



ITC CYBER SUMMIT 2024

Addressing the biggest trends in cyber security

Faster Future: Amplify Your Defences in the Age of AI

Sponsored by:



CYBSAFE



SILVERFORT

Supported by:



Microsoft



Welcome

Mark Weait

Chief Revenue Officer
ITC Secure



CEO Address

Arno Robbertse

Chief Executive
ITC Secure



The State of the Nation

Lt. Gen. Sir Graeme Lamb

KBE, CMG, DSO



Building a Faster Future

Mark Weait

Chief Revenue Officer
ITC Secure

CURRENT CHALLENGES

Economic



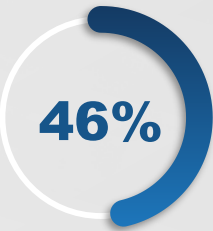
Extreme weather

Environmental



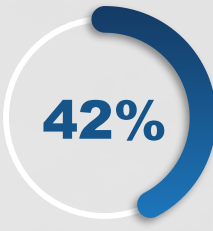
AI-generated misinformation and disinformation

Geopolitical



Societal and / or political polarisation

Societal



Cost-of-living crisis

Technological



Cyber attacks

Source: World Economic Forum Global Risks | Perception Survey 2023-2024

The world needs
cyber security experts

35%

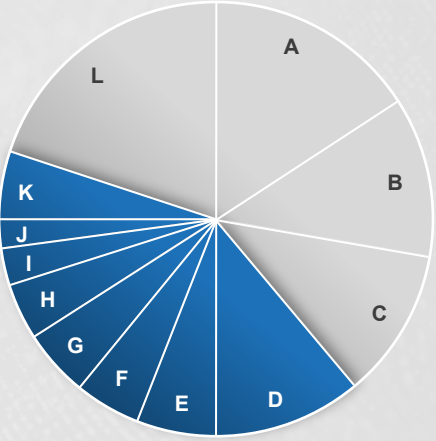
increase in demand for
cyber security experts
over the past year.

AI will boost cyber warfare capabilities, enabling entire offensive and defensive systems that could act autonomously, with unpredictable impacts to networks and connected infrastructure.

– The Global Risks Report 2024, World Economic Forum

Most targeted sectors globally

State-sponsored threat groups target broadly as part of their intelligence collection. Critical infrastructure sectors (highlighted) comprised 41% of the NSNs sent in FY2023.



- A 16% Education
- B 12% Government
- C 11% Think tanks and NGOs
- D 11% IT
- E 6% Communications
- F 5% Finance
- G 5% Transportation
- H 4% Defence industry
- I 3% Energy
- J 2% Manufacturing Infrastructure
- K 5% Other Critical Infrastructure
- L 20% Other

POSITIVE IMPACTS

With modern AI advancements analysing trillions of security signals daily, we have the potential to build a safer, more resilient online ecosystem.

The number of people in cyber security jobs has reached its highest number ever: 5.5 million, according to the [2023 ISC2 Global Workforce Study](#).

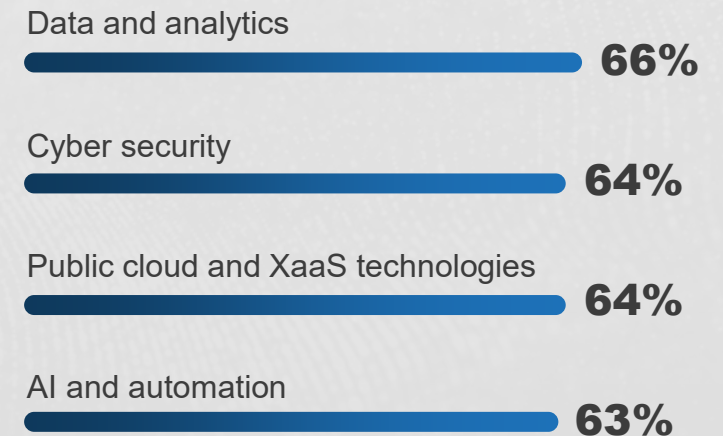
38%

say they now have buy-in from senior leaders for the deployment of emerging tools and technologies.

KPMG Global tech report '23

All new technologies are improving organisations' profitability or performance

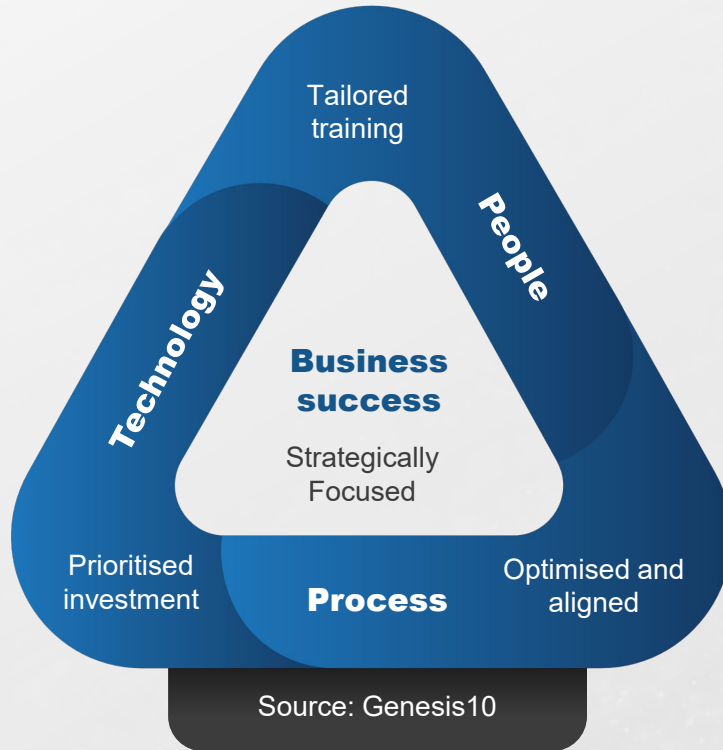
Over the past 24 months, have your digital transformation efforts with the following technologies positively impacted profitability or performance?



KPMG Global tech report '23

CYBER SECURITY – WHERE COMPANIES NEED TO BE

Government Cyber Security Strategy 2022 - 2030



Protect against cyber attack

Secure by design, inherent protection.
(Professional Services)

Minimise the impact of cyber security incidents

Identify and remediate vulnerability.
(Managed Services)

Detect cyber security events

Detect, across every part of the estate to ensure that risks can be mitigated.
(Managed Services)

Manage cyber security risks

Preparedness, expect breach, have a plan.
(Managed Services)

Develop the right cyber security Skills, knowledge and culture

Invest in people, build awareness & expertise.
(Cyber Advisory)

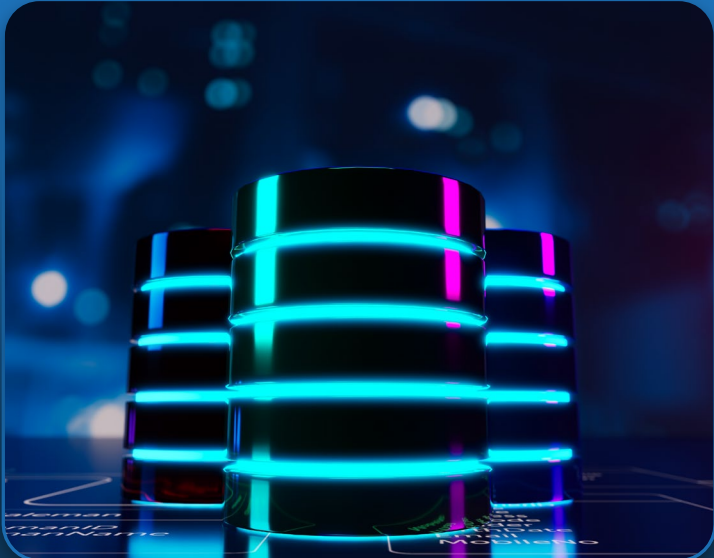


CHANGING MINDSET

Not just systems – this applies to people too

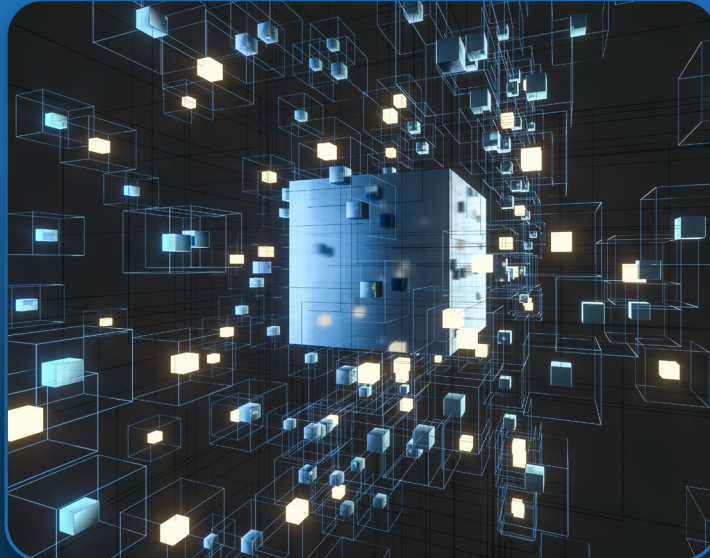
Past

Siloed



Present

Connected & cohesive



Future

Hyper-connected



TODAY'S SESSIONS

Managing Human Cyber Risk

Munya Hoto

CybSafe



Future-proof
your workforce.

Securing Identities in the Digital Realm

Drew Schuil

Silverfort



Innovative
approaches to
safeguarding
identities and access.

The Modern SOC in the Age of AI

Paul Kelly

Microsoft



Steve McKeaveney

ITC Secure



Opportunities and challenges
of AI within the modern SOC.



Networking Break



Managing Human Cyber Risk

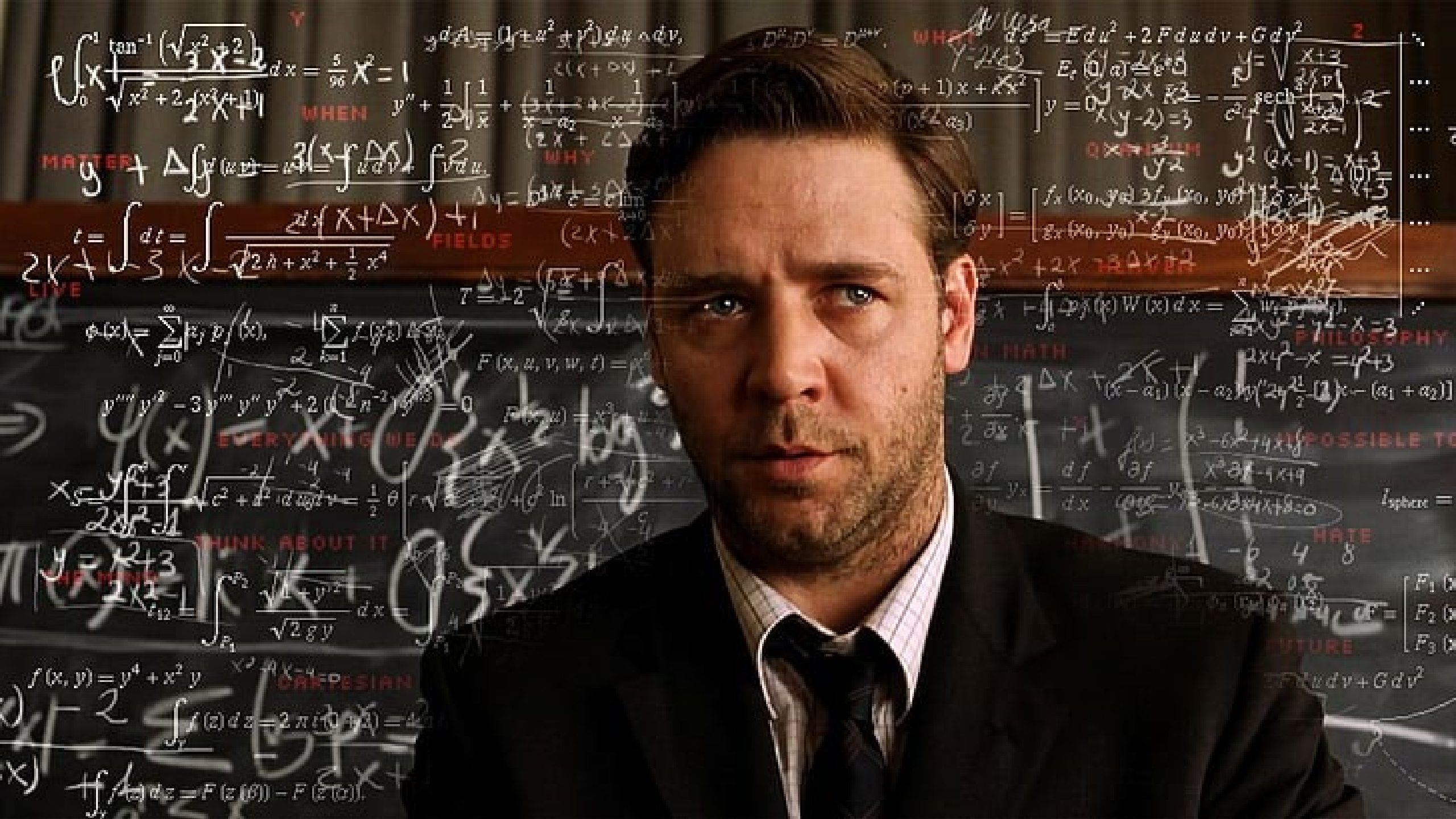
Munya Hoto

Chief Customer & Marketing Officer
CybSafe

Science, Data and Telemetry: A Modern Day Window Into the Soul...er, I mean... Human Cyber Risk

Munya Hoto
CMO, CybSafe





$$\int_0^1 \frac{\tan^{-1}(\sqrt{x^2+2})}{\sqrt{x^2+2}(x^2+1)} dx = \frac{5}{96} \pi^2 = 1$$

WHEN

$$y'' + \frac{1}{2} \left[\frac{1}{x} + \frac{(3x+2)(x-1)}{(2x+1)(x+1)} \right] y' + \frac{3(x+1)}{(2x+1)(x+1)} y = 0$$

MATTER

WHY

$$t = \int dt = \int \frac{2x(x+\Delta x)}{\sqrt{2h+x^2+\frac{1}{2}x^4}} dx$$

FIELDS

$$\phi(x) = \sum_{j=0}^{\infty} \frac{f_j}{j!} \phi^{(j)}(x) = \sum_{k=1}^n \int_{\mathbb{R}} f_k(x) \phi(x) dx$$

EVERYTHING WE DO

$$x_5 = \frac{y^2+3}{2y^2-1} \quad \sqrt{c^2 + \frac{1}{2} \frac{d^2 u}{dt^2}} = \frac{1}{2} \theta \left[r \sqrt{a} + \frac{1}{\theta} \ln \left(\frac{r + \sqrt{a}}{r - \sqrt{a}} \right) \right]$$

THINK ABOUT IT

$$y = \frac{x^2+3}{2x^2-1} \quad \int_{P_1}^{P_2} \frac{\sqrt{1+y^2}}{\sqrt{2gy}} dx = \frac{1}{\sqrt{2g}} \int_{P_1}^{P_2} \frac{\sqrt{1+y^2}}{\sqrt{y}} dx$$

CAKEPESIAN

$$f(x,y) = y^4 + x^2 y \quad \int_{\gamma} f(z) dz = 2\pi i (0+3) = 6\pi i$$

$$\int_{\gamma} f(z) dz = F(z(b)) - F(z(a))$$

$$ds^2 = E du^2 + 2F du dv + G dv^2 \quad Y = \frac{2x+3}{x^2-1} \quad E = \frac{1}{x^2-1} \quad F = -\frac{2x}{(x^2-1)^2} \quad G = \frac{1}{(x^2-1)^2}$$

QXPHISM

$$\frac{\partial x}{\partial y} = \begin{bmatrix} f_x(x_0, y_0) & 3f_x(x_0, y_0) \\ g_x(x_0, y_0) & 2g_x(x_0, y_0) \end{bmatrix}$$

$$\frac{1}{2} x^2 + 2x - 3 \Delta x \Delta y \quad \int_0^1 \phi_j(x) W(x) dx = \sum_{k=1}^n w_k \phi_j(x_k)$$

PHILOSOPHY

$$\frac{\partial}{\partial y} \Delta x + \frac{2x}{(x-a_1)(x-a_2)} y' (2x^2-1) x - (a_1+a_2) \left[\frac{1}{2} \frac{\partial}{\partial x} x + 1 \right]$$

$$\frac{\partial f}{\partial y} y_x = \frac{df}{dx} - \frac{\partial f}{\partial x} y_y \quad f(x) = \frac{x^3-6x^2+4x+9}{x^2-4x+9}$$

$$x^3-6x^2+4x+9 = (x^2-4x+9)(x+b) = x^3 + (-4+b)x^2 + (9-4b)x + 9b$$

$$-4+b = -6 \quad 9-4b = 4 \quad 9b = 9 \quad b = -2$$

$$x^3-6x^2+4x+9 = (x^2-4x+9)(x-2)$$

$$f(x) = \frac{x^3-6x^2+4x+9}{x^2-4x+9} = x-2$$

$$f(x) = x-2 \quad f'(x) = 1$$

$$f(x) = x-2 \quad f''(x) = 0$$

$$f(x) = x-2 \quad f'''(x) = 0$$

$$f(x) = x-2 \quad f^{(4)}(x) = 0$$

$$f(x) = x-2 \quad f^{(5)}(x) = 0$$

Traditionally...

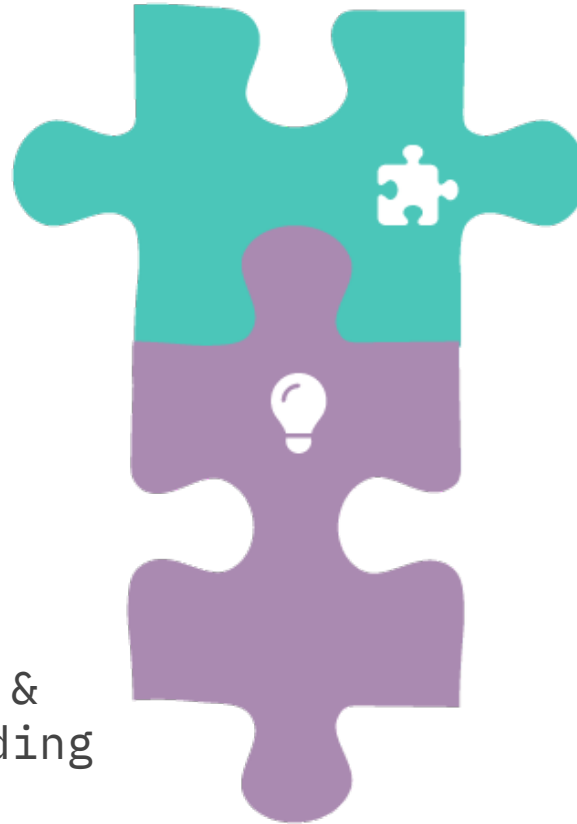


Knowledge &
Understanding



- Training modules
- Emails
- Intranet posts
- Videos
- Newsletters
- Quizzes
- Presentations
- Webinars
- Games

85 Knowledge & Understanding



15 Security behaviors

- Phishing simulations



<15% of users

who complete
security awareness
training actually
change their
behavior



'From promoting awareness to embedding behaviours', Information Security Forum



The world has changed

↑ 82%

Let employees work remotely some of the time, 42% working flexibly¹

↑ 1.1k+


Average number of times employees switch between applications daily²

74%

of breaches involved the human element, which includes social engineering attacks, errors or misuse³

1. Gartner Return to the Workplace Benchmarking Against Your Peers Webinar Poll (5 June 2020)
2. From PEGA Systems: Demystifying the desktop: What workforce intelligence reveals about technology and employee productivity
3. Verizon DBIR 2023



A background image showing a group of people, primarily young adults, looking at their smartphones. The image is slightly blurred, focusing on the foreground individuals. The lighting is soft, and the overall tone is dark, with the subjects' faces and hands illuminated by the phone screens.

35%

change a word or a character in their existing password when asked to change

24%

created passwords containing **12+ characters**

34%

Created passwords made up from a single dictionary word **with some character placements**

32%

Created passwords with **reference to personal information**





Only **45%**

have **turned on automatic updates**

30%

of participants said they **have never heard of MFA**

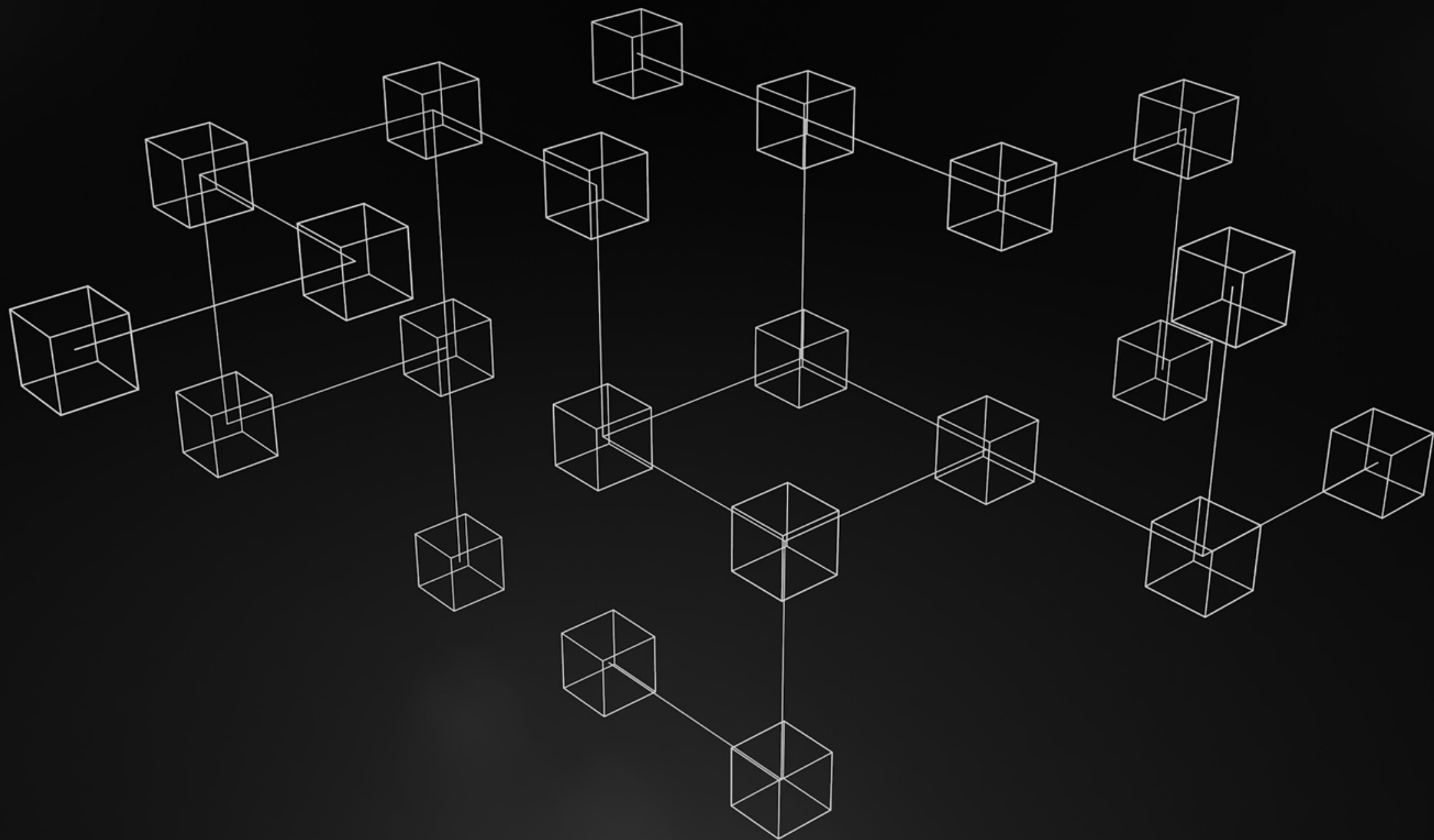
67%

always or very
often **check legitimacy of emails/messages**

24%

Don't know how to back up their important data





SB187

Does not share a file containing PII

SB184

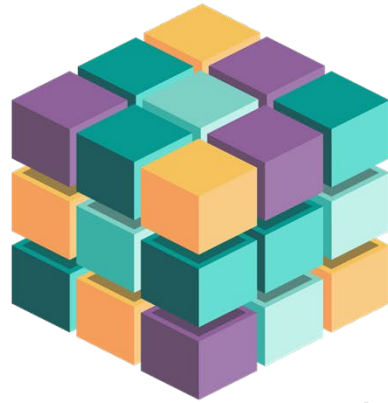
Does not share a file containing confidential

SB198b

Does not use unapproved desktop or laptop for work purposes

SB001

Enables multi-factor authentication



SebDB

The world's **most comprehensive**
security behavior database

not post PII in a public channel

SB189

Does not use unapproved applications

SB211

Does not share PII in email messages

SB212

Does not share confidential information

SB151

Does not use weak passwords





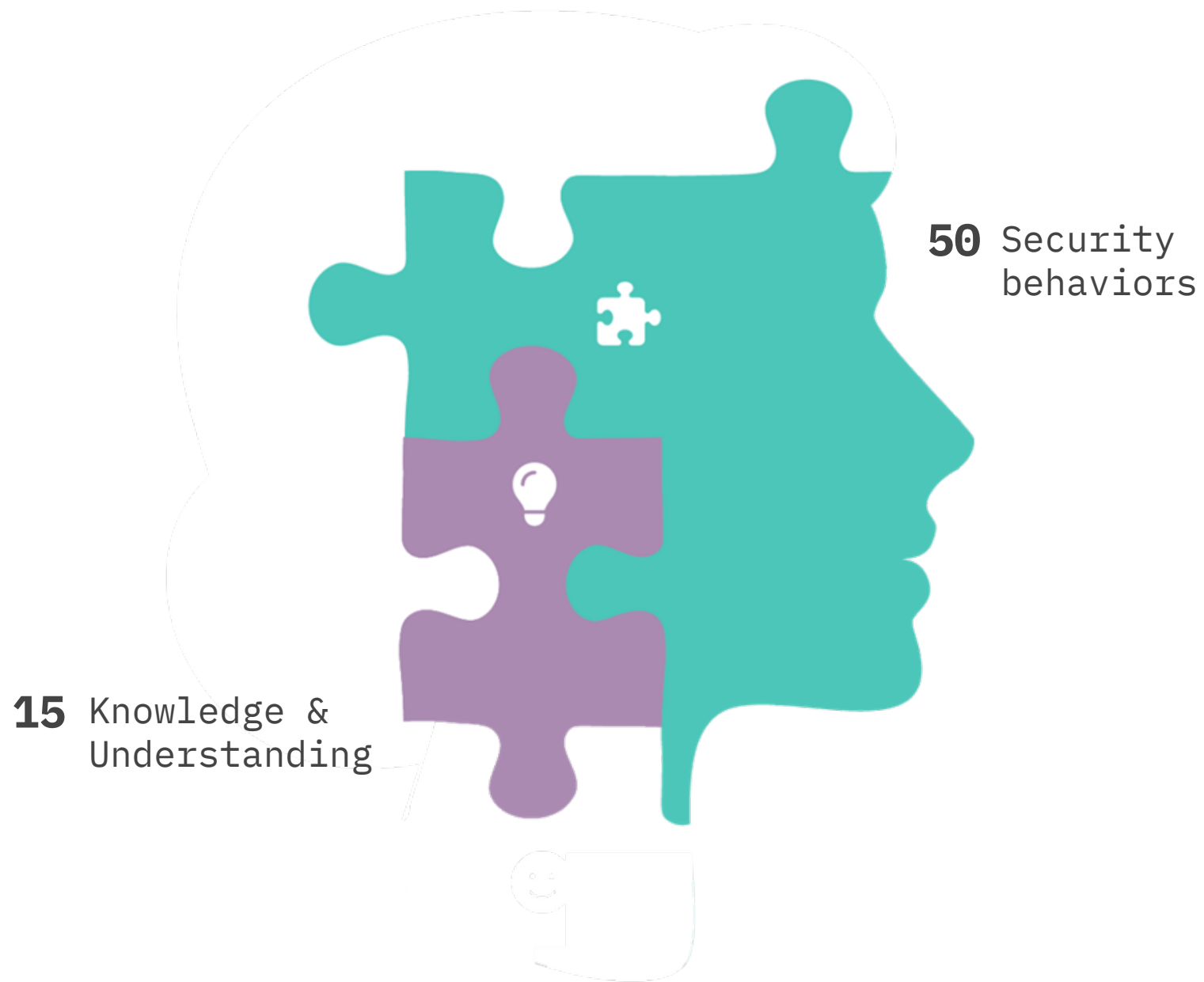
Microsoft 365, Microsoft Purview and DLP, Microsoft Teams,
Microsoft Defender, Microsoft Intune Device Management

Email phishing	SB159	Does not click a phishing link
Email phishing	SB159b	Does not click a simulated phishing link
Password hygiene	SB150	Does not use a password that has been compromised in a data breach
Mobile device use	SB174a	Does not log in from a mobile running out of date operating software
Mobile device use	SB175	Does not log in from a rooted mobile device
Mobile device use	SB198a	Does not use unapproved mobile device for work purposes
Mobile device use	TEMP213a	Does not use a mobile device that is infected with malware
Workstation risks	SB174b	Does not log in from a desktop/laptop running out of date operating software
Workstation risks	SB198b	Does not use unapproved desktop or laptop for work purposes
Workstation risks	SB032	Does not insert unauthorised devices/media into work devices/network
Workstation risks	TEMP213b	Does not use a laptop/desktop device that is infected with malware

CYBSAFE.COM

MFA	SB001	Enables multi-factor authentication for workplace accounts
SaaS use	SB189	Does not use unapproved applications on work devices
Data handling	SB182	Does not send sensitive information out of the business (email or otherwise)
Data handling	SB184	Does not share a file containing confidential information
Data handling	SB185	Does not post confidential information in a public messaging channel
Data handling	SB186	Does not post PII in a public channel
Data handling	SB187	Does not share a file containing PII
Data handling	TEMP211	Does not share PII in email messages
Data handling	TEMP211	Does not share confidential information in email messages
Third party breaches	SB171	Does not use work email address that has been compromised in a data breach
Secure browsing	SB155	Does not download content or material from unauthorised websites





Old world



5 Confidence

10 Engagement

10 Exposure

50 Security behaviors

5 Digital resilience

15 Knowledge & Understanding



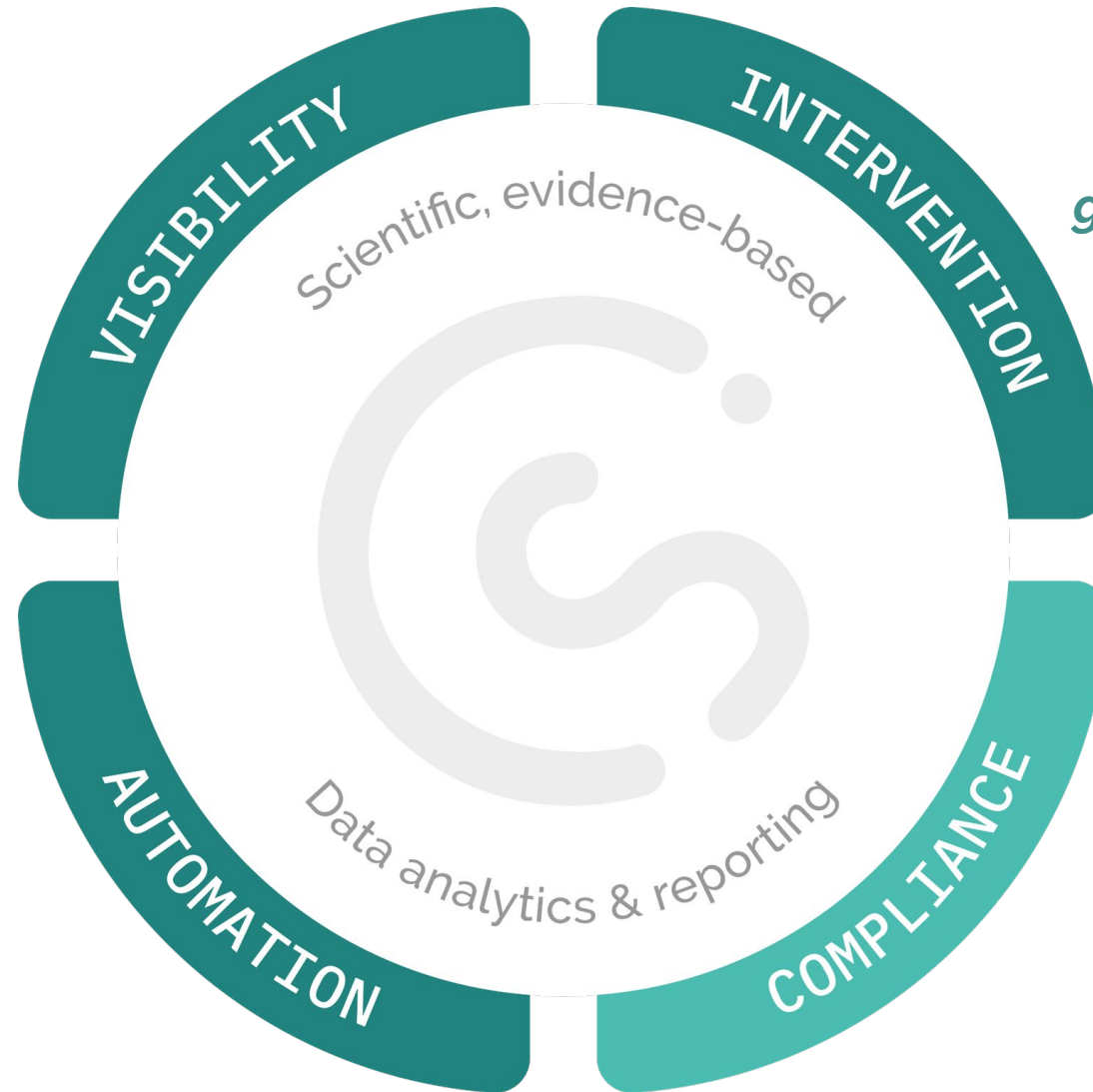
Sensitive data access

5 Attitude

New world, better outcomes



Leverage telemetry for **insight** into employee risk



Personalised **guidance and support** specific users and user groups.

Automate risk reduction and behaviour change

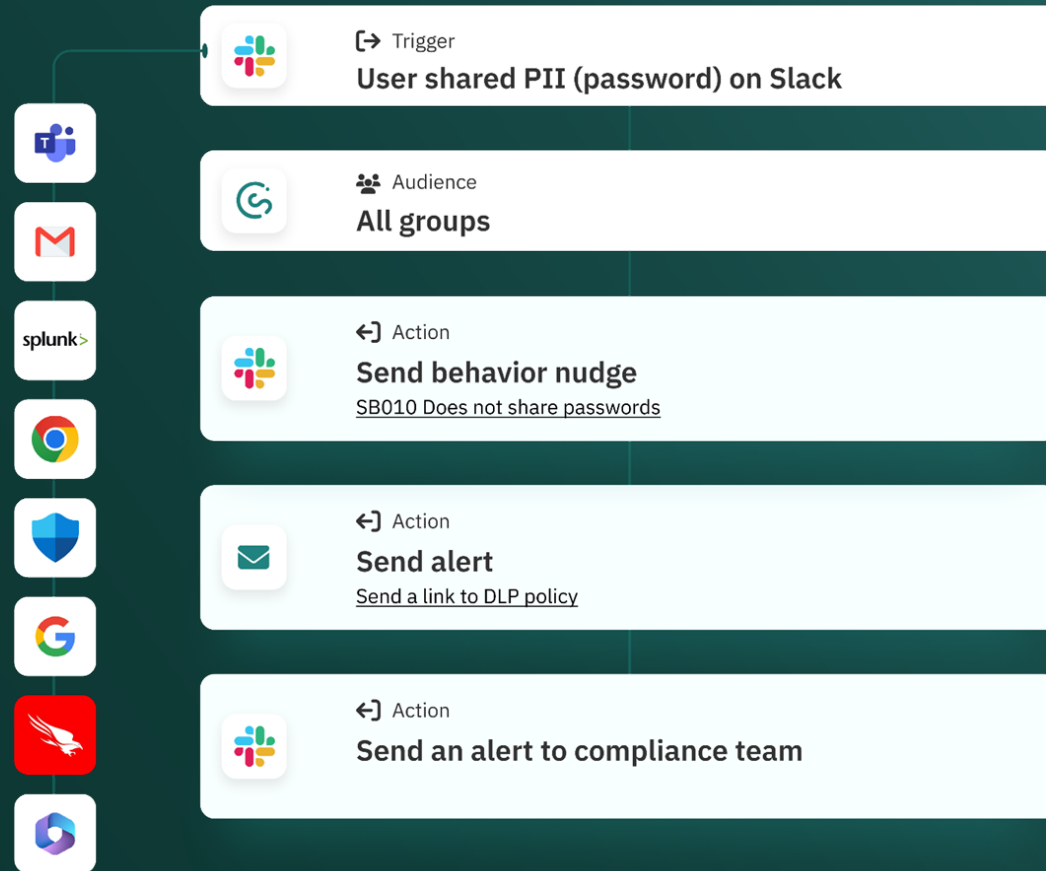
Security advice, **training, simulated phishing** and assessment.



What are workflows?

Automate human risk management tasks without code.

New workflow



+ New action

- Send notification
- Create calendar event
- Create Jira ticket
- Filter users
- Notify manager
- Send webhook

Use cases

- Employee onboarding
- Line manager engagement
- User notifications & reminders
- Administrator notifications
- Monitor human risk management initiatives
- Triggering actions in 3rd party software
- Phishing training and simulations
- Security behavior triggers
- Security awareness training tasks
- Risky behavior alerts
- Slack and Microsoft Teams notifications



Three levels of human risk analytics

1

Human cyber risk quantification

Risk outcomes quantified with likelihood and impact

2

Human cyber risk grades

Track human risk at a glance for individuals and groups

3

Human cyber risk factors

Metrics, measurements and indicators that combine to determine human risk



Human cyber risk quantification

Risk outcomes quantified with likelihood and impact

Risk outcomes

Risk is calculated as a combination of likelihood and impact. The likelihood is produced by CybSafe from our behaviour event intelligence data, and the impact of each risk outcome is configurable on the [Impact settings](#) page

RISK001

Malware Infection

Very high

4.21 (+5%)

RISK002

Data Theft

Medium

2.83 (0%)

RISK003

Physical Damage

Low

1.33 (-8%)

RISK004

Privacy Violation

High

3.94 (-1%)

RISK005

Identity Theft & Fraud

Low

1.46 (+3%)

RISK006

Personal Exposure

High

3.19 (0%)

RISK007

Account Compromise

High

3.04 (-3%)

RISK008

Data Leak

Very high

4.08 (-2%)



Human cyber risk grades

Track human risk at a glance for individuals and groups



First name: Leroy
Last name: Masson
Email: leroy.masson@23847
733-anonymised.com
Last seen: a month ago
Date added: 16 December
2015
Country: GB
Organization: Howe Inc
Department: Sales

Update details

49

Security behaviours
SebDB weighted behaviours scores

42

Knowledge & understanding
SebDB weighted course completion

56

Exposure
Passphrase usage, SaaS and
compromised credentials

72

Engagement
Increase in security hero score over 90
days

63

Attitude
Attitude

68

Confidence
Average confidence over 90 days

N/A

Digital hygiene
Personal cyber security survey

High

Access to sensitive data
Self reported













Human cyber risk factors

Metrics, measurements and indicators that combine to determine human risk

Analytics Recommendations Linked behaviours **Risk factors**

Contributions

Only risk factors with measurements contribute to the score, this shows the actual contribution rates and scores for each risk factor.

Risk factor	Contribution	Coverage	Score	Score change
Security behaviours	52.6%	 Low	 64/100	64.4 (64.4%)
Knowledge & understanding	15.8%	 High	 75/100	75 (75%)
Exposure	10.5%	 High	 96/100	95.5 (95.5%)
Engagement	10.5%	 High	 24/100	24 (24%)
Attitude	5.3%	 High	 65/100	64.8 (64.8%)



Change security behavior. Change the game.

Reduce the number of incidents caused by **risky security behaviors**.



GUIDE

Personalised, scientific guidance, nudges and training for employees.

+



PHISH

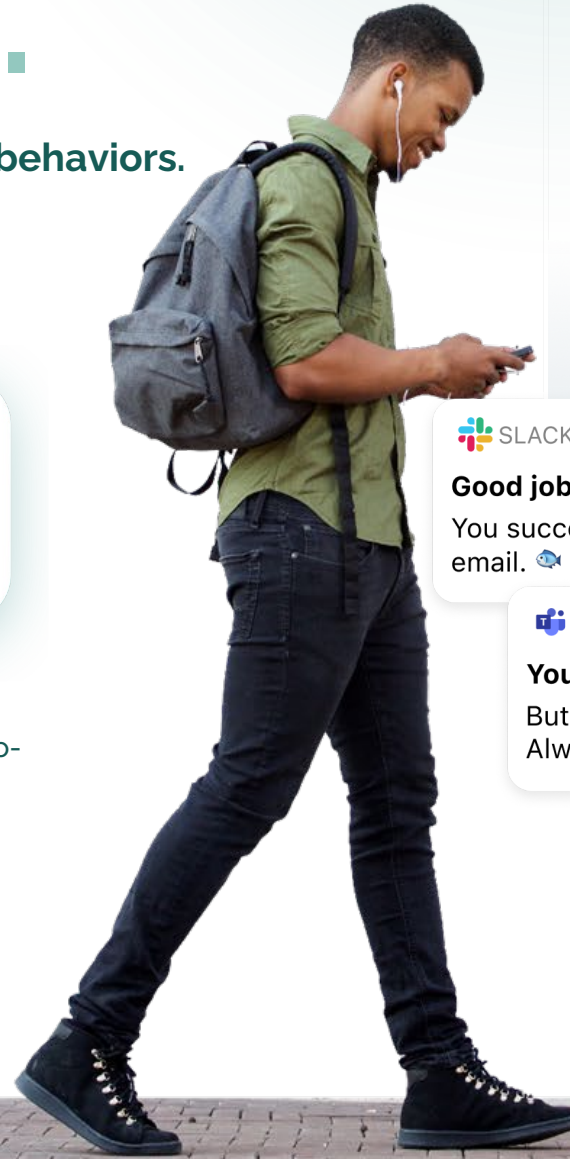
Scientifically-designed simulations & user support to counter social engineering and illuminate risk.

+



RESPOND

Security behavior measurement & no-code workflow automation.



Behaviors targeted

- SB013** Checking emails for signs of deception
- SB091** Does not forward work information to personal email addresses
- SB161** Reports a suspected phishing email
- SB164** Does not open an attachment in a phishing email
- SB171** Does not use work email address that has been compromised in a data breach
- SB173** Does not use work email addresses for non-work purposes
- SB183** Does not send emails to unintended recipient(s)



Good job!

You successfully reported a phishing email. 🐟

3m ago



You spotted it. You deleted it.

But maybe your colleague wasn't so sharp?
Always report suspicious messages.

57m ago

BARRIERS TO SECURITY BEHAVIORS



- Time restraints
- Competing priorities
- Mistrust of password managers
- Bad habits

NUDGE MECHANISMS



- Compare
- Risk
- Facilitate
- Emotion



Trusted by...

sage



ROYAL COLLEGE OF MUSIC
London

xerox


HISCOX

William **HILL**

 **BARCLAYS**


AIB

 robinhood

**NEW
YORK
LIFE**

fenergo

Vhi
HEALTHCARE


THE
BEHAVIOURAL
INSIGHTS
TEAM

 **PTSG**
PREMIER TECHNICAL
SERVICES GROUP LTD

HFW

 **Admiral**

 Dŵr Cymru
Welsh Water



Royal College of Art

 **vodafone**

Lonza

GYMSHARK 

NHS
Northumbria Healthcare
NHS Foundation Trust

HSBC 

COX
ENTERPRISES


ocado

 Office for
National Statistics


MOODY'S

ERGO


Upfield™





A side-profile photograph of a person with dark skin, wearing a light grey t-shirt. They are holding a black smartphone in their right hand. They are also wearing a beaded necklace with orange, white, and black beads, and several beaded bracelets on their left wrist. The background is a solid, muted blue-grey color.

Our vision is for a world
where we use technology
without fear.



Securing Digital Identities

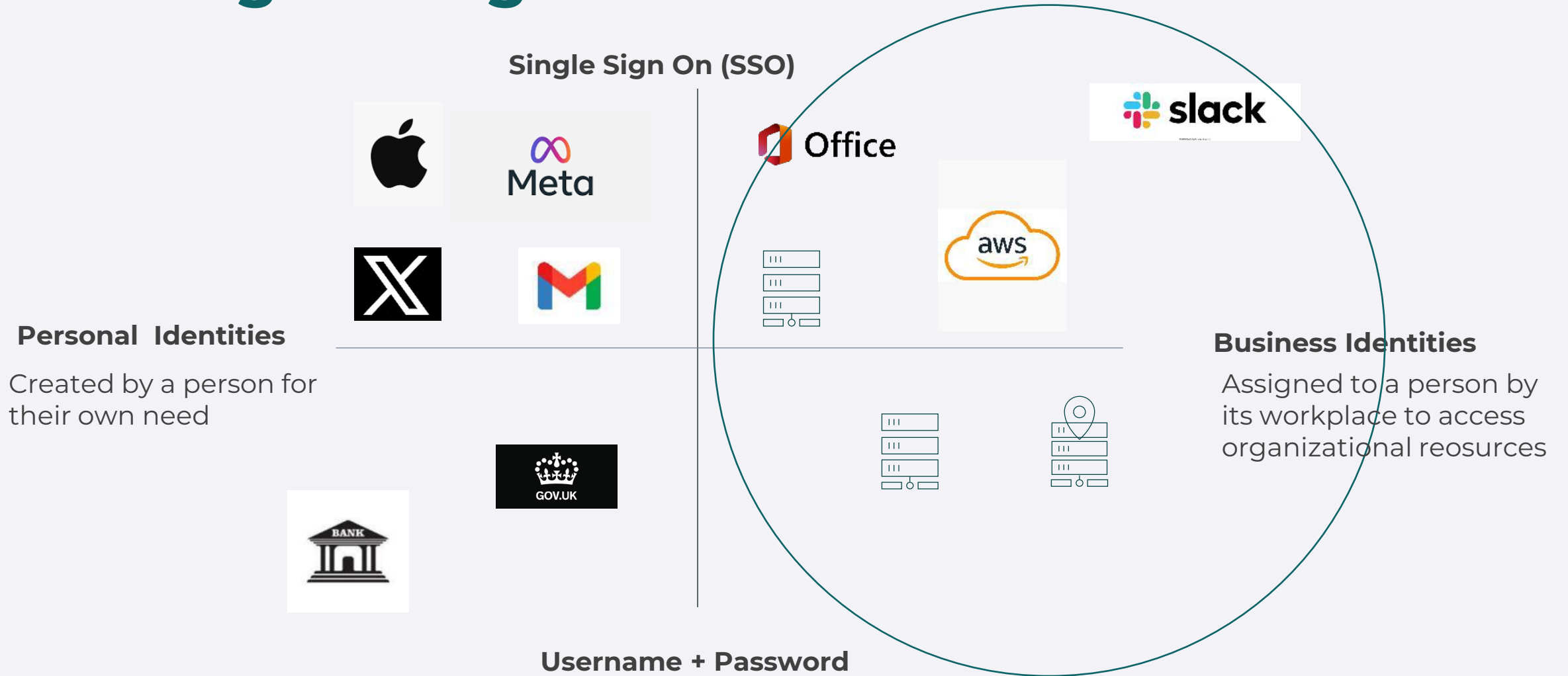
Drew Schuil

Chief Revenue Officer
Silverfort

Securing identities in the digital realm

Drew Schuil - CRO

The age of digital identities



Business identities in a hybrid world

On-prem

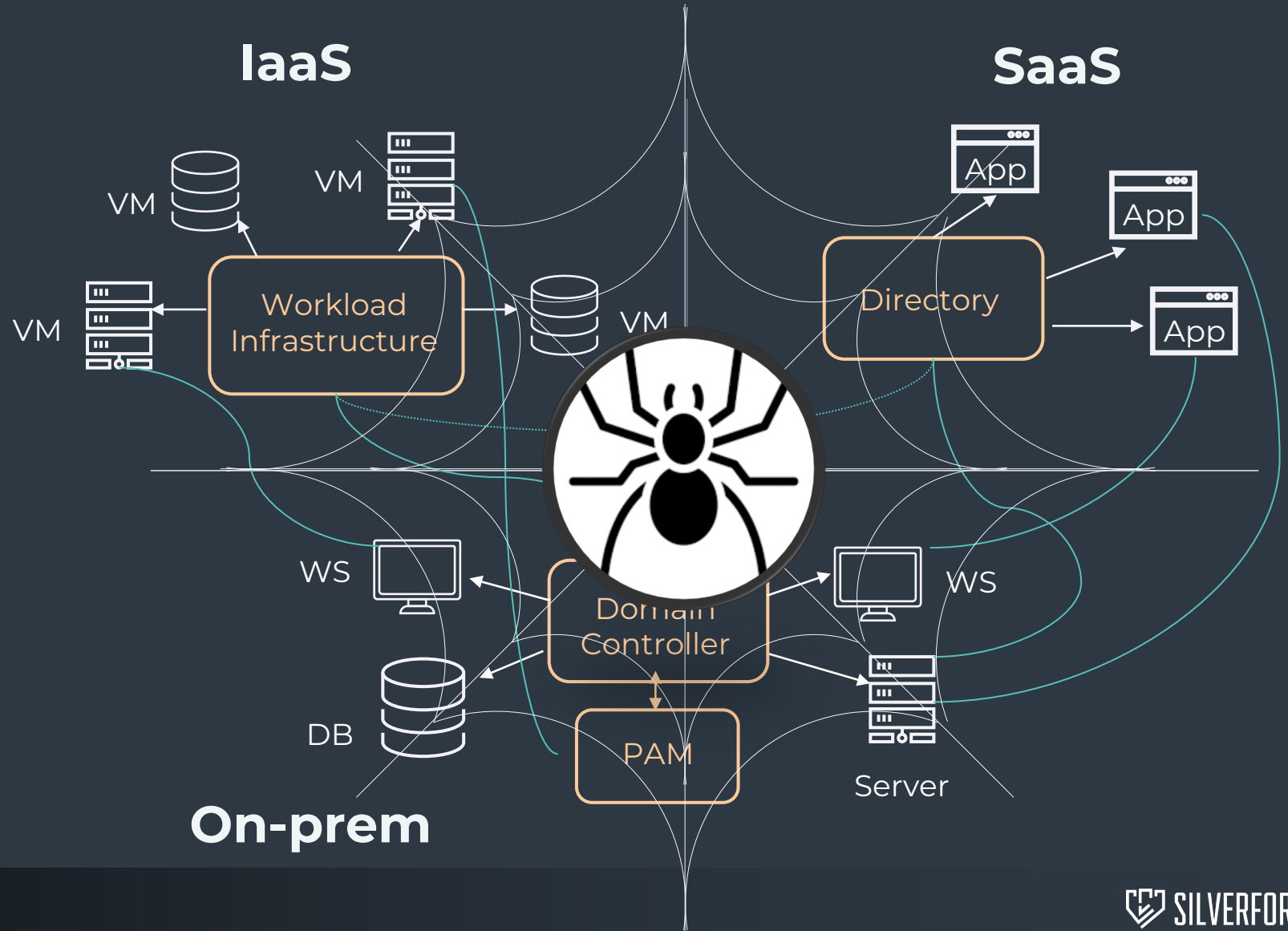
- Access purpose
 - File servers, homegrown apps, databases, etc.
 - IT privileged users
 - Service accounts (machine-to-machine)
- SSO
 - Mostly **Active Directory (AD)**

Cloud

- Access purpose
 - Web & SaaS applications
 - Cloud workloads
- SSO
 - Cloud IdP: **MSFT Entra ID, Okta**
 - Federation service: **ADFS, Ping Federate**

The hybrid, interconnected enterprise environment

- Modern IT environments include on-prem, IaaS, & SaaS resources
- They feature a high volume of interconnectivity
- Complex & difficult to monitor
- Easily targeted attack surface.



Where is the identity security gap?

MFA

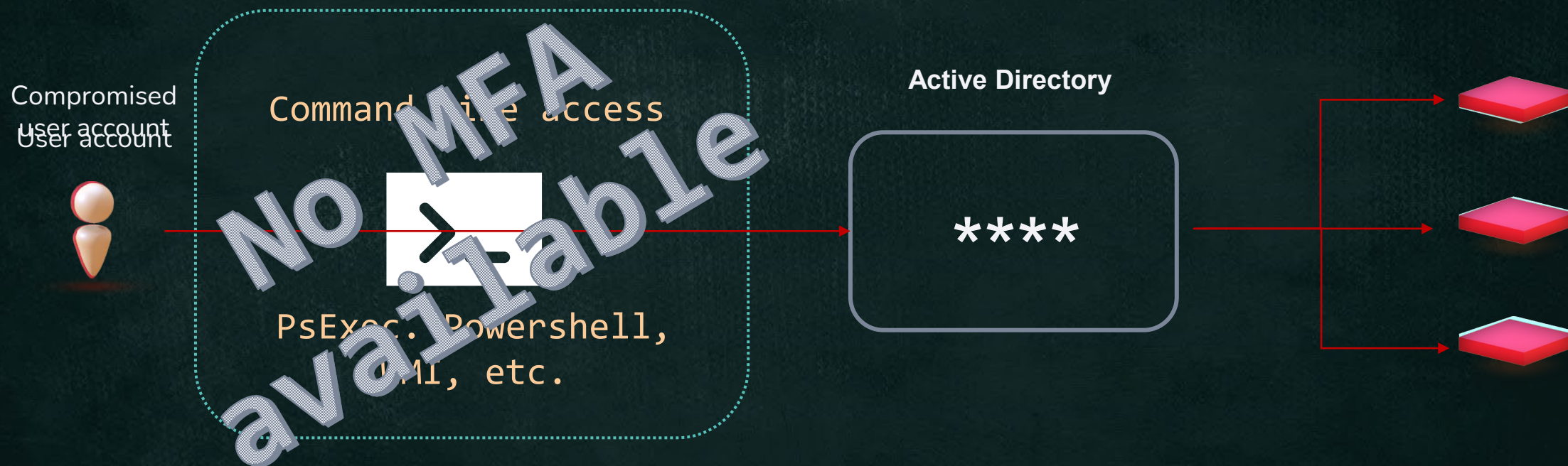


Service Accounts



Top-3 cyber insurance carrier: “More than 90% of our ransomware claims involve Active Directory & compromised credentials.”

The MFA Blind Spot



These interfaces pre-date MFA...

Attackers know about these blind spots...



The **MFA** blind spot

Many sensitive resources still rely on legacy protocols & IAM infrastructure such as **Active Directory**, that **don't support MFA**



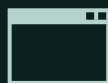
Command-line tools
(e.g. PsExec, PowerShell,
SSH, RDP, WMI, Run As)



Admin consoles
(e.g. vCenter, monitoring
tools)



**File systems &
databases**
(e.g. CIFS, SQL)



Legacy applications
(homegrown or 3rd
party)



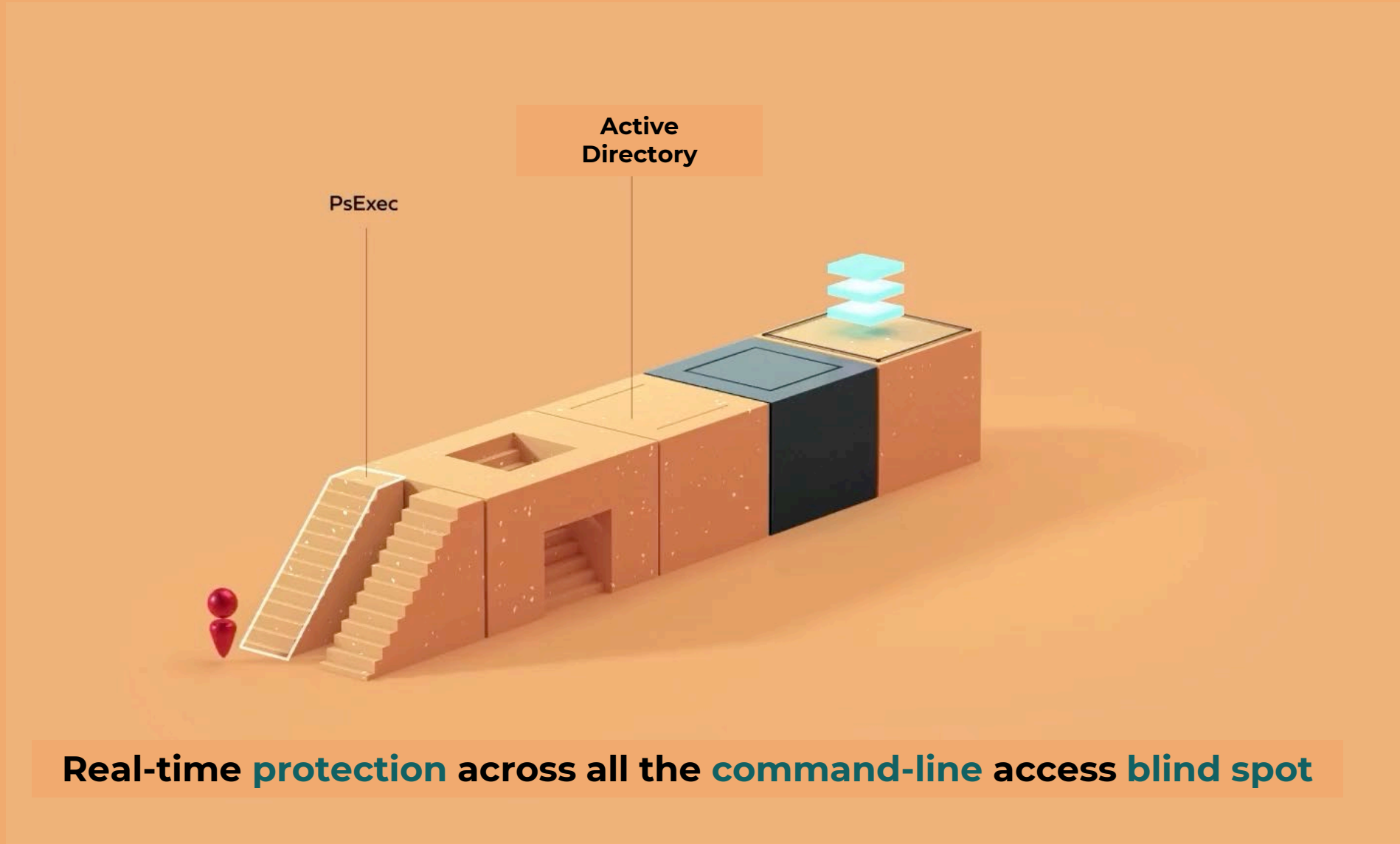
Network devices
(e.g. firewalls,
routers, switches)



**OT & air-gapped
Environments**

82% of ransomware attacks are exploiting this identity security gap to spread.
Tougher **cyber insurance** requirements & regulations now **require MFA for these systems**

Do you have an “*MFA anywhere*” initiative?



The **Service Accounts** blind spot

- Non-human identities are **difficult to protect**
- PAM - PW rotation & vaulting **takes years** & is disruptive to people + process



Highly privileged:

Can cause large damage
when compromised



Unknown dependencies:

Where are they?
How are they used?



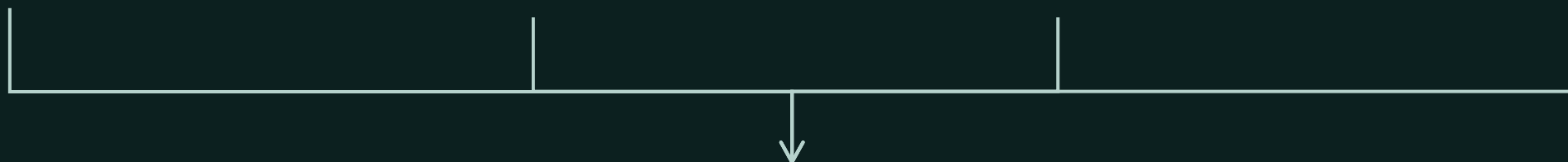
Difficult to protect:

Rotating passwords often
breaks apps



Regularly abused:

Used interactively outside of
intended purpose

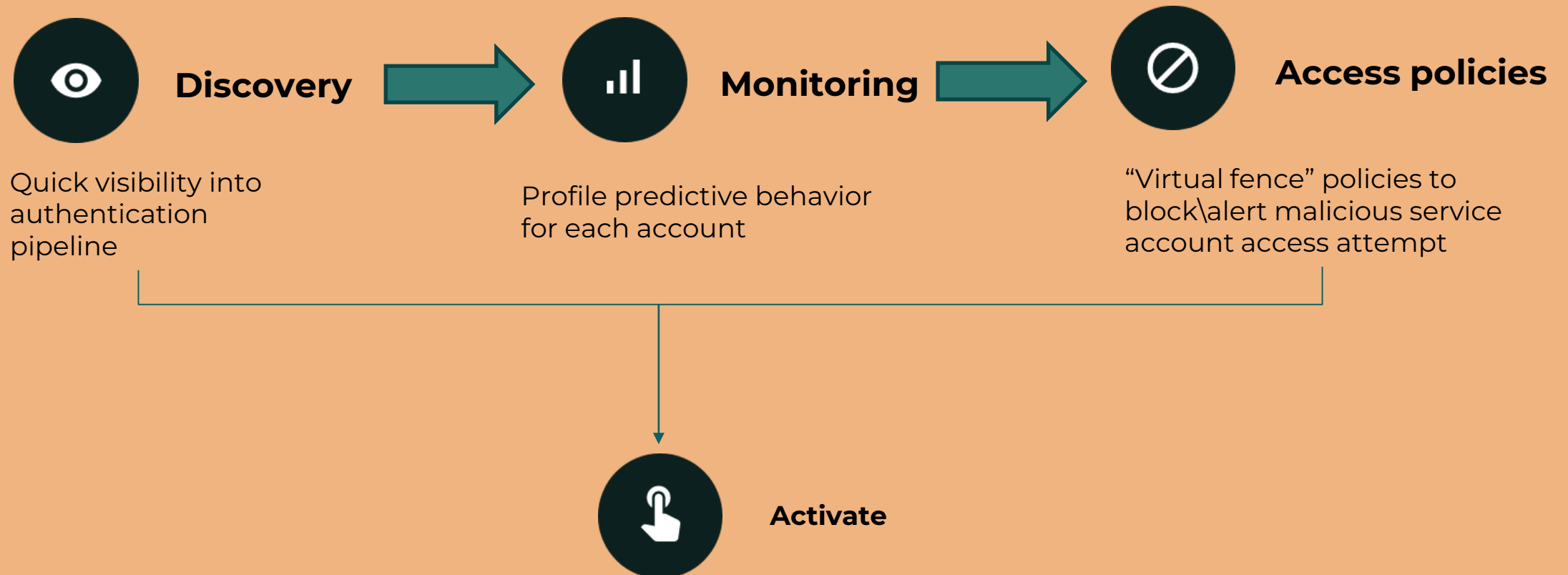


Service Accounts are highly vulnerable & targeted by attackers

“We are 1-year into a 3-year PAM journey, and only 10% deployed”

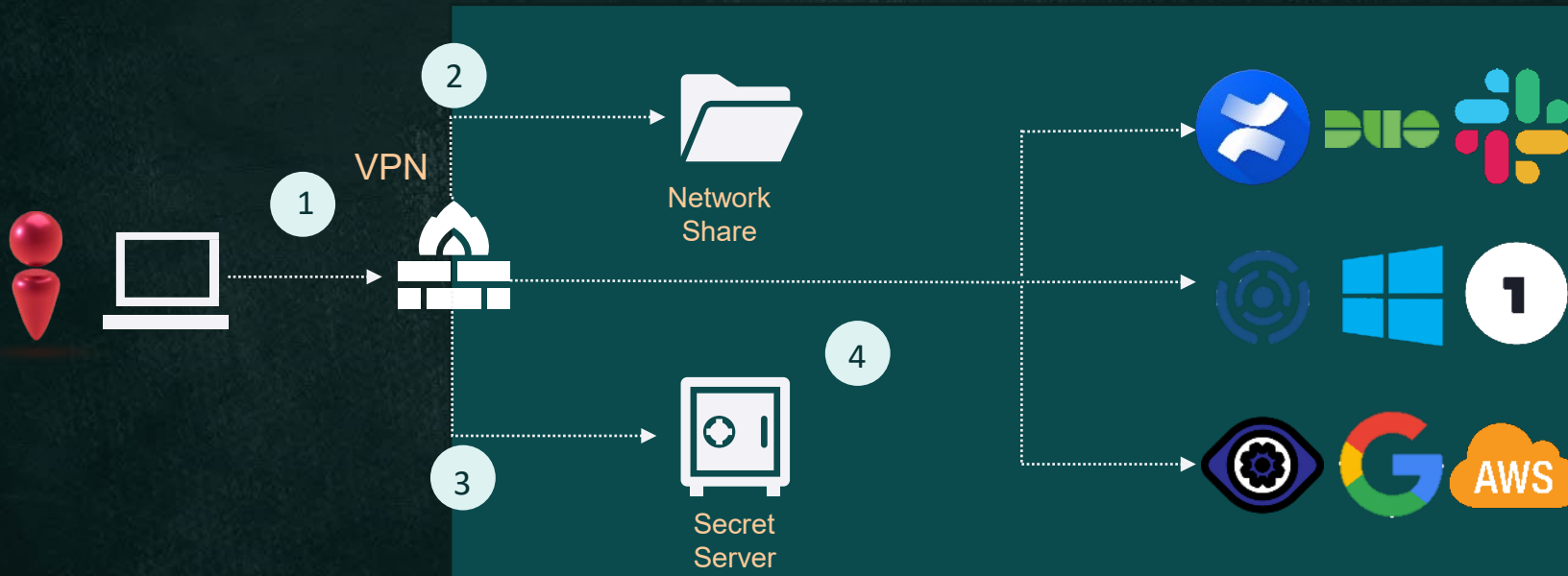
– CISO, large US-based payroll company

Service account protection in weeks, not years



Uber Attack Flow

September 2022 Hacker achieves access to many Uber sensitive systems and data



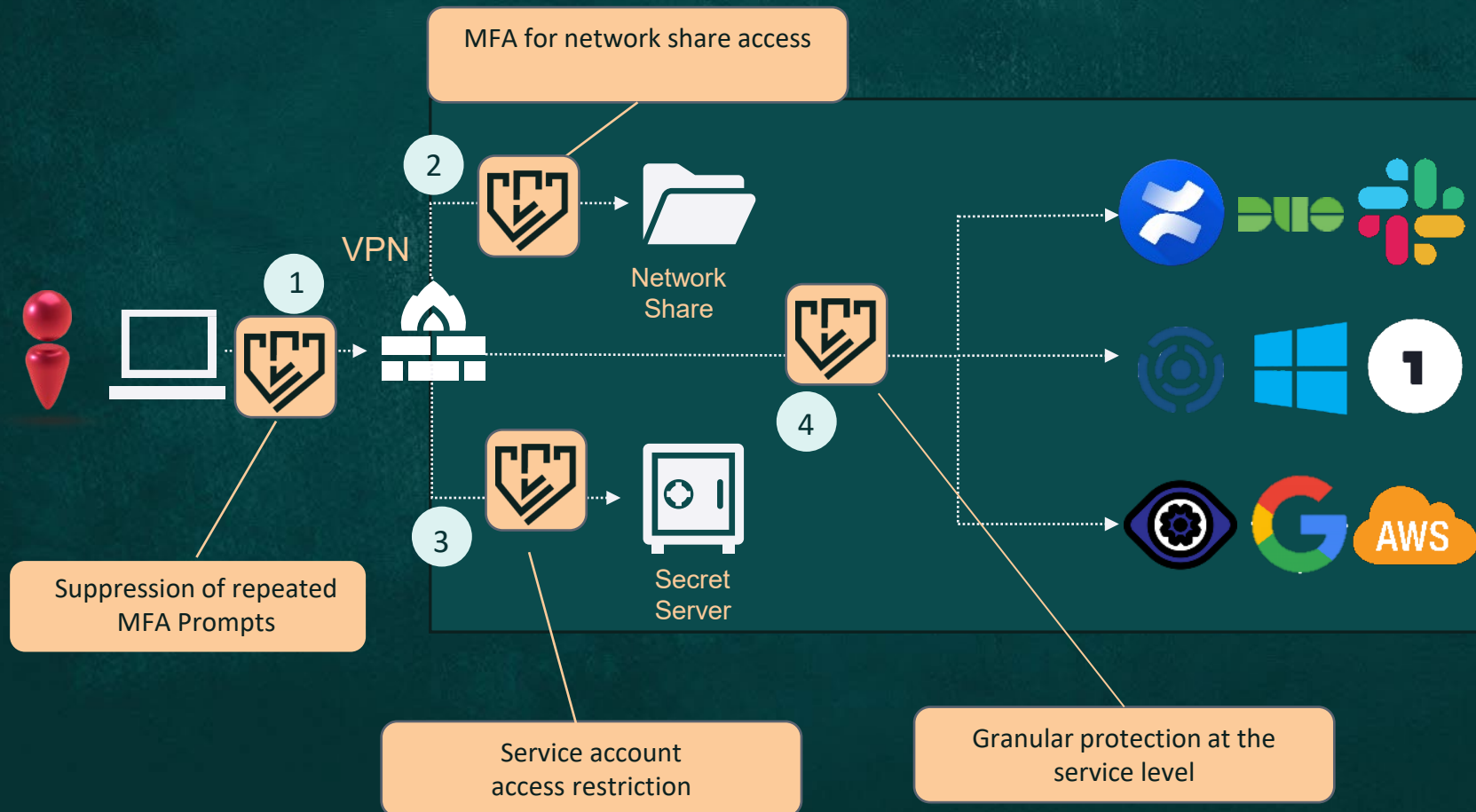
Attack Flow:

- 1. Initial Access:** MFA bombing to gain access via VPN
- 2. Shared Folder Access:** Steal service account credentials from shared folder.
- 3. Empty Vault:** Steal secrets from Secret Server
- 4. Access sensitive resources:** Use secrets to access variety of sensitive resources

Uber attack flow & kill-chain

September 2022

Hacker achieves access to many Uber sensitive systems and data



Attack Flow:

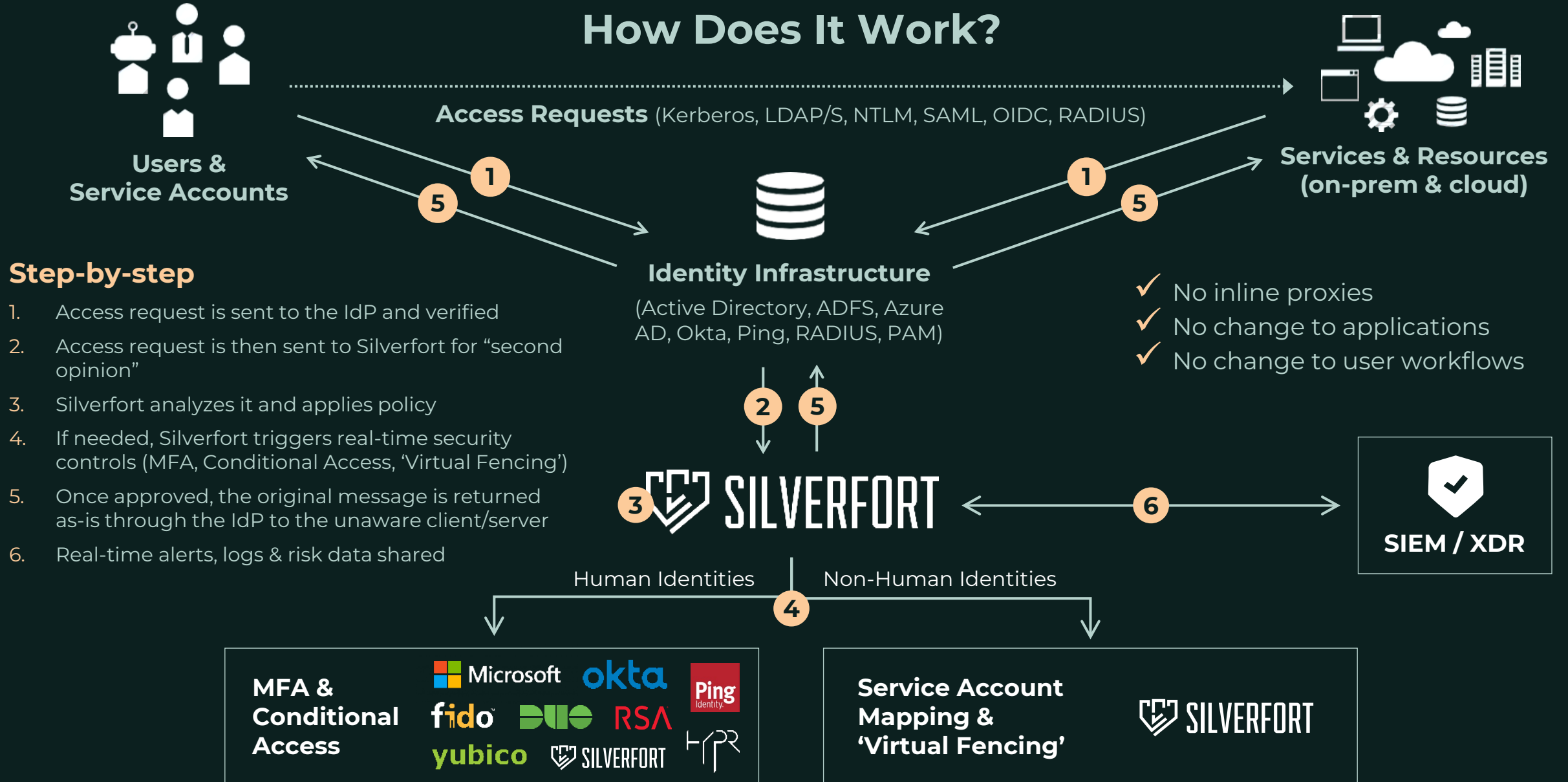
1. **Initial Access:**
MFA bombing to gain access via VPN
2. **Shared Folder Access:**
Steal service account credentials from shared folder.
3. **Empty Vault:**
Steal secrets from Secret Server
4. **Access sensitive resources:**
Use secrets to access variety of sensitive resources

HostName : t5-AWS-1812-1
Instance ID : i-09848417440735529
Private IP Address : 10.61.58.10
Availability Zone : eu-west-1a
Instance Size : t3.medium
Architecture : ARM64

```
Administrator: Windows PowerShell (I)  
PS C:\Users\sfaadmin> Enter-PSSession -ComputerName t5-aws-dc12-1
```

A security layer on top of your existing IAM infrastructure

How Does It Work?



The Unified Identity Protection Journey

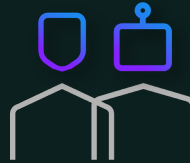
Key customer use cases



ITDR Visibility
into authentication
traffic & AD hygiene



Extend MFA
to 'unprotectable'
assets without
agents or proxies



Service Accounts
discover, monitor &
protect without rotating
passwords



Identity-based attack
propagation
(ie. ransomware) with
adaptive Zero Trust
policies & MFA



Cloud migration
Bridge AD to Azure AD
on-prem apps to AAD
Conditional Access

For every organization

More advanced



Silverfort Raises \$116M in Series D

Read the full story —→



54.2 K

AUTHENTICATIONS



104
Privileged
Users



Azure AD



Okta

Ping



323
Users



Active
Directory



ADFS



302
Service
Accounts



RADIUS

VERIFIED

Demo

BLOCKED

0
Anomaly
Detection

1 1 1 1 0
1 0 1 1
1 1 0 1
0 0 1 1
0
Known
Threats

1 1
1 1
1 1
0 0
External Risk
Indicators



373
Servers



Industrial systems



VPN



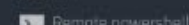
VDI



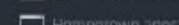
RDP



SSH



Remote powershell



Homegrown apps



20.4 K
Services



297
Cloud Apps

Identity Protection (Last Month)

323 / 323
USERS PROTECTED

1.4 K / 54.2 K
AUTHENTICATIONS VERIFIED

14 / 302
SERVICE ACCOUNTS
PROTECTED

Users by Risk Level

3
CRITICAL

11
HIGH

7
MEDIUM

Authentications (Last Month)

AD - Kerberos (37.2 K)
AD - LDAP (817)
Azure AD (4.8 K)
PingFederate (43)
Windows Logon (581)

AD - NTLM (10.4 K)
AD - LDAPS (382)
Okta (0)
RADIUS (19)
Silverfort API (1)



Q&A

Thank You

Chat with us at the stand!



The Modern SOC in the Age of AI



Paul Kelly

Director, Security
Business Group
– Microsoft



Steve McKeaveney

Head of Customer
Success
– ITC Secure



Ask the Experts



Closing Remarks



Networking Drinks



THANK YOU FOR ATTENDING THE ITC CYBER SUMMIT 2024

Addressing the biggest trends in cyber security

Faster Future: Amplify Your Defences in the Age of AI

Sponsored by:

Sponsored by

