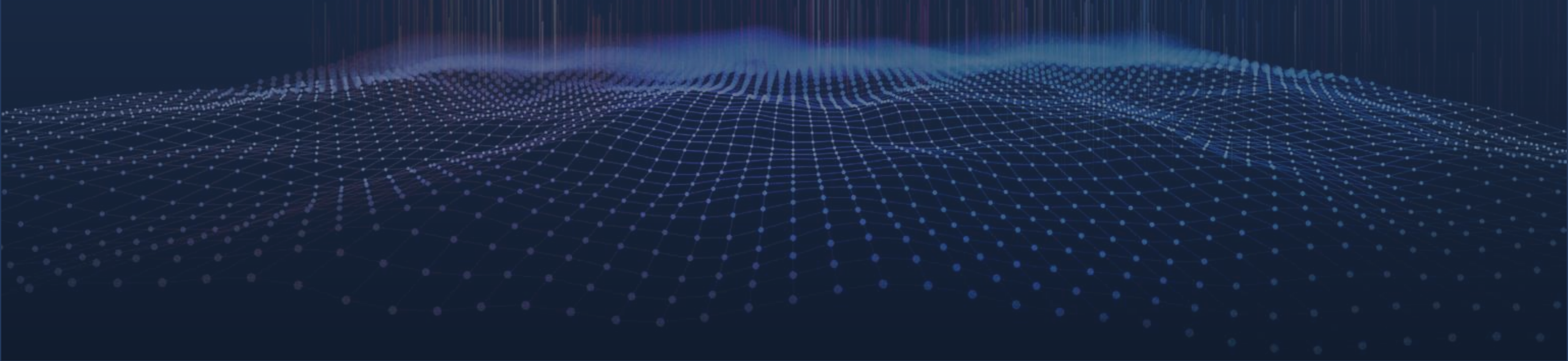
The primary difference between SAML and OAuth is that **SAML generally facilitates exchange of a single user's authentication and authorization data across secure domains**. In contrast, OAuth typically works on behalf of a specific application to share user information on a limited basis with other applications.

"SAML supports both user authentication and authorization while OAuth is only for authorization. If the business priority is confirming user identity, SAML is the only choice. If the business priority is securely and easily managing user privileges, OAuth may be the better choice."

But can they be used TOGETHER? – YES!
Because each as a particular capability unique to the usage, Microsoft services such as Azure use both for application provisioning where SAML grants system access and OAuth grants access to protected resources.

Microsoft

Threat Insights



Security Snapshot

Microsoft's Digital Crimes Unit (DCU)

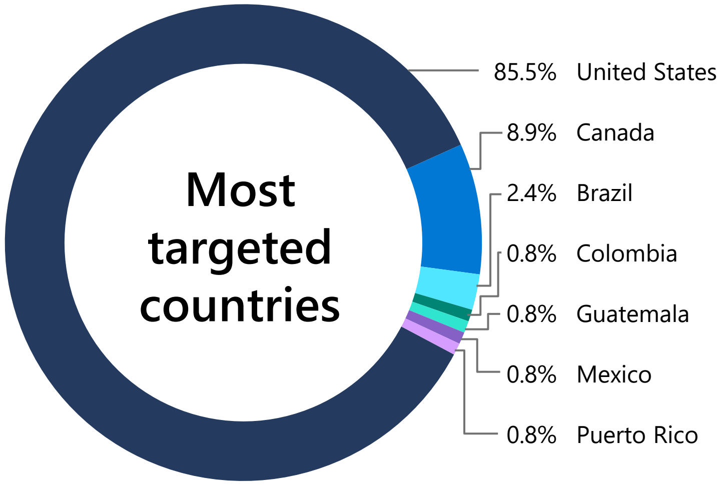
Directed the removal of more than 531,000 unique phishing URLs and 5,400 phish kits between July 2021 and June 2022, leading to the identification and closure of over 1,400 malicious email accounts used to collect stolen customer credentials.[1]

Email Threats:
Median time for an attacker to access your private data if you fall victim to a phishing email is one hour, 12 minutes.[1]

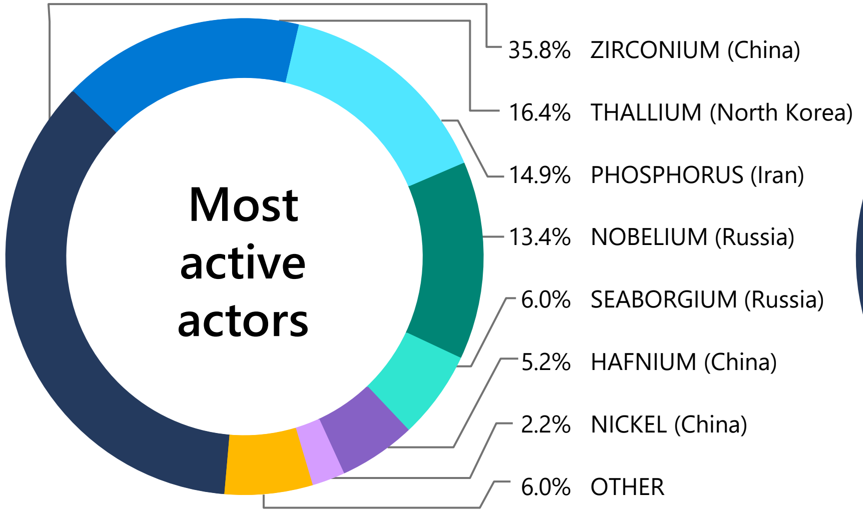
Endpoint Threats:
Median time for an attacker to begin moving laterally within your corporate network if a device is compromised is one hour, 42 minutes.[1]

Americas (including United States)

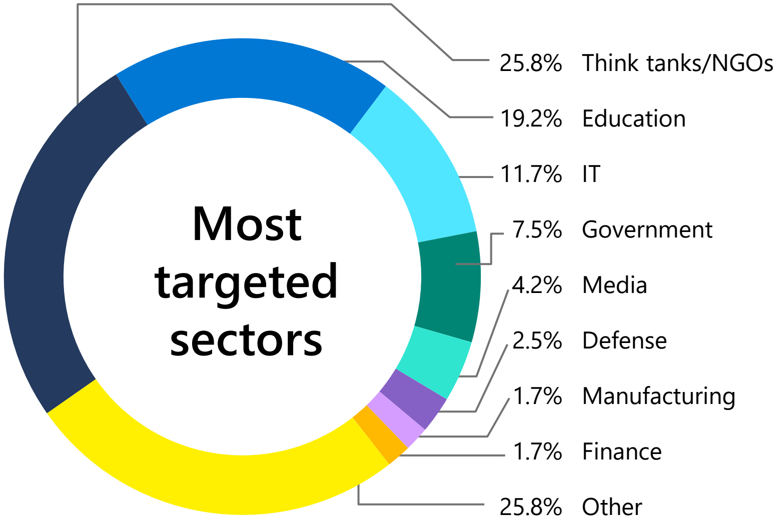
Apr-Jun 2022



US targets remained a major focus of nation state actors, particularly compared to other countries in the Americas.



Interest in US entities came from all over. ZIRCONIUM (China) continued email web bug campaigning against consumer accounts. THALLIUM attempted to compromise think tanks and university accounts.



NOBELIUM's focus on supply chain compromises drove the IT sector targeting, while PHOSPHORUS' targeting of university scholars drove education sector targeting.

Note: 1. Other is inclusive of all other categories excluding those previously named.

Microsoft

Actionable Insights

Defending against attacks

Cybercriminals add double extortion to attack strategy

1

Problem

Stolen passwords and unprotected identities
More than malware, attackers need credentials to succeed. In nearly all successful ransomware deployments attackers gain access to privileged, administrator level accounts granting broad access to an organizations' network.

Action

Authenticate identities
Enforce multifactor authentication (MFA) on all accounts, prioritize administrator and other sensitive roles. With a hybrid workforce, require MFA on all devices, in all locations, at all times. Enable passwordless authentication like FIDO keys or Microsoft Authenticator for apps that support it.

Defending against attacks

Cybercriminals add double extortion to attack strategy

2

Problem

Missing or disabled security products
In almost every observed ransomware incident, at least one system exploited in the attack had missing or misconfigured security products that allowed intruder to tamper with or disable certain protections.

Action

Address security blind spots
Like smoke alarms, security products must be installed in the correct spaces and tested frequently. Verify that security tools are operating in their most secure configuration, and that no part of a network is unprotected.

Defending against attacks

Cybercriminals add double extortion to attack strategy

3

Problem

Misconfigured or abused applications
You might use a popular app for one purpose, but that doesn't mean criminals can't weaponize it for another goal. Too often, "legacy" configurations mean an app is in its default state, allowing any user wide access across entire organizations. Don't overlook this risk or hesitate to change app settings for fear of disruption.

Action

Harden internet facing assets
Consider deleting duplicative or unused apps to eliminate risky, unused services. Be mindful of where you permit remote helpdesk apps like TeamViewer. These are notoriously targeted by threat actors to gain express access to laptops.

Defending against attacks

Cybercriminals add double extortion to attack strategy

4

Problem

Slow patching
It’s a cliché, like “Eat your vegetables!” – but it’s a critical fact: The best way to harden software it to keep it updated. While some cloud-based apps update with no user action, companies must apply other vendor patches immediately. In 2022 Microsoft observes that older vulnerabilities are still a primary driver in attacks.

Action

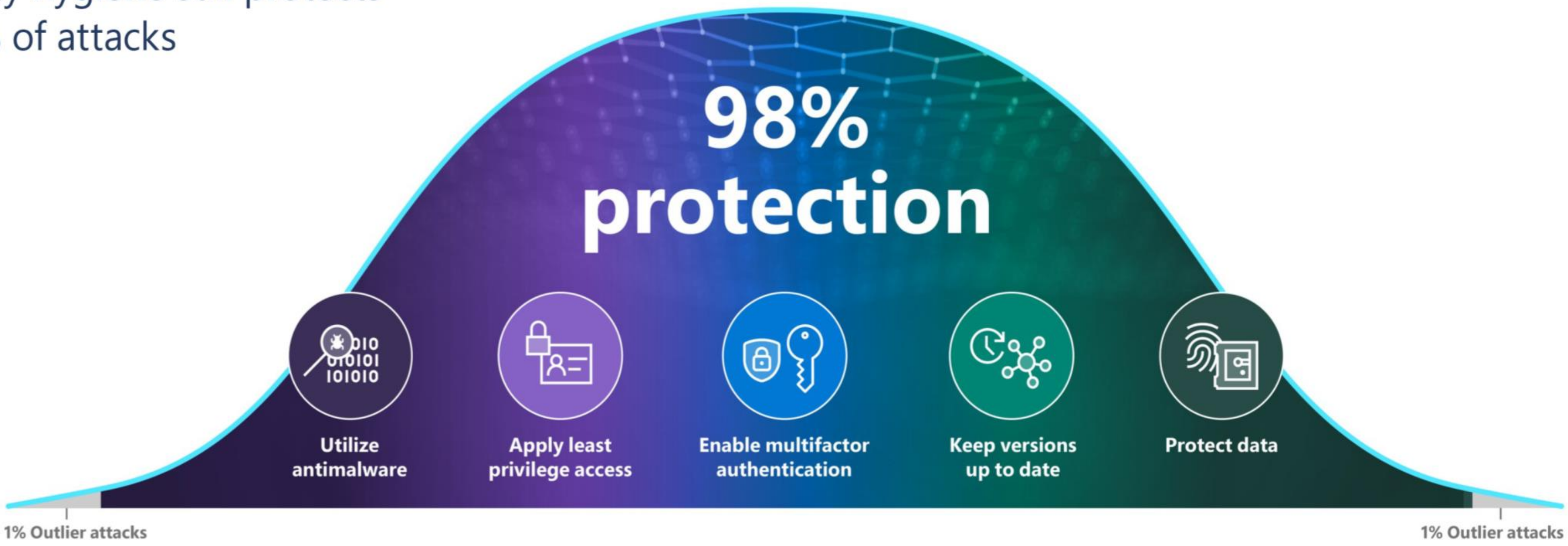
Keep systems up to date
Make software inventory a continuous process. Keep track of what you are running and prioritize support for these products. Use your ability to patch quickly and conclusively to gage where transitioning to cloud based services is beneficial.

Microsoft

Protecting against these threats

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

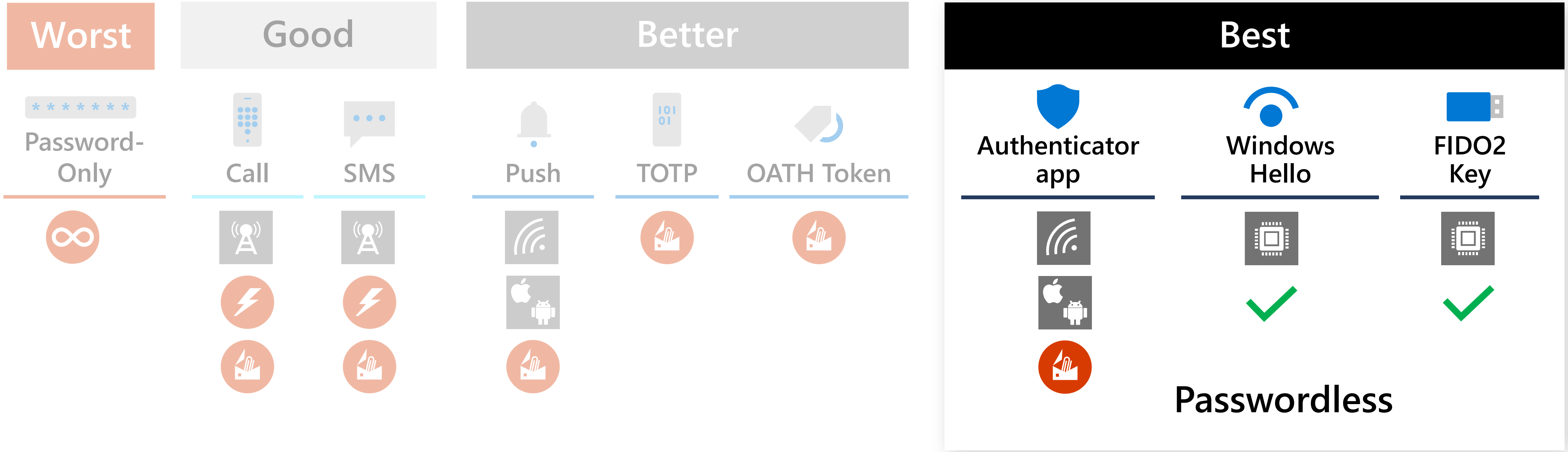
Stop malware attacks from executing by installing and enabling antimalware solutions on endpoints and devices. Utilize cloud-connected antimalware services for the most current and accurate detection capabilities.

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.

Strong Multi-Factor Authentication

The best options aren't that difficult



Worst

Password-Only

Good

Call

SMS

Better

Push

TOTP

OATH Token

Best

Authenticator app

Windows Hello

FIDO2 Key

Passwordless

Legend

■ Dependencies

● Risks

Phone Carrier

Channel Jacking

Wi-fi

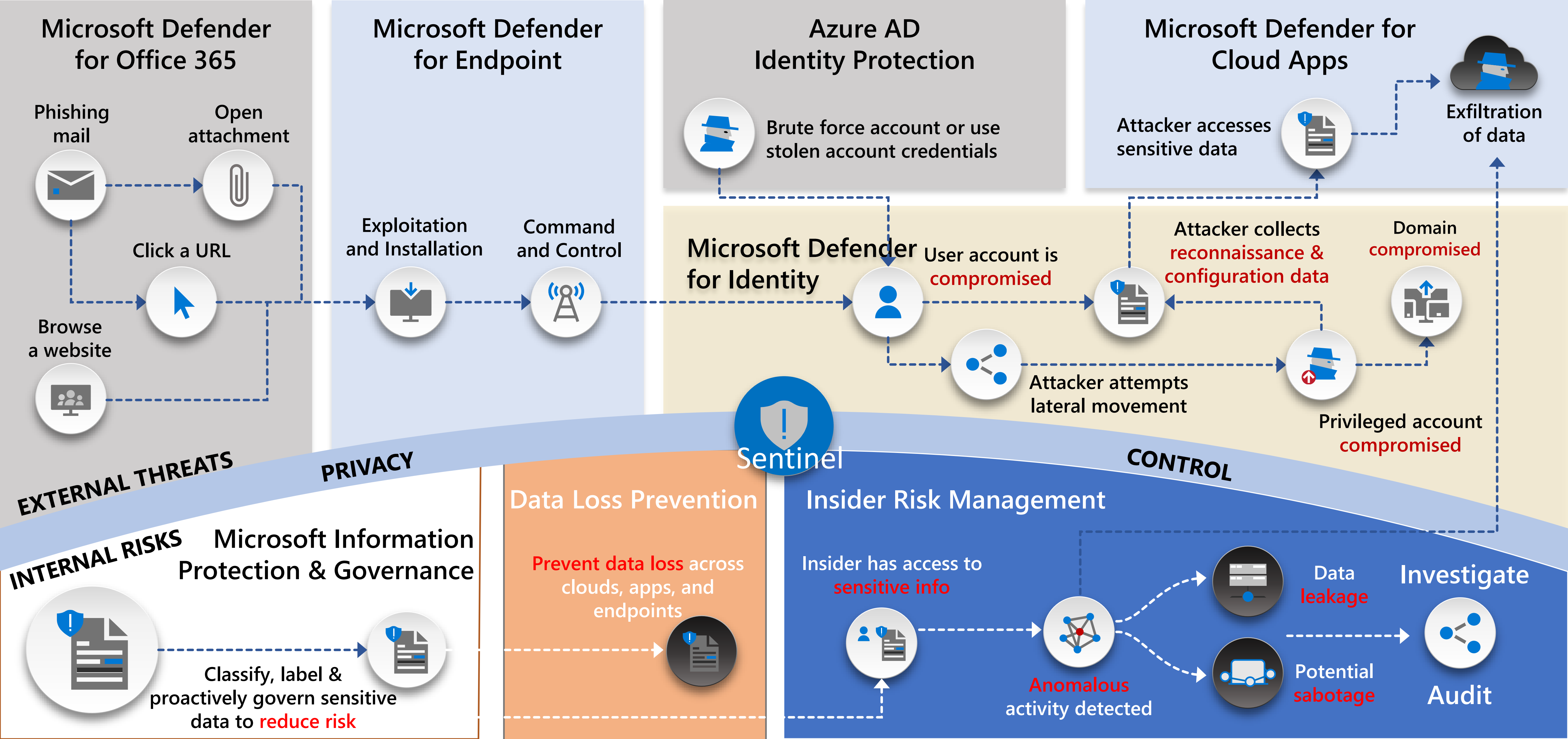
Real-time phishing

Mobile OS notifications

Hardware support required

✓ Only susceptible to hardware attacks

Threat Protection – Kill Chain process



Microsoft Defender for Office 365

Phishing mail

Open attachment

Click a URL

Browse a website

Microsoft Defender for Endpoint

Exploitation and Installation

Command and Control

Azure AD Identity Protection

Brute force account or use stolen account credentials

Microsoft Defender for Cloud Apps

Attacker accesses sensitive data

Exfiltration of data

Microsoft Defender for Identity

User account is compromised

Attacker collects reconnaissance & configuration data

Domain compromised

Attacker attempts lateral movement

Privileged account compromised

Sentinel

EXTERNAL THREATS

PRIVACY

CONTROL

INTERNAL RISKS

Microsoft Information Protection & Governance

Classify, label & proactively govern sensitive data to reduce risk

Data Loss Prevention

Prevent data loss across clouds, apps, and endpoints

Insider Risk Management

Insider has access to sensitive info

Anomalous activity detected

Data leakage

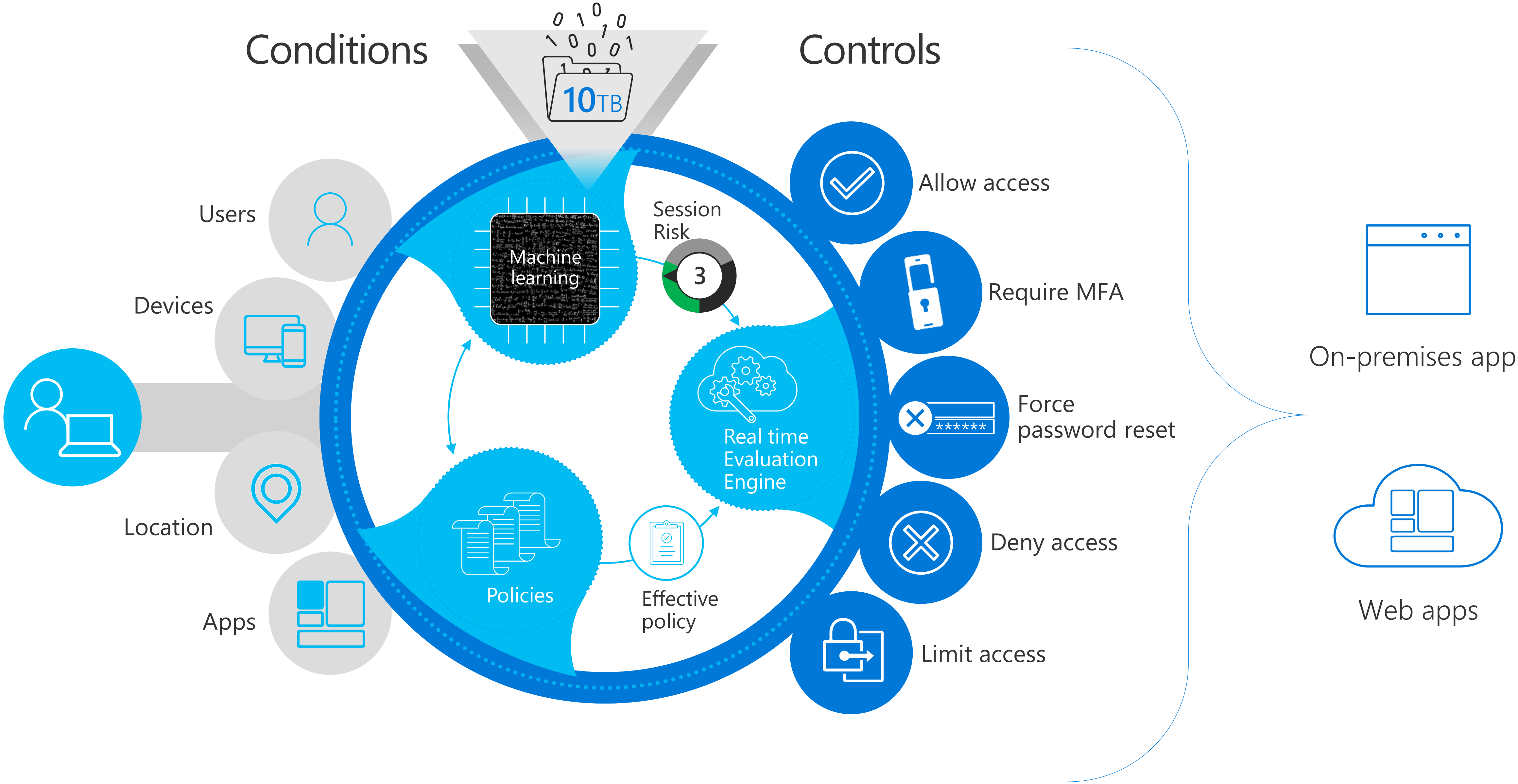
Potential sabotage

Investigate

Audit

Conditional Access

Protecting at the Front Door



Microsoft

Thank you

© 2022 Microsoft Corporation. All rights reserved.