ENJOY SAFER TECHNOLOGY™

Password Related Cyber Breaches on the Rise

Presenter: Ronald Gange

Presentation Overview

The current Australian Threat Landscape

The Problem/s with Passwords

A Simple Solution: Two-factor Authentication

Product Demonstration - ESET Secure Authentication

Q and A

What is ESET

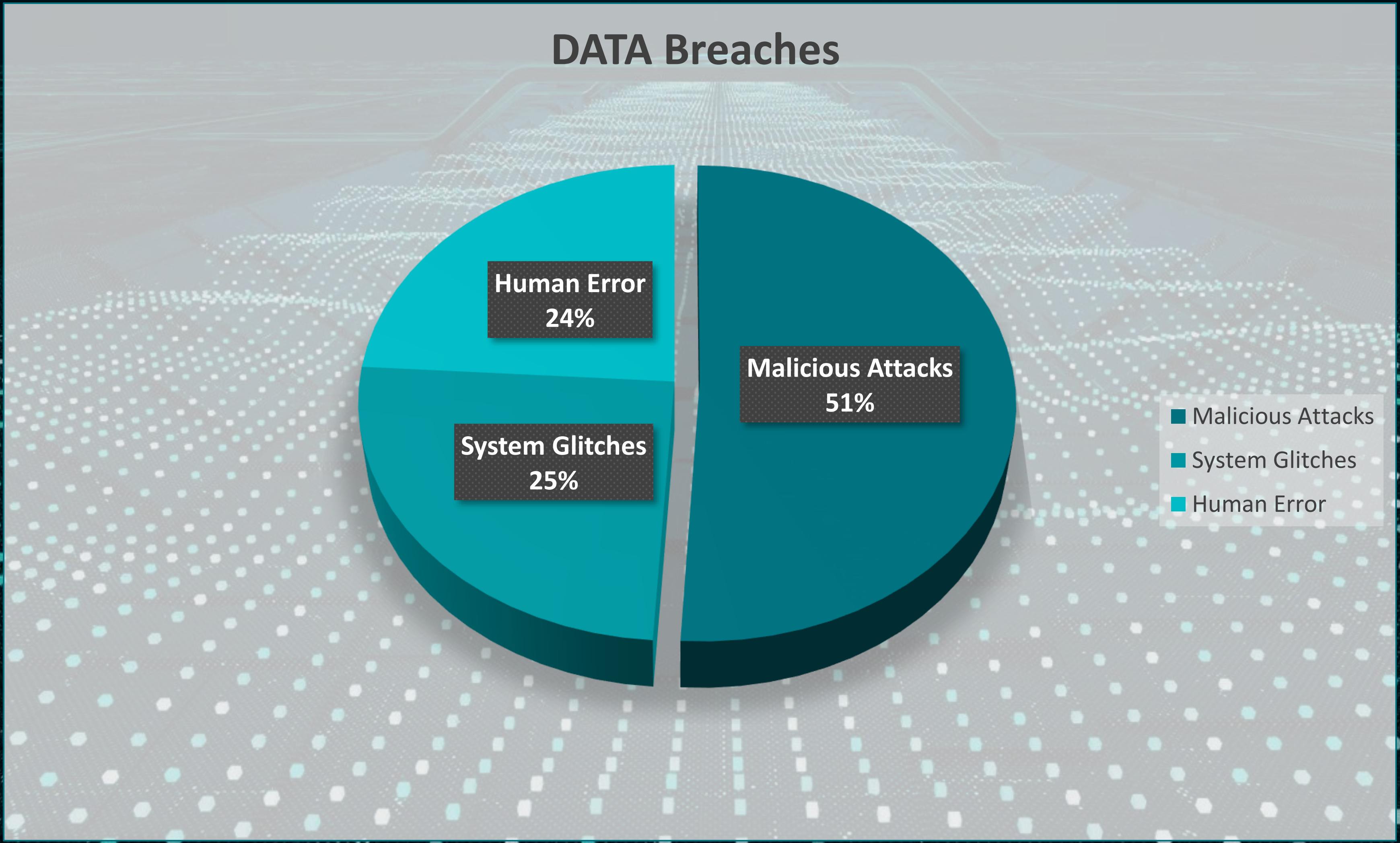
- **#1 global endpoint security** partner from the European Union
- Regional and local offices on **all continents**
- Multilayered security, machine learning and human expertise combined
- **Stable, privately-held** company with own funding
- **30 years** of technology-driven innovation

The Current Australian Threat Landscape

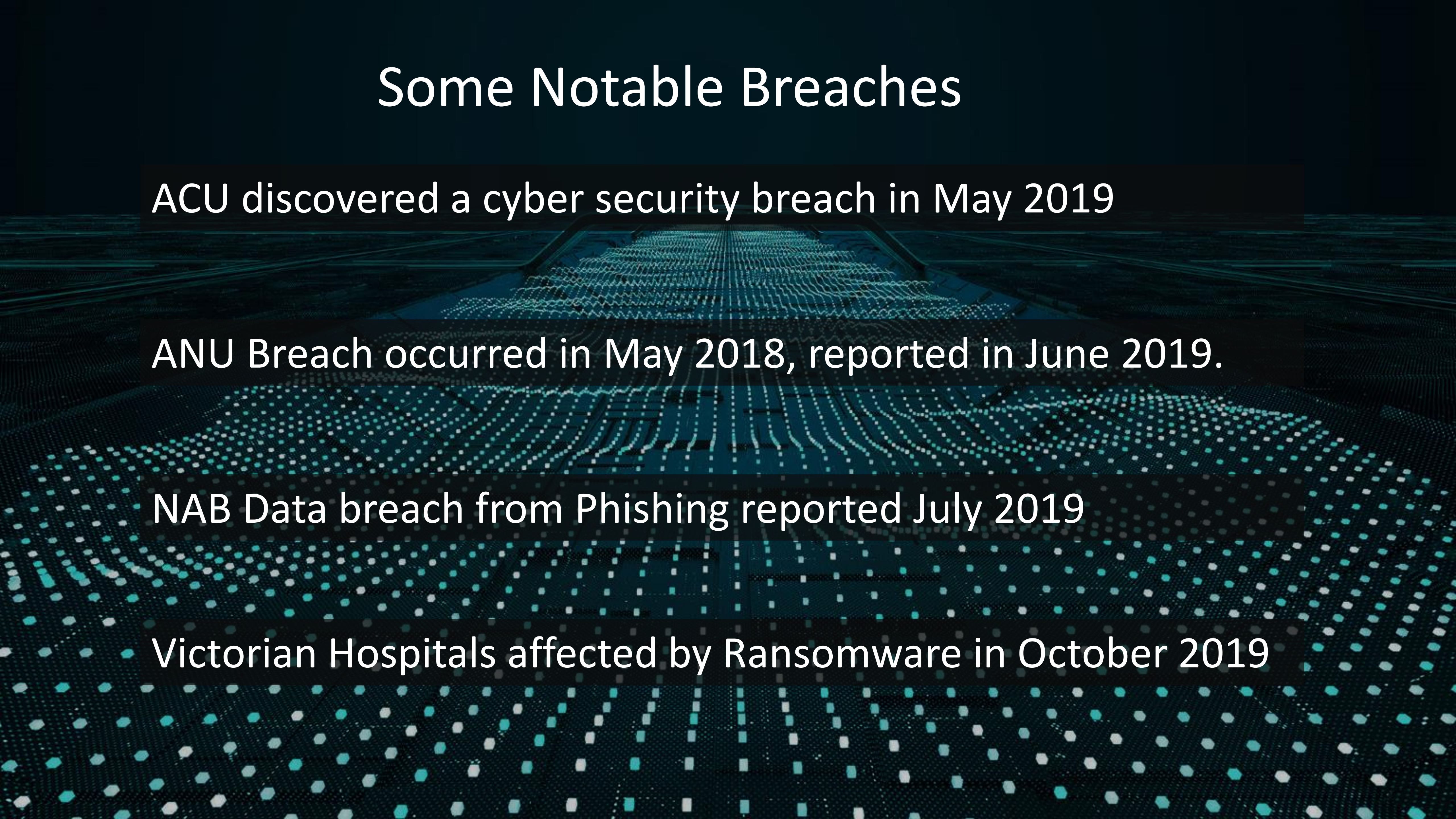
What Is A Data Breach?

A data breach occurs when confidential, private, or other sensitive information is accessed without authorisation or is lost. A data breach can occur accidentally, or as a result of a deliberate attack.

Causes of Data Breach



Some Notable Breaches



ACU discovered a cyber security breach in May 2019

ANU Breach occurred in May 2018, reported in June 2019.

NAB Data breach from Phishing reported July 2019

Victorian Hospitals affected by Ransomware in October 2019

Reported Breaches

1000 Data breaches

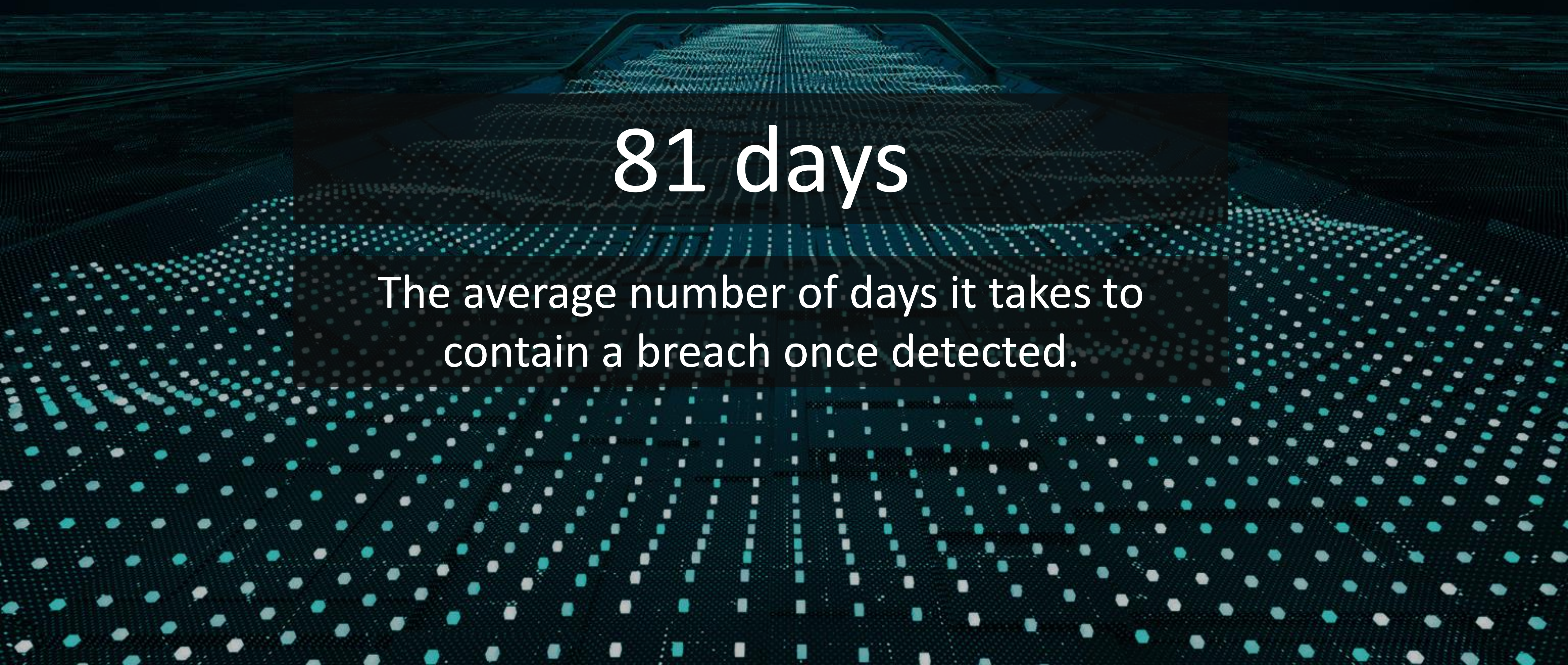
The number of data breaches reported 1 year after mandatory breach notification came into effect.

Breach Detection Gap

200 days

The average number of days it takes before a breach is detected.

Breach Containment



81 days

The average number of days it takes to contain a breach once detected.

The Real Cost of Data Breaches

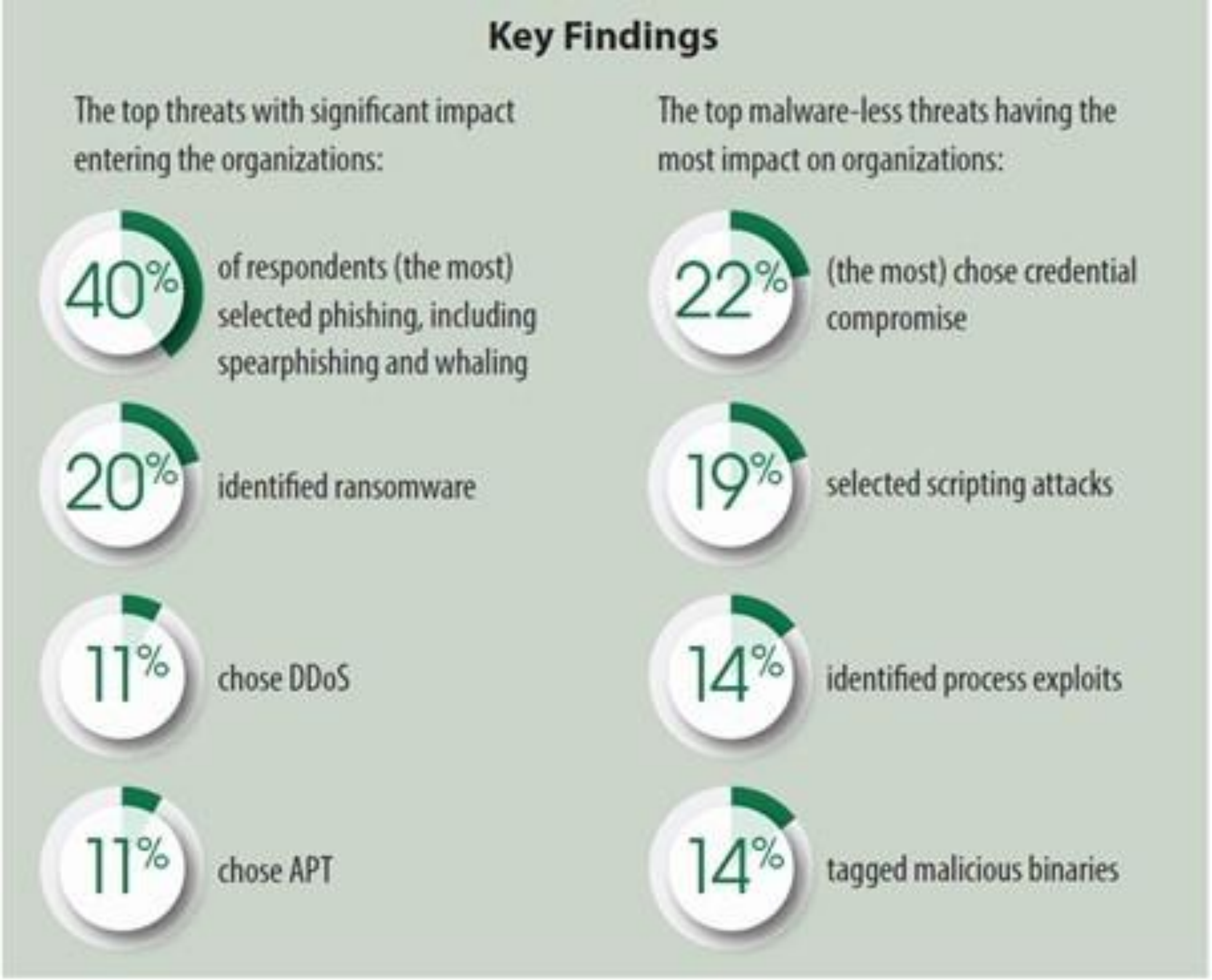
The average cost of a data breach $3M

The penalty for not reporting a breach $2.1M-$10M

PRICELE$$

The cost **to** businesses due to loss of reputation

SANS International
Threat Landscape Survey



Key Findings

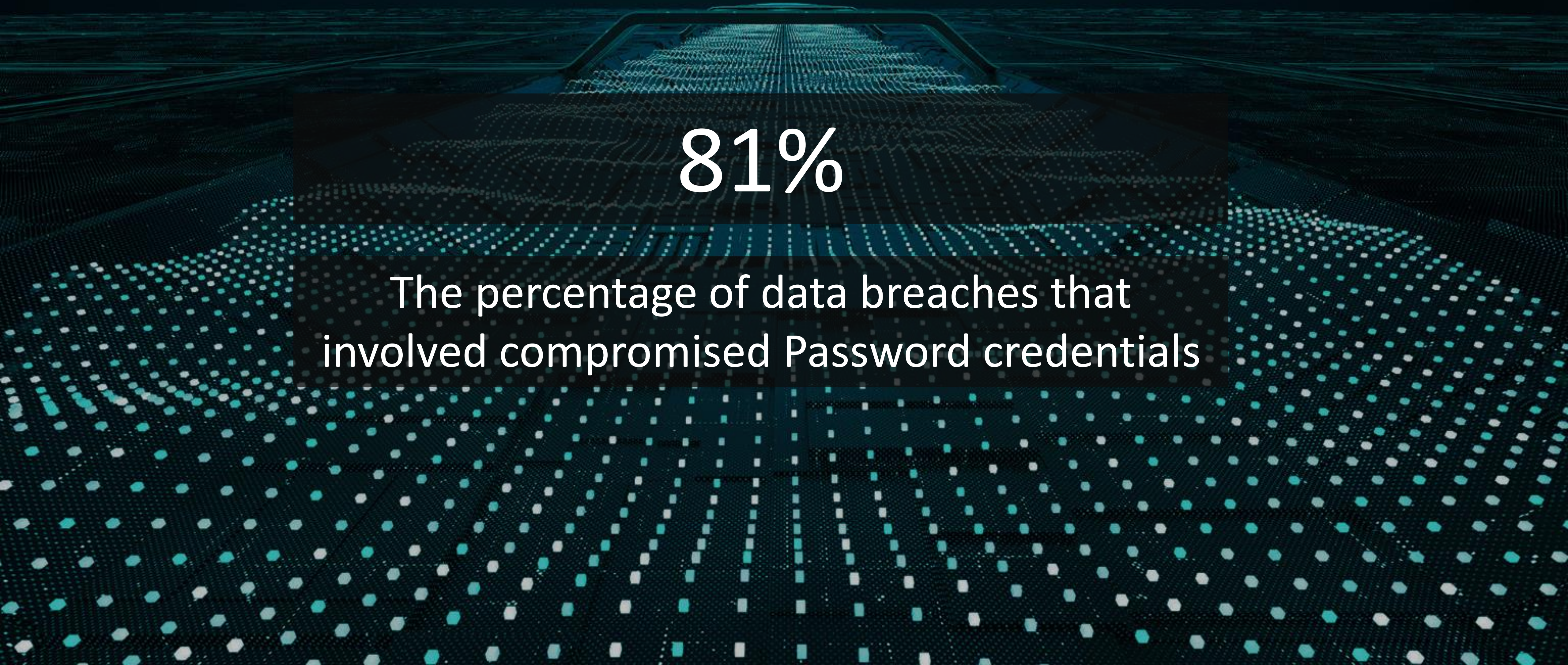
The top threats with significant impact entering the organizations:

- 40% of respondents (the most) selected phishing, including spearphishing and whaling
- 20% identified ransomware
- 11% chose DDoS
- 11% chose APT

The top malware-less threats having the most impact on organizations:

- 22% (the most) chose credential compromise
- 19% selected scripting attacks
- 14% identified process exploits
- 14% tagged malicious binaries

Passwords related Breaches

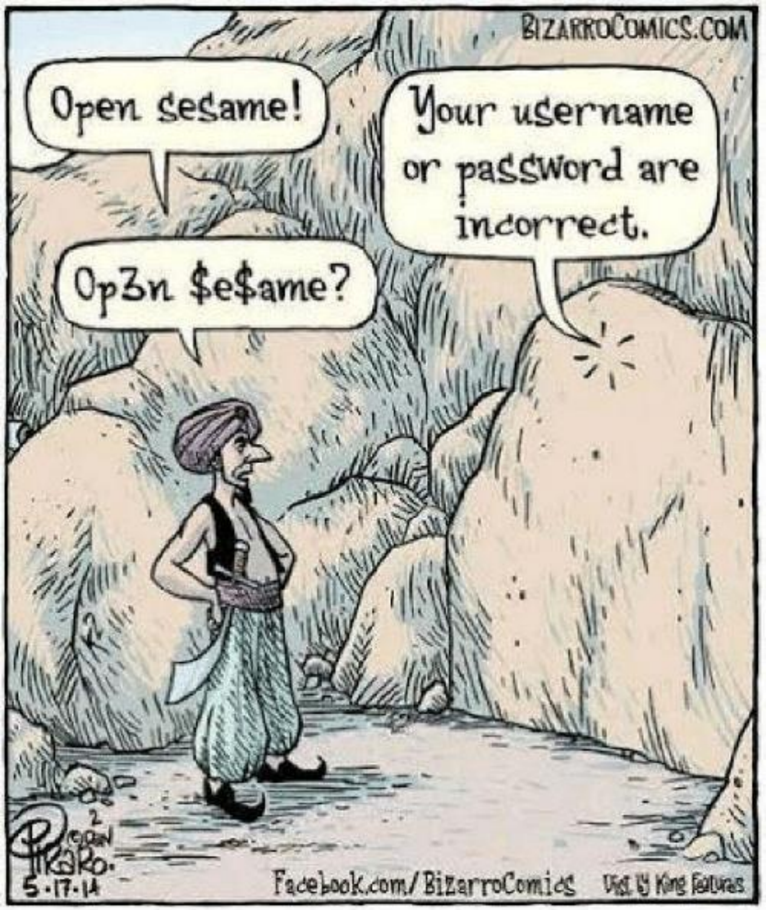


81%

The percentage of data breaches that involved compromised Password credentials

The Problem with Passwords

What is a password?



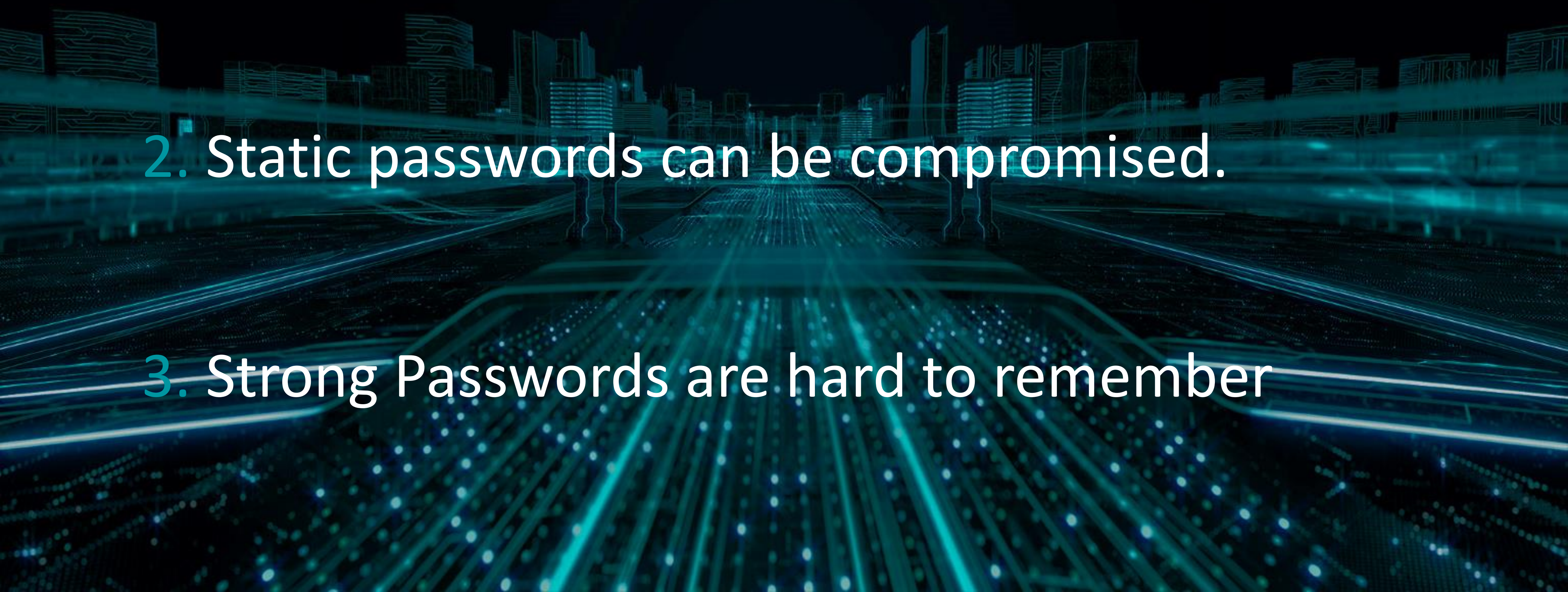
Incorr3ct u$ername

Why Passwords alone are not effective

1. Passwords don’t prove identity

2. Static passwords can be compromised.

3. Strong Passwords are hard to remember



Some alarming password statistics

- 81% of breaches involve weak and compromised passwords
- 70% Employees reuse passwords
- 72% use insecure passwords
- The average cost of a breach in 2018 is $3.86M

Pwn3d

Worldwide, 3 Billion credentials and passwords stolen every year! Many of them ending up for sale or published on the Dark Web.

Check to see if any of your online accounts have been compromised:https://haveibeenpwned.com/

Traditional Approach to Passwords

- Password length and complexity – impossible to remember, get’s written down.
- Password expiration – causes password fatigue frustration and… Password1, gets changed to Password2
- Unique passwords – This defeats the purpose when the same unique password is for EVERYTHING!

Managing Passwords

- Using password management tools eg. KeePass, LastPass, Eset Password Manager
- Using Passphrases: “I catch the 707 bus every morning.”

Better, but still not enough as it still relies on a master password with the same issues.

Better Solutions – Managing Passwords

- Multiple Layered Protection – “Defense in Depth” User Access Control, Anti Malware, Detection capability (SIEM etc)
- Multi Factor Authentication, increases authentication, and difficulty of attack.

Multi Factor Authentication

1. Knowledge Factor - Something only you know

2. Possession Factor - Something only you have

3. Inherence Factor - Something only you are.

What is 2FA

- 2 Factor Authentication is the industry standard for Authentication and Increases the security of Authentication process.

- Renders stolen passwords useless

Why doesn’t everyone use 2FA?

- Myth #1 – Passwords are secure enough
- Myth #2 – It’s too hard to do
- Myth #3 – It’s too expensive

ESET Secure Authentication - Benefits

- Ease of Installation, Deployment and Management.
- Protects multiple logon systems in your environment
- Integrates into Active Directory/Windows Server environment
- Uses multiple types of authentication delivery options

  - Hard Token

  - Mobile Phone App - Push Authentication

  - Text message

ESET Secure Authentication

- Access to your company’s VPN
- Remote Desktop Protocol
- Additional authentication for desktop login (signing into an operating system)
- Web/cloud services via Microsoft ADFS 3.0, such as Office 365
- Microsoft Web Apps, such as OWA
- Exchange Control Panel & Exchange Administrator Center
- VMware Horizon View
- RADIUS-based services
- Easy integration with your RADIUS-based services or via an API to your existing Active Directory-based authentication. Non Active Directory customers with custom systems can use the easy-to-deploy SDK.

Product Demonstration

Questions and Answers

30 YEARS OF
CONTINUOUS
IT SECURITY
INNOVATION