BeyondTrust

Support & Empower a Hybrid Workforce with Universal Privilege Management

Paul Davies
Senior Solutions Architect

Agenda

- **CISO considerations** for a changing workforce & the security impact of a rapid transition

- **Next Normal**: Implement & scale strong security protocols to enable a hybrid workforce

- **Universal Privilege Management** - Securing every privilege, every time

Agility & Adaptability

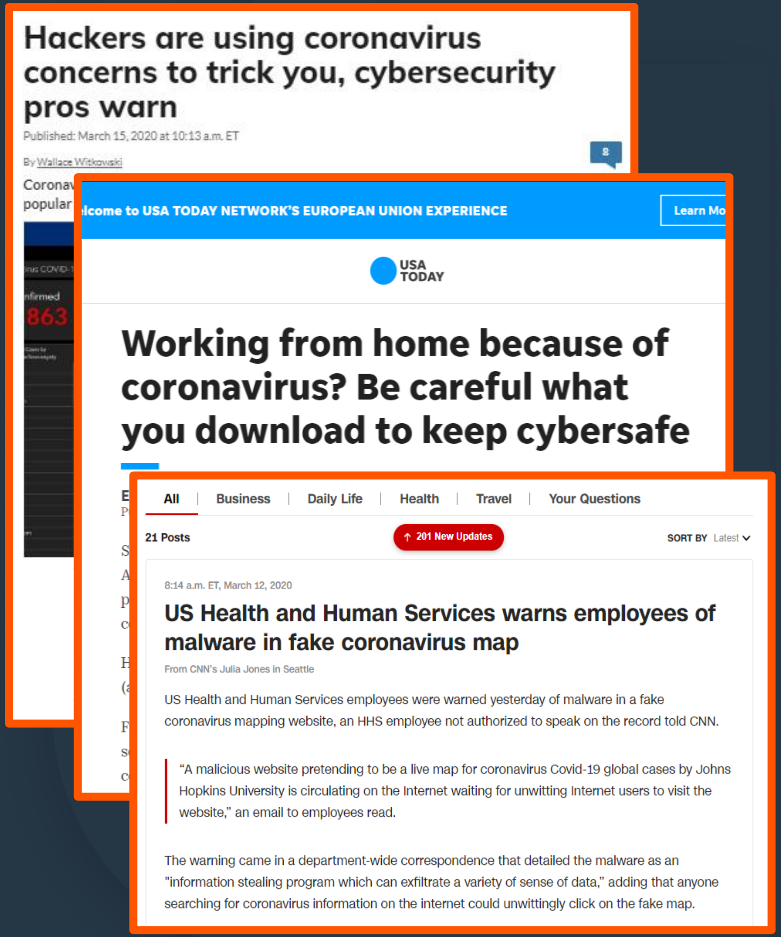
tactical responses during a challenging period

- VPN requirements went from 25k to 150k overnight
- Workarounds required to support patching & updating
- IT working 24/7 to issue devices and MFA tokens
- Accelerated deployment plans, including cloud
- Forced security policy and practice reviews & changes
- IT working 24/7 to issue devices and MFA tokens
- Security of Remote Working & Collaboration Tools
- Moved from defending lines to defending dots

https://www.controlrisks.com/our-thinking/insights/covid-19-and-remote-working

Agility & Adaptability

is not just for enterprises



Hackers are using coronavirus concerns to trick you, cybersecurity pros warn

Published: March 15, 2020 at 10:13 a.m. ET

By Wallace Witkowski

Coronav
popular

lcome to USA TODAY NETWORK'S EUROPEAN UNION EXPERIENCE Learn Mo

USA TODAY

Working from home because of coronavirus? Be careful what you download to keep cybersafe

All | Business | Daily Life | Health | Travel | Your Questions
21 Posts
↑ 201 New Updates
SORT BY Latest

8:14 a.m. ET, March 12, 2020

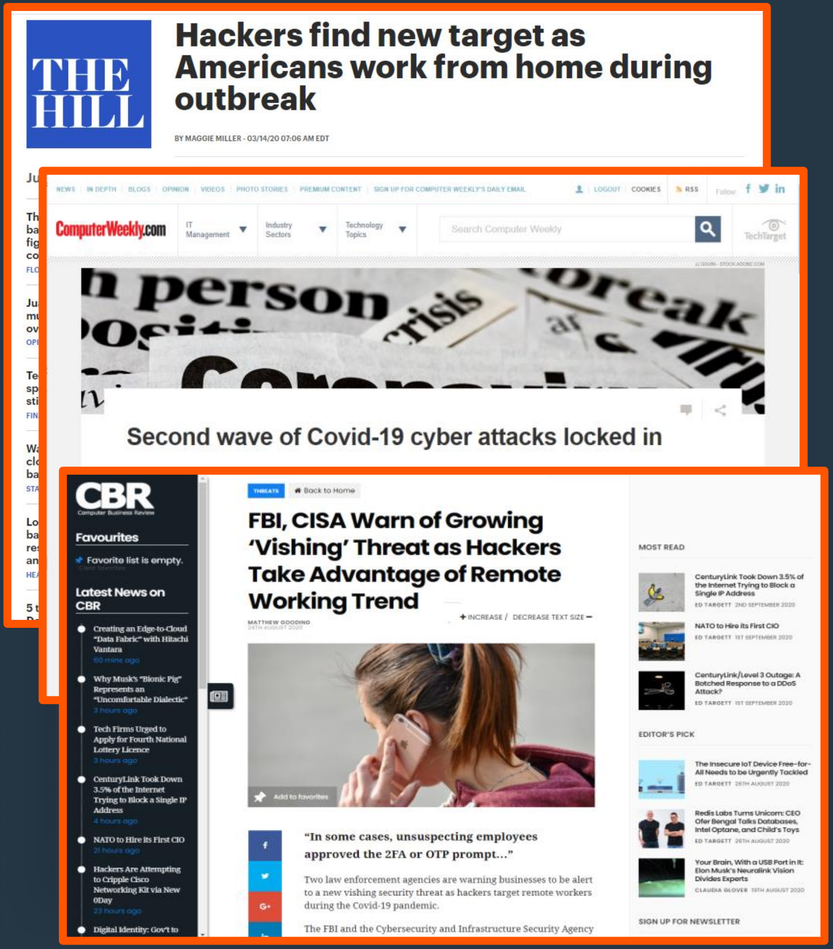
US Health and Human Services warns employees of malware in fake coronavirus map

From CNN's Julia Jones in Seattle

US Health and Human Services employees were warned yesterday of malware in a fake coronavirus mapping website, an HHS employee not authorized to speak on the record told CNN.

> "A malicious website pretending to be a live map for coronavirus Covid-19 global cases by Johns Hopkins University is circulating on the Internet waiting for unwitting Internet users to visit the website," an email to employees read.

The warning came in a department-wide correspondence that detailed the malware as an "information stealing program which can exfiltrate a variety of sense of data," adding that anyone searching for coronavirus information on the internet could unwittingly click on the fake map.



THE HILL

Hackers find new target as Americans work from home during outbreak

BY MAGGIE MILLER - 03/14/20 07:06 AM EDT

NEWS | IN DEPTH | BLOGS | OPINION | VIDEOS | PHOTO STORIES | PREMIUM CONTENT | SIGN UP FOR COMPUTER WEEKLY'S DAILY EMAIL | LOGOUT | COOKIES | RSS | Follow
ComputerWeekly.com
IT Management
Industry Sectors
Technology Topics
Search Computer Weekly
TechTarget

Second wave of Covid-19 cyber attacks locked in

CBR Computer Business Review
Favourites
Favorite list is empty.
THREATS
Back to Home
+ INCREASE / DECREASE TEXT SIZE −
Add to favorites

Latest News on CBR

- Creating an Edge-to-Cloud "Data Fabric" with Hitachi Vantara — 60 mins ago
- Why Musk's "Bionic Pig" Represents an "Uncomfortable Dialectic" — 3 hours ago
- Tech Firms Urged to Apply for Fourth National Lottery Licence — 3 hours ago
- CenturyLink Took Down 3.5% of the Internet Trying to Block a Single IP Address — 4 hours ago
- NATO to Hire its First CIO — 21 hours ago
- Hackers Are Attempting to Cripple Cisco Networking Kit via New 0Day — 23 hours ago
- Digital Identity: Gov't to

FBI, CISA Warn of Growing 'Vishing' Threat as Hackers Take Advantage of Remote Working Trend

MATTHEW GOODING
24TH AUGUST 2020

"In some cases, unsuspecting employees approved the 2FA or OTP prompt..."

Two law enforcement agencies are warning businesses to be alert to a new vishing security threat as hackers target remote workers during the Covid-19 pandemic.

The FBI and the Cybersecurity and Infrastructure Security Agency

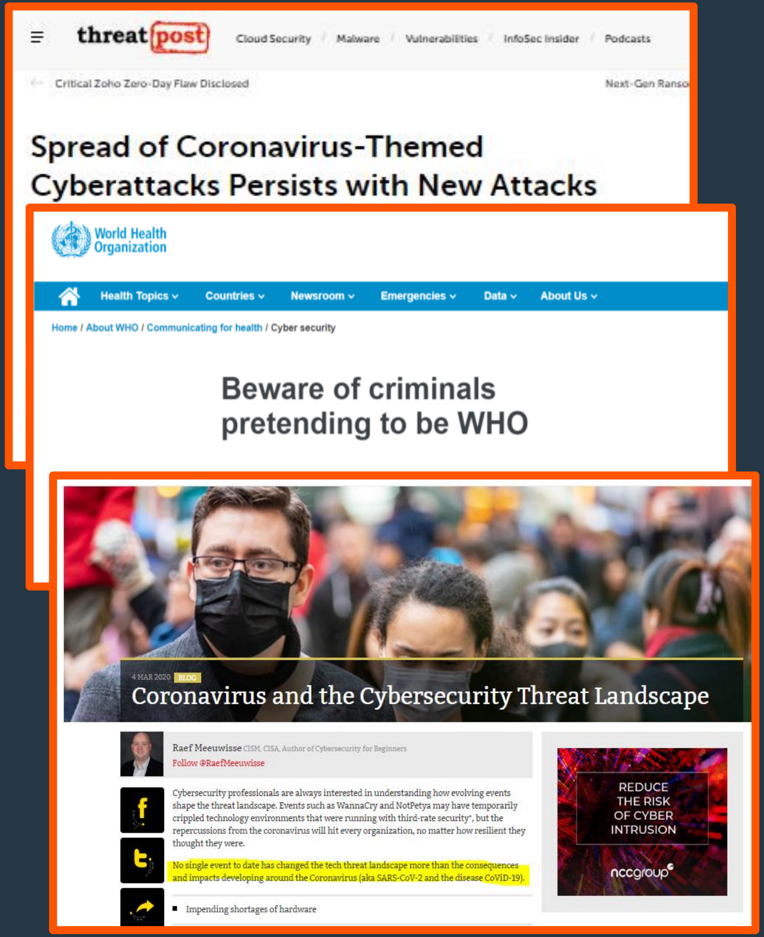
MOST READ

- CenturyLink Took Down 3.5% of the Internet Trying to Block a Single IP Address — ED TARGETT 2ND SEPTEMBER 2020
- NATO to Hire its First CIO — ED TARGETT 1ST SEPTEMBER 2020
- CenturyLink/Level 3 Outage: A Botched Response to a DDoS Attack? — ED TARGETT 1ST SEPTEMBER 2020

EDITOR'S PICK

- The Insecure IoT Device Free-for-All Needs to be Urgently Tackled — ED TARGETT 26TH AUGUST 2020
- Redis Labs Turns Unicorn: CEO Ofer Bengal Talks Databases, Intel Optane, and Child's Toys — ED TARGETT 26TH AUGUST 2020
- Your Brain, With a USB Port in It: Elon Musk's Neuralink Vision Divides Experts — CLAUDIA GLOVER 19TH AUGUST 2020

SIGN UP FOR NEWSLETTER



threatpost
Cloud Security / Malware / Vulnerabilities / InfoSec Insider / Podcasts
Critical Zoho Zero-Day Flaw Disclosed
Next-Gen Ranso

Spread of Coronavirus-Themed Cyberattacks Persists with New Attacks

World Health Organization
Health Topics
Countries
Newsroom
Emergencies
Data
About Us

Home / About WHO / Communicating for health / Cyber security

Beware of criminals pretending to be WHO

4 MAR 2020 BLOG

Coronavirus and the Cybersecurity Threat Landscape

Raef Meeuwisse CISM, CISA, Author of Cybersecurity for Beginners
Follow @RaefMeeuwisse

Cybersecurity professionals are always interested in understanding how evolving events shape the threat landscape. Events such as WannaCry and NotPetya may have temporarily crippled technology environments that were running with third-rate security*, but the repercussions from the coronavirus will hit every organization, no matter how resilient they thought they were.

No single event to date has changed the tech threat landscape more than the consequences and impacts developing around the Coronavirus (aka SARS-CoV-2 and the disease CoViD-19).

- Impending shortages of hardware

https://www.infosecurity-magazine.com/news/businesses-covid-attack/

Agility & Adaptability

is not just for enterprises

416 Security & 425 Business Executives Surveyed

41% Experienced COVID Related Cyber-Attack

94% Experienced Cyber-Attack during last 12 months

Individuals, corporate IT, ICS & OT systems all targeted

Subject and scale change, but users are still the focus

https://www.infosecurity-magazine.com/news/businesses-covid-attack/

Agility & Adaptability

Is not without risk

‘Zerologon’ CVE-2020-1472

- Elevation of Privilege (EoP) Vulnerability
- CVSSv3 Score: 10/10
- Allows any attacker on the local network to completely compromise a Windows Domain
- Patched on August 11, 2020
- Seen in multiple active Ransomware campaigns via fake updates & those targeting SSL VPN vulnerabilities

https://www.secura.com/pathtoimg.php?id=2055
https://www.darkreading.com/threat-intelligence/critical-zerologon-flaw-exploited-in-ta505-attacks/d/d-id/1339141

Poll Question

1. What % of your users are currently working remotely?

   a) 0-10%

   b) 11-50%

   c) 51-99%

   d) 100%

   e) Unknown

CISO considerations for a changing workforce & the security impact of a rapid transition

CISO Considerations

for a changing workforce & the security impact of a rapid transition

- **Remote Access** is the #1 attack pathway
- **BYOD & Shadow IT**: Unmanaged devices, unknown services, insecure tools
- **Unmanaged credentials** are hard to control and increase risk
- **Challenges of Compliance**
- Choose solutions that don’t require large IT teams/timelines to implement
- Focus on rapid, efficient, non-intrusive additions to your existing cybersecurity tooling
- Enable your workforce, don’t hinder them working

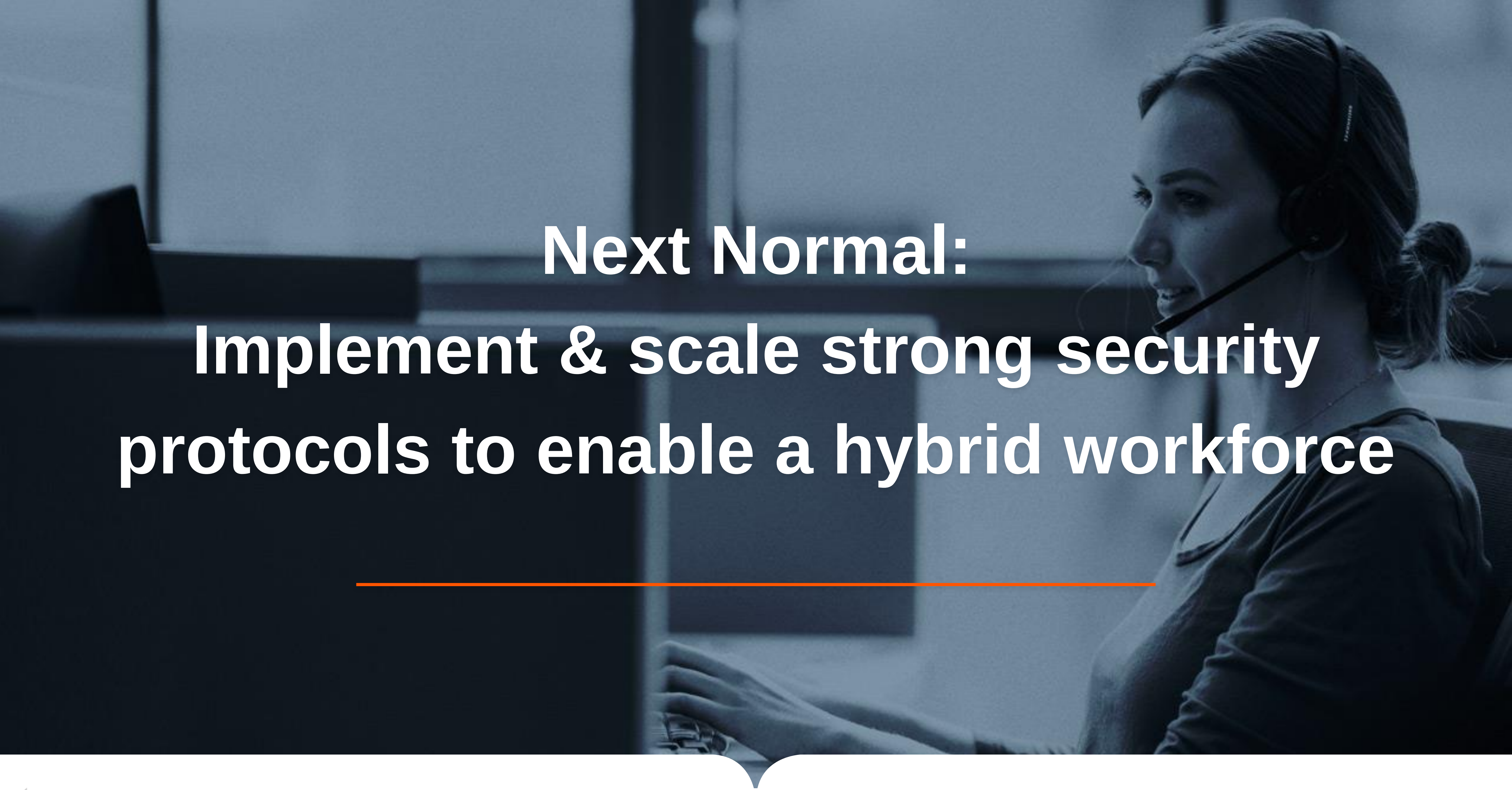
Poll Question

2. What are your organisations plans for the work force over the next 3 months?

a) Full return to pre-lockdown working environment

b) Hybrid blend of remote and in ‘office’ working

c) No return to the ‘office’ planned



Next Normal:
Implement & scale strong security protocols to enable a hybrid workforce

Enable Hybrid Workers

allowing them to work effectively from anywhere without compromising security

RECOMMENDATION	SOLUTION	
Store and manage privileged credentials centrally	Privileged Account & Session management	✓
Efficiently limit and monitor access to systems, applications & privileges	Secure Remote Access & Privilege Management	✓
Mitigate the risk of Shadow IT & Insecure Tool Usage	Consolidate to a single, secure & scalable remote access solution	✓
Monitor for Audit & Compliance	Integrated solutions, centralized management, session recording	✓

Take Control of Credentials

Store and manage privileged credentials centrally

- **Automate discovery and management** of privileged accounts
- **Sessions are automatically managed** by the remote access solution
- **Role and attribute-based access** enable the correct privileged credentials to be automatically injected into the session
- **No privileged credentials**, need to leave the organization, and be typed in
- **Credential rotation** can be automated, including after every use to limit

Reduce the Attack Surface

Replace "All Or Nothing" Access With Granular Levels Of Permissions

- **Enforce least privilege** by giving users just the right level of access for their roles
  - Includes defining which endpoints users can access, and when
  - Password-less & Just-in-Time Privilege (JIT) management
- **Restrict unapproved protocols** and limit approved sessions to a predefined route
  - Most external users or vendors only need access to very specific systems
- **Consolidate tracking, approval, and auditing** of privileged accounts
  - Review access, usage and management and in one place

Consolidate Solutions

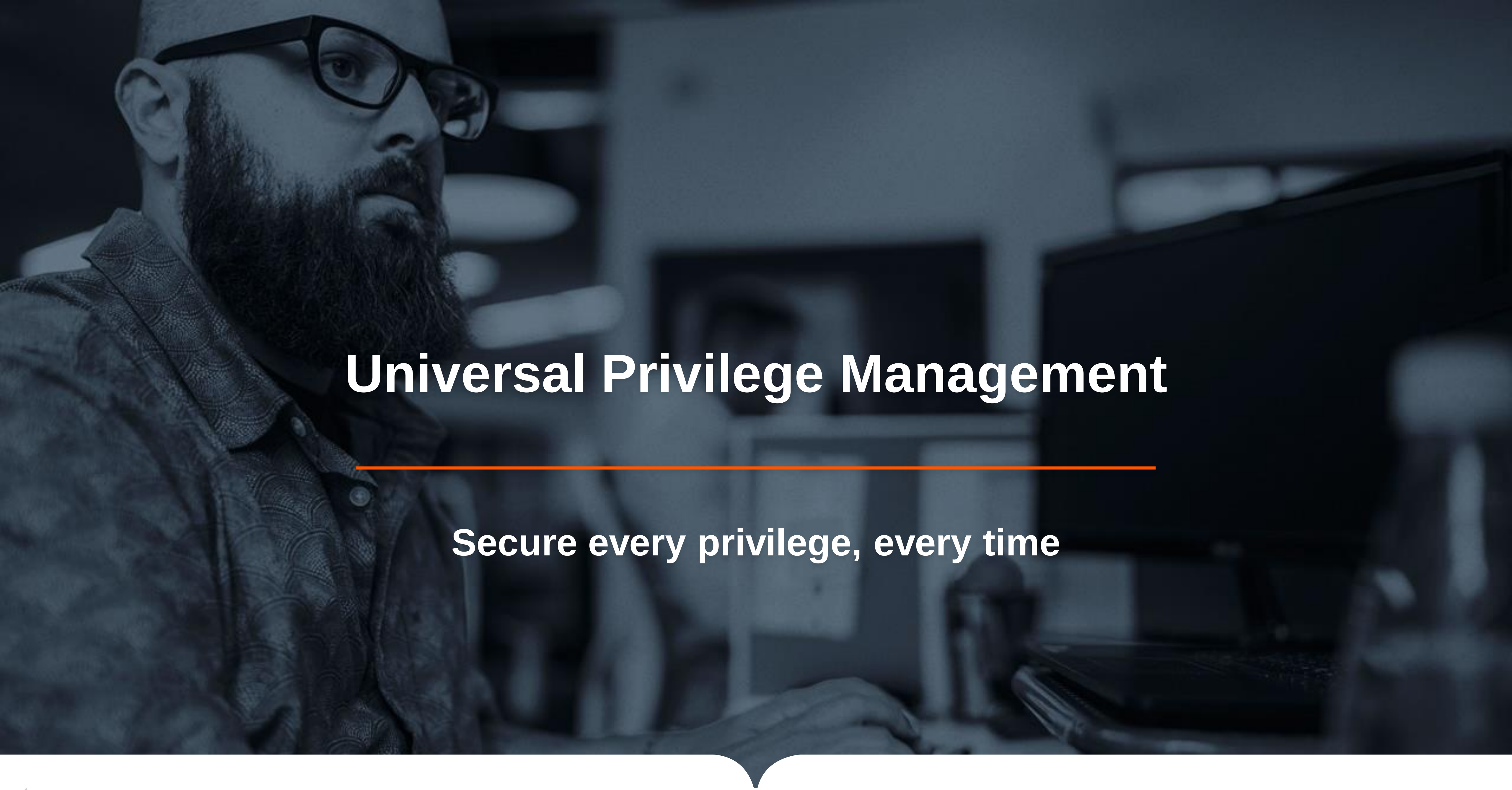
increase security by minimizing the attack surface whilst enabling productivity

- **Drive Efficiency -** Enable your IT teams, service desk and users to be more efficient, effective and enabled to operate in a more diverse range of situations
- **Maximize Existing Investments -** Utilize out-of-the-box integrations with a ITSM solutions and automate more using APIs and Software Development Kits
- **Reduce Costs -** Eliminate overlapping costs and address the hidden costs of insecure tools and workarounds
- **Achieve Compliance -** Create audit trails, with every session and credential use logged, with a central repository view of remote access activity

Compliance as an outcome

identify and record the “who, what, where, and when” for access activities

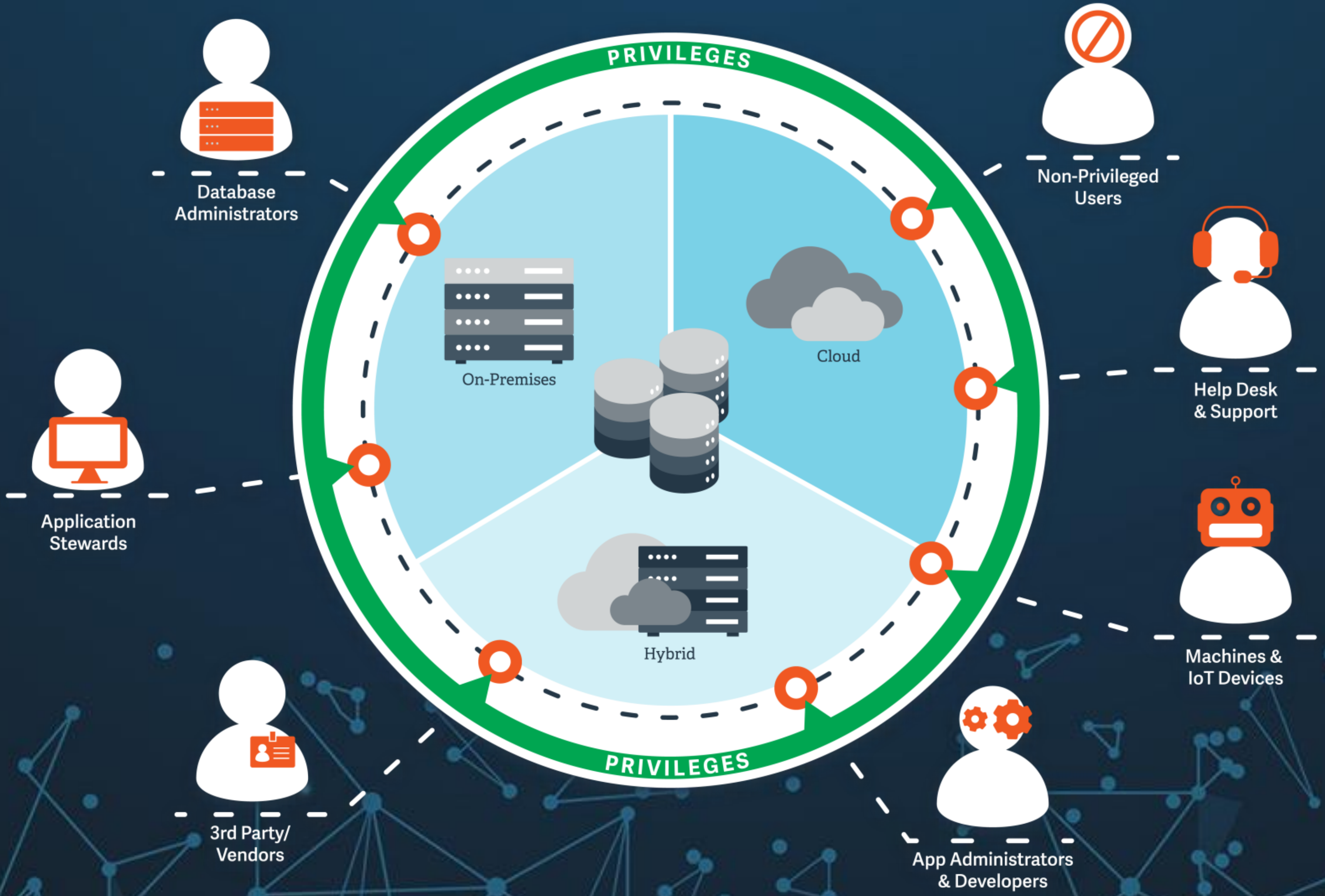
- Compliance requirements are often categorized into three primary purposes: to **protect, control, and audit** the use of IT resources and the sensitive data they contain
- **Secure Remote Access** solutions should include features to enable these requirements:
  - Assign all users a unique ID before allowing them to access critical systems and data and control the addition, deletion and modification of those IDs and credentials.
    (CIS, PCI, NIST, HIPPA, GDPR)
  - Track, control, prevent, and correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.
    (CIS, PCI, NIST, HIPPA, GDPR)
  - Implement only one primary function per server and enable only necessary service, protocols, daemons etc. as required for the function of the system.
    (PCI, CIS)



Universal Privilege Management

Secure every privilege, every time

The number of privileged users is growing rapidly



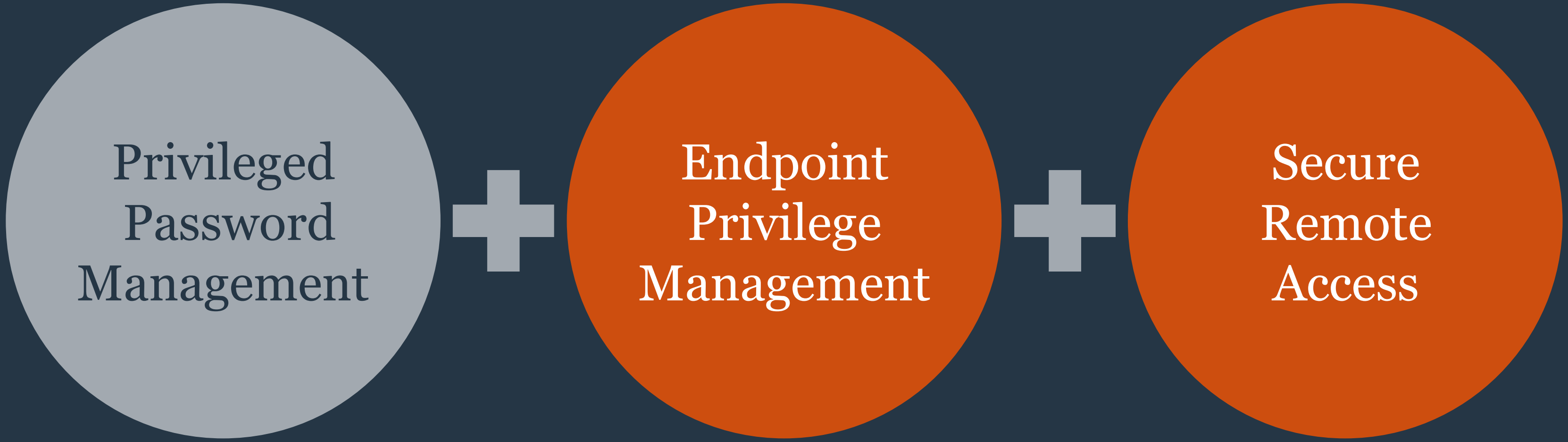
New era brings new problems

How do I…

- Eliminate non-essential admin accounts?
- Discover all privileged accounts across my enterprise?
- Block non-compliant and malicious software?
- Know what vendors are doing in my network?
- Apply least-privilege best practices?
- Remove root access from servers?
- Integrate privilege controls with change management workflows?
- Secure all privileged credentials in my network?
- Pass my compliance audits?
- Integrate privilege controls with ITSM workflows?

UNIVERSAL PRIVILEGE MANAGEMENT

Secures & manages privileges across every user, session & asset…



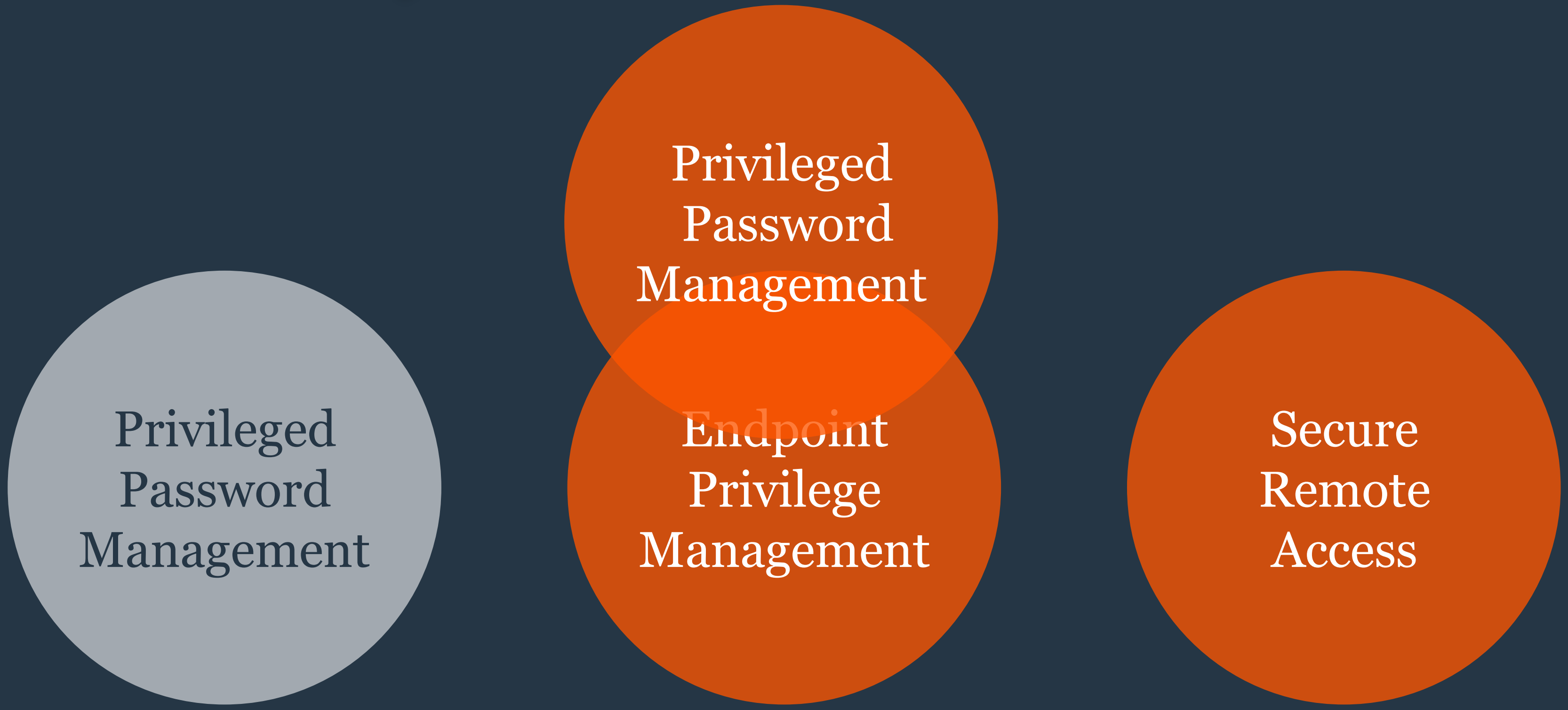
Privileged Password Management

Endpoint Privilege Management

Secure Remote Access

UNIVERSAL PRIVILEGE MANAGEMENT

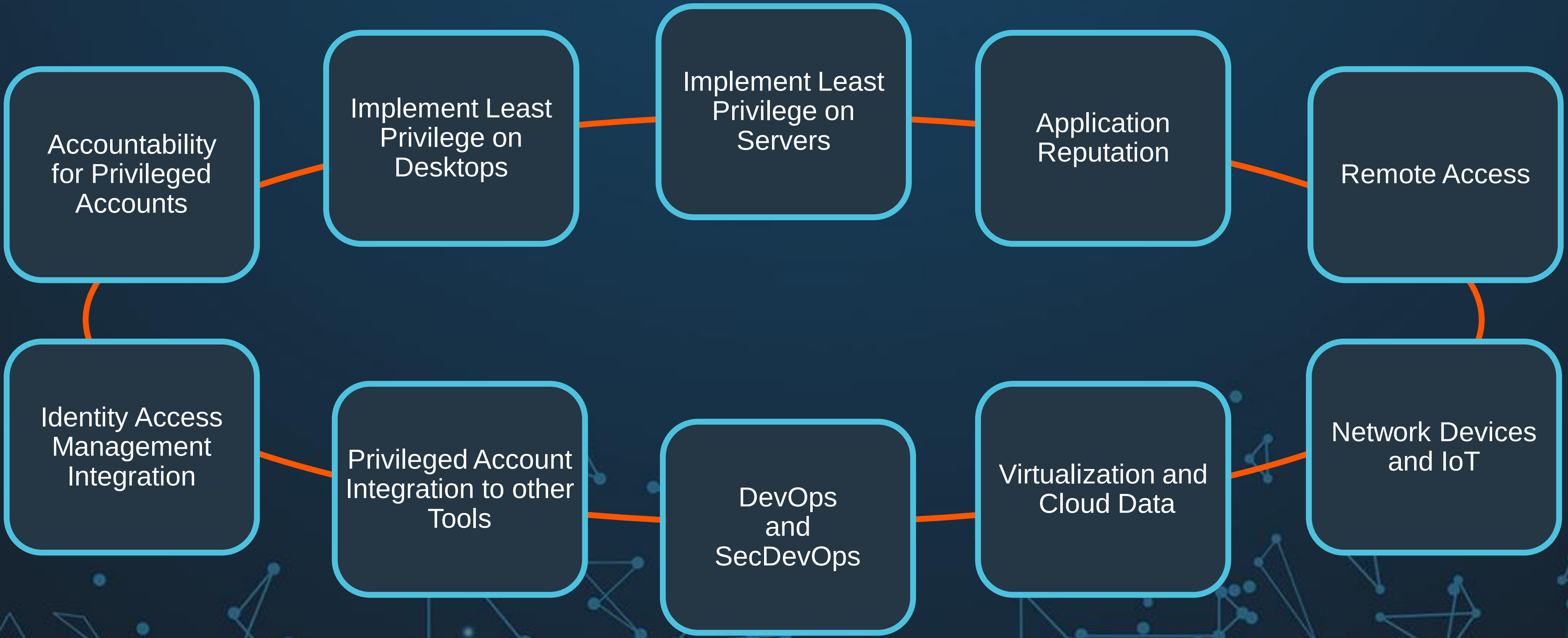
And unifies your entire privilege universe to drastically reduce the attack surface



Privileged Password Management
Privileged Password Management
Endpoint Privilege Management
Secure Remote Access

The Path to Universal Privilege Management

QUICKLY SOLVE FOR A VARIETY OF USE CASES



Accountability for Privileged Accounts

Implement Least Privilege on Desktops

Implement Least Privilege on Servers

Application Reputation

Remote Access

Network Devices and IoT

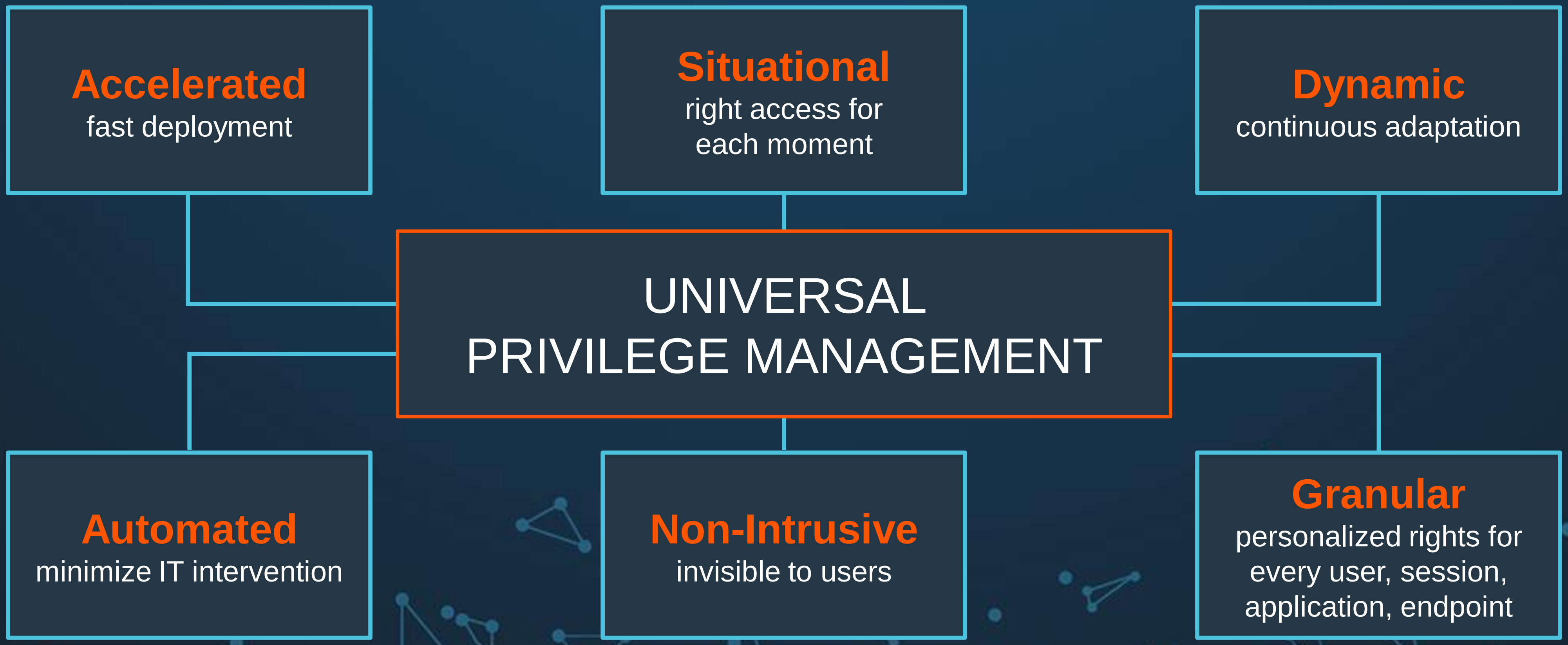
Virtualization and Cloud Data

DevOps and SecDevOps

Privileged Account Integration to other Tools

Identity Access Management Integration

Fast Security and Productivity Gains



Accelerated
fast deployment

Situational
right access for
each moment

Dynamic
continuous adaptation

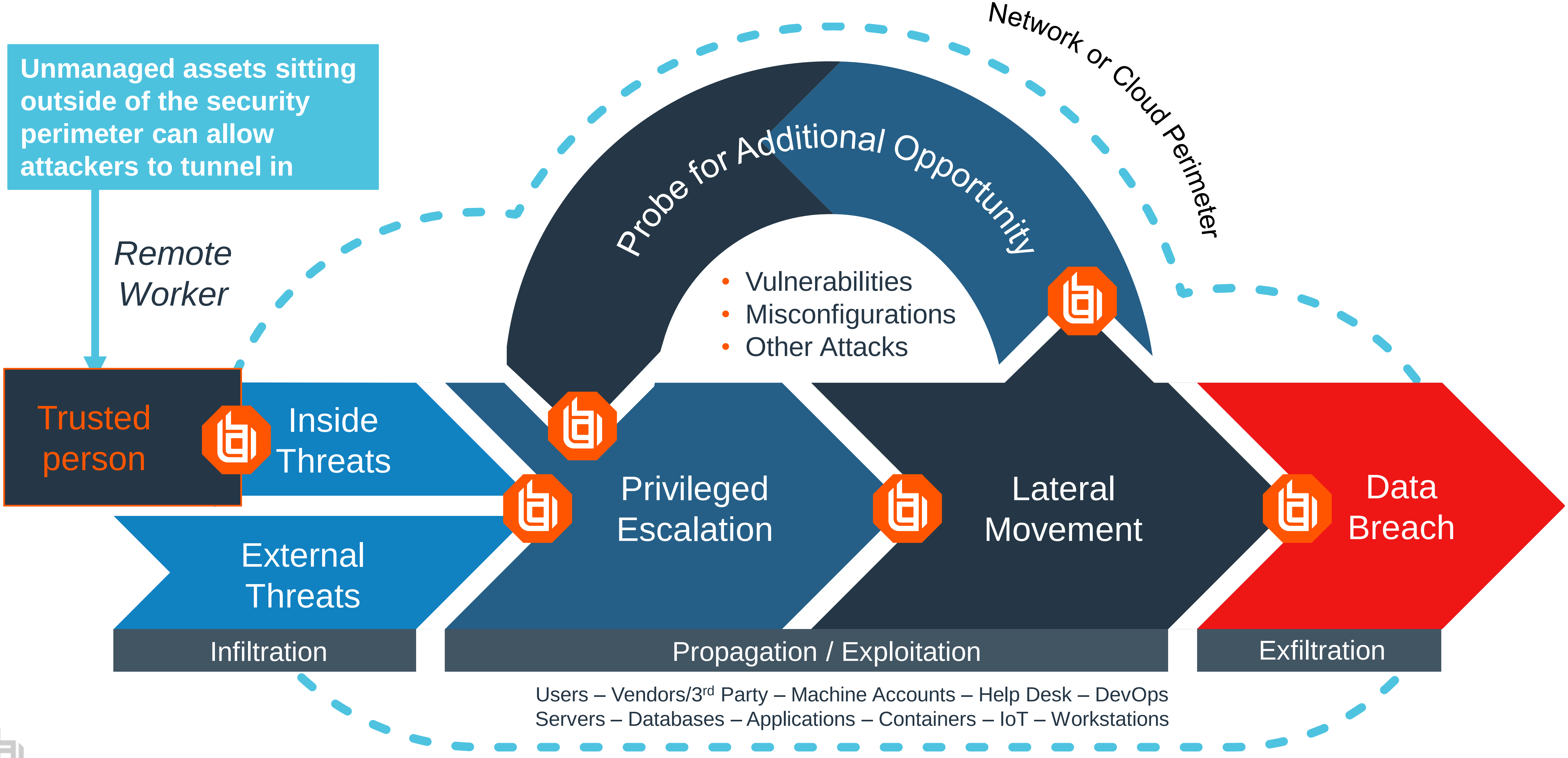
UNIVERSAL
PRIVILEGE MANAGEMENT

Automated
minimize IT intervention

Non-Intrusive
invisible to users

Granular
personalized rights for
every user, session,
application, endpoint

The Attack Chain & Hybrid Workers



Unmanaged assets sitting outside of the security perimeter can allow attackers to tunnel in

Remote Worker
Trusted person
Network or Cloud Perimeter
Probe for Additional Opportunity
Vulnerabilities
Misconfigurations
Other Attacks
Inside Threats
External Threats
Privileged Escalation
Lateral Movement
Data Breach
Infiltration
Propagation / Exploitation
Exfiltration
Users – Vendors/3rd Party – Machine Accounts – Help Desk – DevOps
Servers – Databases – Applications – Containers – IoT – Workstations

BeyondTrust

UNIVERSAL PRIVILEGE MANAGEMENT

The BeyondTrust Solution

DISCOVERY • THREAT ANALYTICS • REPORTING • CONNECTORS • CENTRAL POLICY & MANAGEMENT

PRIVILEGED PASSWORD MANAGEMENT

Discover, manage, audit, and monitor privileged accounts and sessions of all types

ENDPOINT PRIVILEGE MANAGEMENT

Remove excessive end user privileges on Windows, Mac, Unix, Linux and network devices

SECURE REMOTE ACCESS

Secure, manage, and audit remote privileged access sessions for vendors, admins and the service desk

BEYONDINSIGHT PLATFORM

Maximize visibility, simplify deployment, automate tasks, improve security and reduce privilege-related risks with the industry's most innovative and comprehensive privileged access management platform

ON-PREMISE — CLOUD — HYBRID

Thank You & Questions