



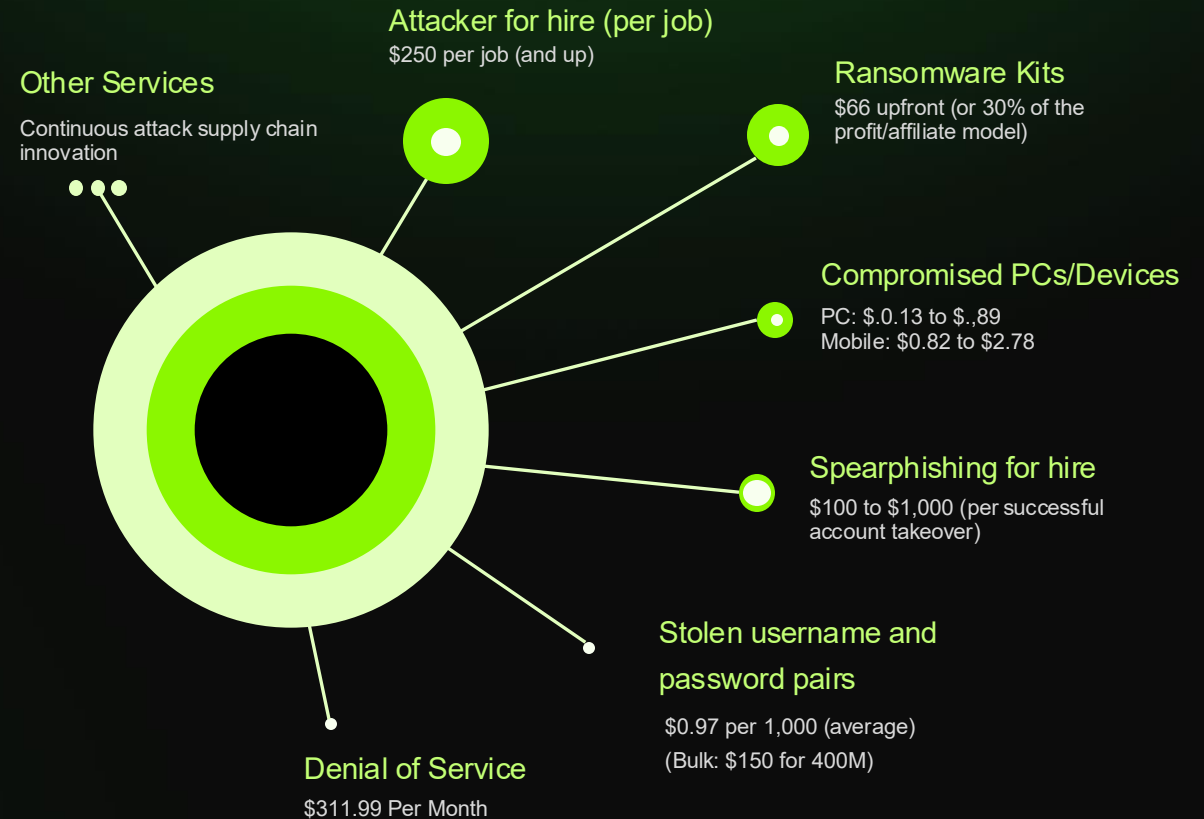
Trust But Verify



# The Threat Landscape Has Changed

It has never been cheaper or easier to breach administrator accounts. How do we use ID Verification to tackle the growing threat of bad actors like **Scattered Spider**

- It has never been cheaper to purchase usernames and Passwords
- 81% of hacking-related breaches use stolen or weak valid passwords (Verizon DBIR 2024)
- Over 60% of SMBs hit by cyberattacks go out of business within 6 months (Cybersecurity Ventures)
- 45% of help desk time is spent on identity issues (Roy Verberne)
- Compliance audits increased by 30% YoY in 2023/24 (Drata)



Microsoft Digital Defense Report 2023

# The Rise of AI Assisted Attacks

## What Happened

- In 2023 a 15-minute Social Engineering attack was launched by the Scattered Spider hacking group using AI Voice phishing to bypass security.

## Impact

- 70,000 Employees stopped from Working
- Thousands of clients could not check in or out
- Gambling and POS devices went down
- Total Financial Impact: Over \$100,000,000



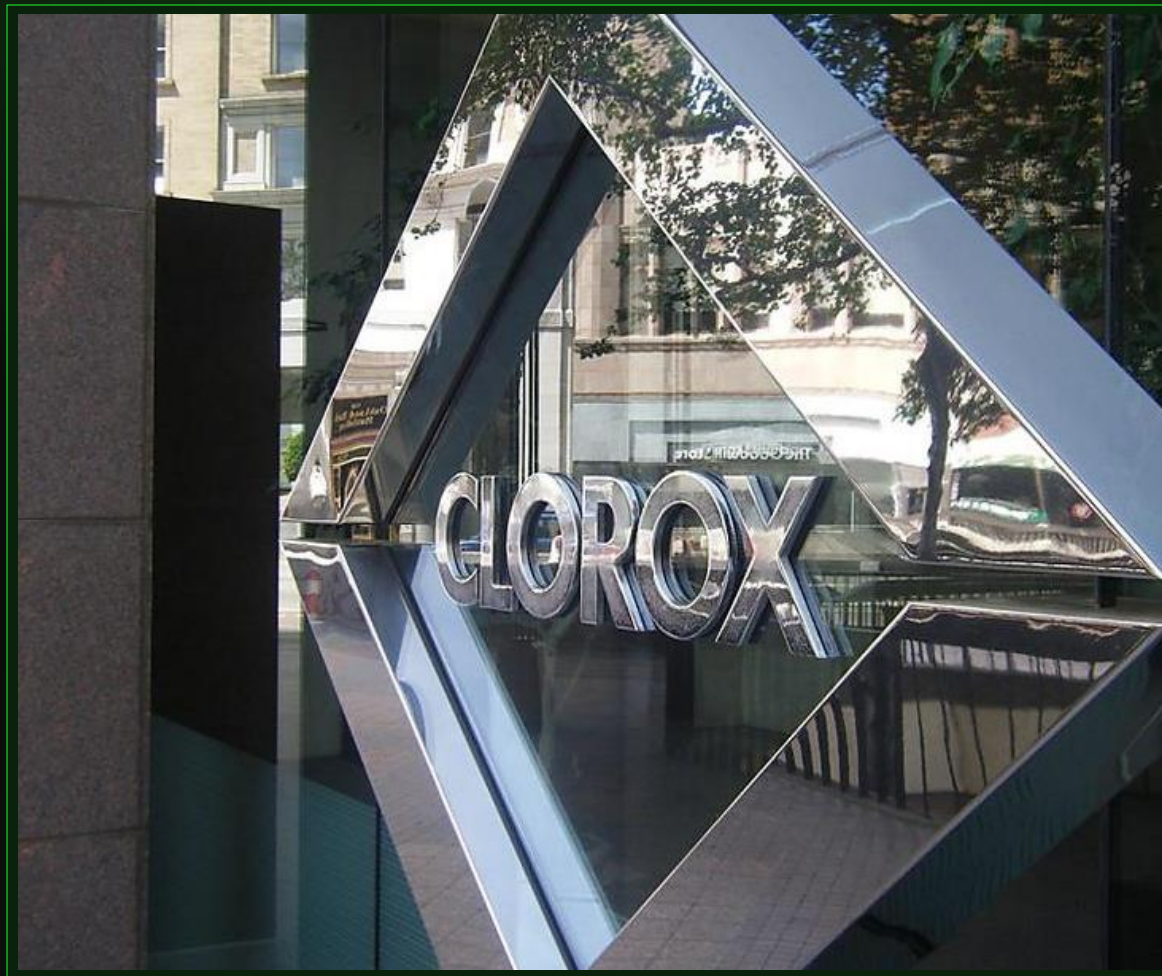
# Help Desk Exploitation

## What Happened

- August, 2023, Scattered Spider posed as Clorox employees who had "forgotten their passwords" support agents reset both login credentials and MFA, without verifying employee IDs

## Impact

- US \$380 million in total damages
- US \$50 million in remediation, forensic analysis
- Manufacturing and shipping operations halted
- Manual ordering procedures adopted, with products temporarily missing from store shelves



# Persistent Ransomware Attacks

## What Happened

- In 2025 DragonForce and Scattered Spider launched a Ransomware and advanced Social Engineering attack, leveraging phishing and SIM-swap calls to a third-party IT helpdesk

## Impact

- Estimated damages between £270m and £440m
- Online store was offline for ~7 weeks
- Food halls and clothing shops faced empty shelves due to automated stock systems being offline
- Lost Revenue Over £ 300,000,000



# Malicious Insider Attacks

## What Happened

- On May 10, 2023, Tesla discovered that two former employees had leaked a massive trove of internal data—about 100 GB across 23,000 files

## Impact

- 775,735 employees addresses, phone numbers, email and Social Security numbers
- Client bank details were leaked
- 2,400 vehicle acceleration complaints plus around 1,500 braking-related issues (like "phantom braking")—all from 2015–2022



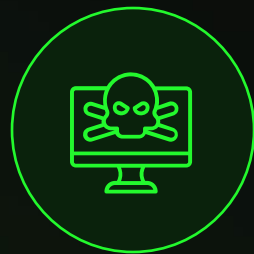
# Identity is the New Perimeter

Identity impersonation or abuse, is estimated to be the cause of over 90% of data breaches

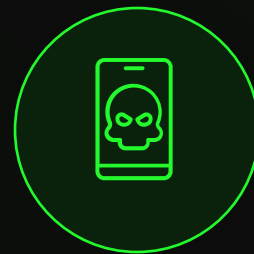
## Bad Actors With Admin Rights Can:



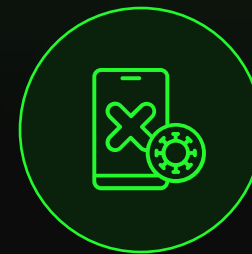
Disable Security  
Settings



Install Malicious  
software



Run  
Ransomware



Steal Sensitive  
information

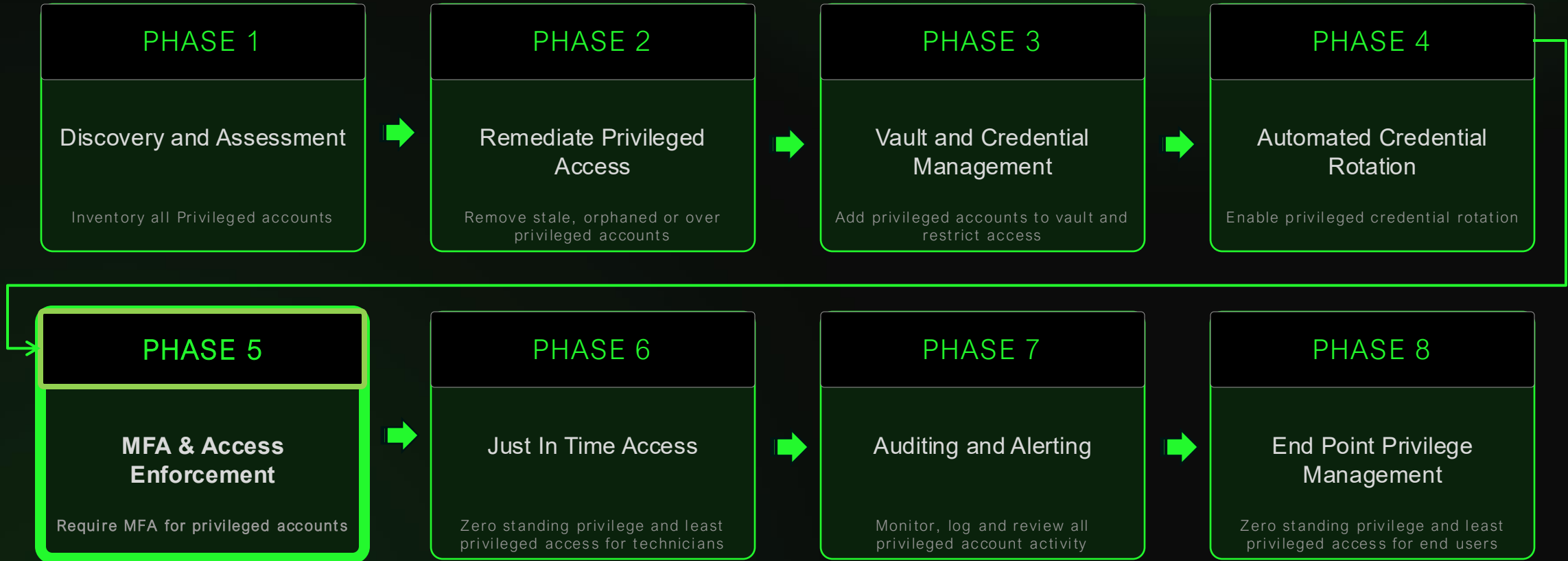


Weaponize  
systems against  
the organization

Restricting Admin rights can mitigate **94%** of Microsoft vulnerabilities

# Implement Zero Trust

## Phased Approach to Endpoint Privileged Management



# Identity Verification Could Have Prevented These Breaches

Select verification method

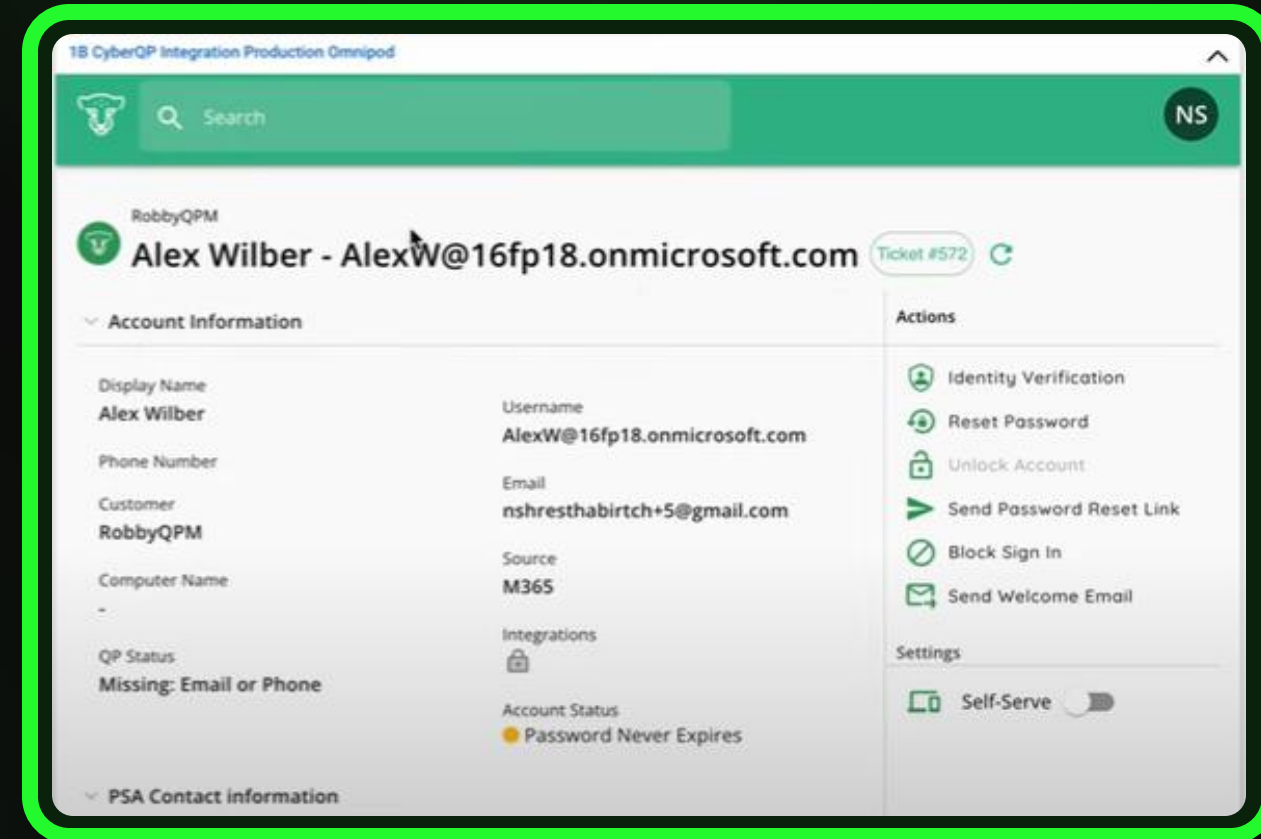
<p><b>SMS</b></p> <p>Select a phone number</p> <ul style="list-style-type: none"><li><input type="radio"/> 123123123 (CyberQP)</li><li><input type="radio"/> 123123123 (Work Telephone Number/Extension)</li><li><input type="radio"/> 456456456 (Work Mobile Number) <i>Preferred*</i></li></ul> <p><b>Send</b></p>	<p><b>Email</b></p> <p>Select an email</p> <ul style="list-style-type: none"><li><input type="radio"/> aaronw@acmecorp.com (CyberQP)</li><li><input type="radio"/> aaronw@acmecorp.com (Email) <i>Preferred*</i></li><li><input type="radio"/> aaronw@gmail.com (Email 2)</li></ul> <p><b>Send</b></p>	<p><b>Push Notification</b></p> <p>Select a notification type</p> <ul style="list-style-type: none"><li><input type="radio"/> Self-serve app</li><li><input type="radio"/> Self-serve app with verification code</li><li><input checked="" type="radio"/> MS Authenticator</li></ul> <p><b>Send</b></p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

# Identity Verification Fully Logged form the PSA

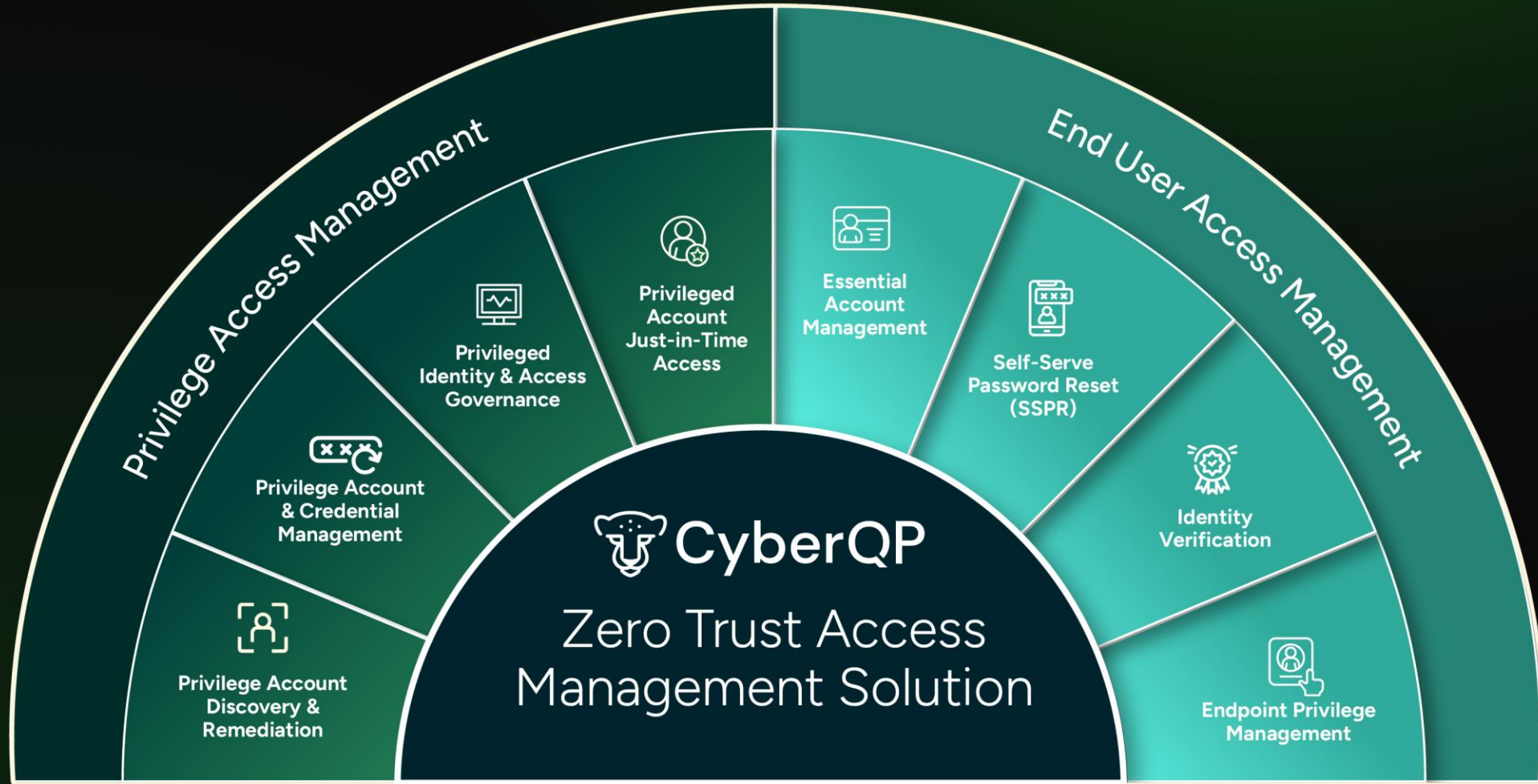
## Prevent Social Engineering & Impersonation Attacks:

Defend IT service desks against social engineering, impersonation, and insider threats that can lead to unauthorized access, data breaches, or privilege escalation.

Empower technicians with multiple options to verify end-user identities — including SMS, email, secure push notifications from a branded mobile app, or Microsoft Authenticator



# CyberQP Platform



# Identity Verification Considerations

## THE WHY

- 1. Trust But Verify** – Even if you think you know your clients.
  - Log ID Verification for all users on all tickets
- 2. Leverage existing workflows** – Like MS Auth or SMS
  - Reduce Training Time and increase adoption
- 3. NIST 800-63 A: Identity Assurance Levels (IALs) 3**
- 4. CMMC IA controls** – Required for Level 2 + 3
  - Meet insurance requirements and stay compliant.
- 5. Reduce Risk** – of breach by over 90%
  - Enforce Access Management and MFA
- 6. Log all interactions** – Record all user identities are valid directly in the PSA or via reports

## THE HOW

- 1. Train Every User:** Every user should be trained on how to interact with the Help Desk. Save time and training by leveraging existing tools and workflows
- 2. No ID, No work, No Exceptions:** Having ID verification in place is the start, but to get the value and protecting your environments you need to enforce ID Verification on every interaction.
- 3. Verify Techs and End-users:** The same way a technician can ask to verify an ID an end user can ask the Tech to verify they are who they say they are too.
- 4. Log ID Verification on Every Ticket:** Have proof for your insurance paperwork, incident response plan or compliance check list.

THE LANDSCAPE  
HAS CHANGED

HOW WE PROTECT  
YOUR BUSINESS

CYBERQP PLATFORM

SECURITY THROUGH SIMPLICITY

GETTING STARTED

# Ready to Improve Your Security?

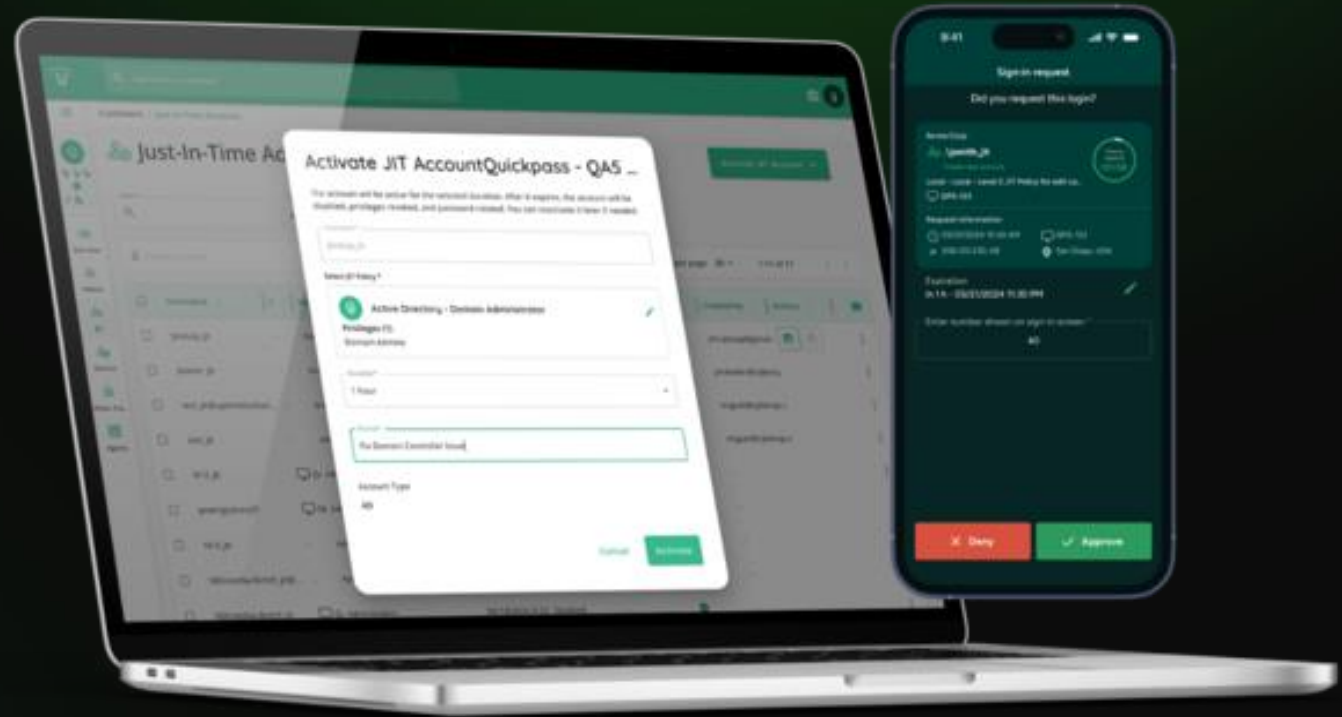
Let's protect your business by taking control of  
Privileged Access and Identity Automation

**End User Identity  
Verification**

**Just In Time  
Technician Access**

**End User Privilege  
Management**

**Self-Serve Password  
Reset / Essential  
Account Management**



## Come see us at our booth!

# Thank You

