Zero Trust & The Flaming Sword of Justice

How The Security Leader Enables Business Outcomes

Dave Lewis
Global Advisory CISO

May 2023

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

WHOAMI

- Dave Lewis
- Global Advisory CISO, Cisco
- Hacker
- Grey Beard
- Coffee Drinker
- Whisky Distillery Co-Owner
- Football Club Co-Owner

What is love

It’s On Fire Yo!

What is Zero Trust?

- Where/how/when trust is decided has changed
- Must continuously verify
- Assume all networks are hostile
- This is not a “rip & replace” conversation

User

Devices

Network

Apps & Data

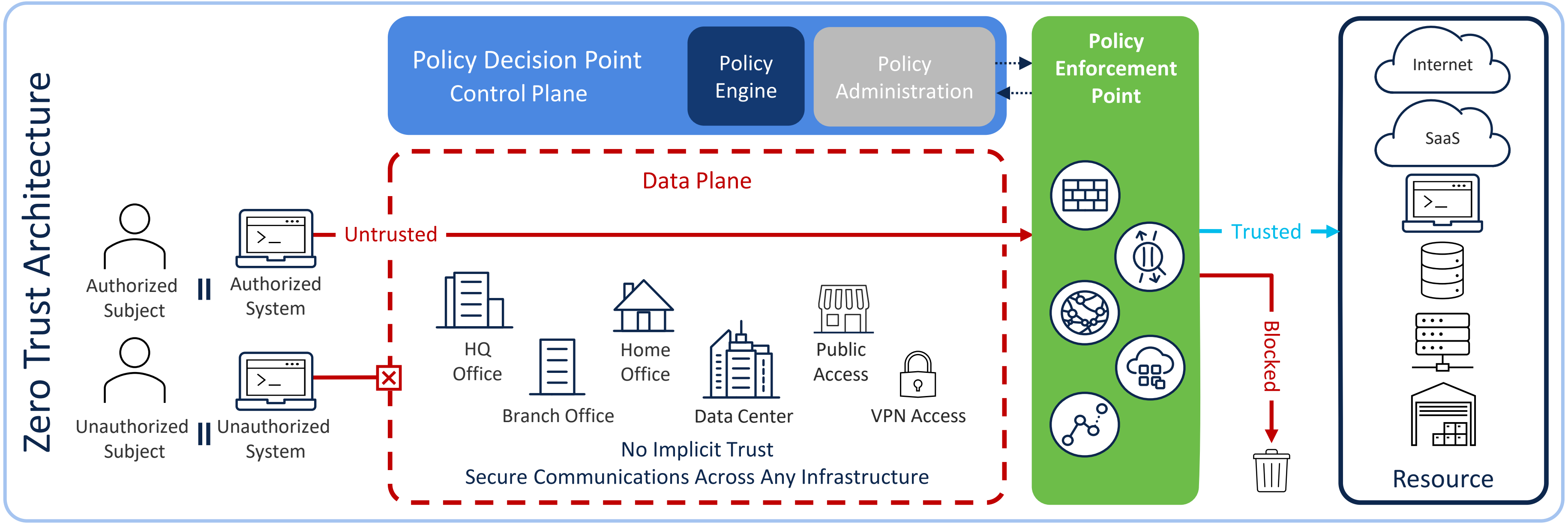
Zero Trust: Principles

- No implicit trust
- Strongly authenticated user
- Strongly authenticated device
- Encrypted connection to resource
- Policy decision and enforcement

(Read the rest at NIST SP 800-207)

CISCO SECURE

NIST SP 800-207: Zero Trust Architecture



Zero Trust capabilities

Establish Trust

Enforce Trust-Based Access

Continuously Verify Trust

Respond to Change in Trust

What it takes to get Zero Trust right

Zero Trust requirements

Establish Trust

- User / device / service identity
- Posture + context
- Risk-based authentication

Enforce Trust-Based Access

- Micro-segmentation
- Unified access control
- Least privilege + explicit trust

Continuously Verify Trust

- Re-assessment of trust
- Indicators of compromise
- Shared signals
- Behavior monitoring — threat and non-threat activity
- Vulnerability management

Respond to Change in Trust

- Prioritized incident response
- Orchestrated remediation
- Integrated + open workflows

User & Device Security

Network & Cloud Security

Application & Data Security

ZTN Value Proposition

Devaluation of stolen credentials

Low hanging fruit sours.

Complicates lateral movement through uniform security policy.

Attackers have to work that much harder.

WORKED FINE IN DEV
OPS PROBLEM NOW
memegenerator.net

Don’t trust something just because it’s on the “inside” of your firewall

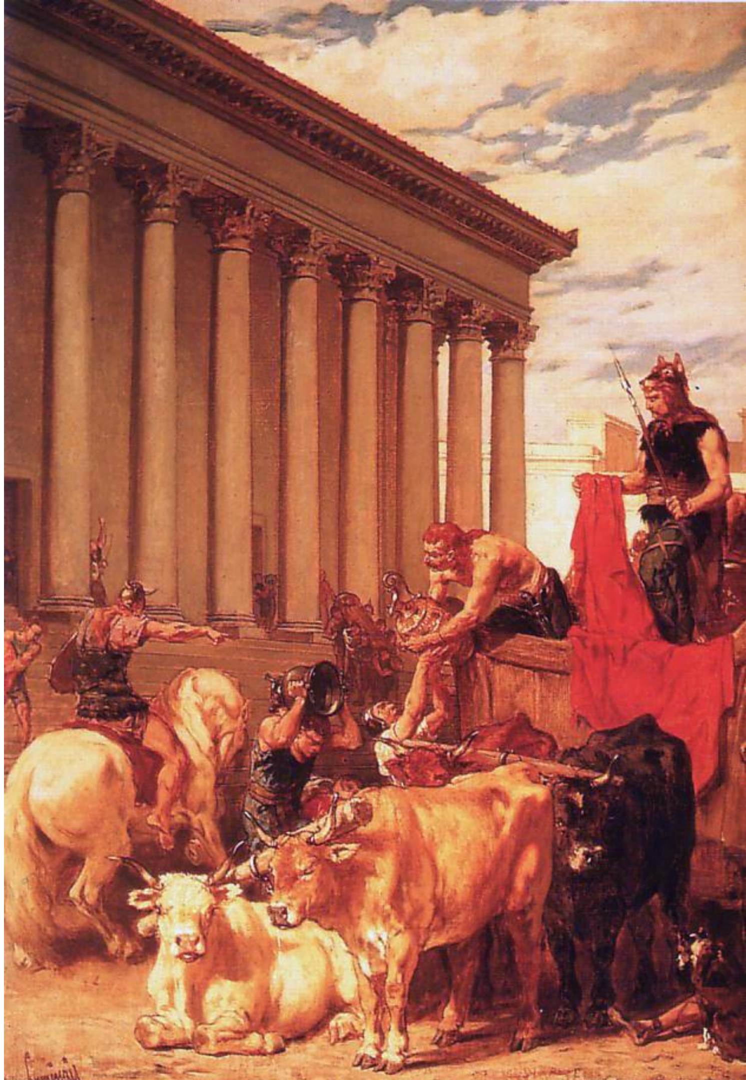
Is the password…password?

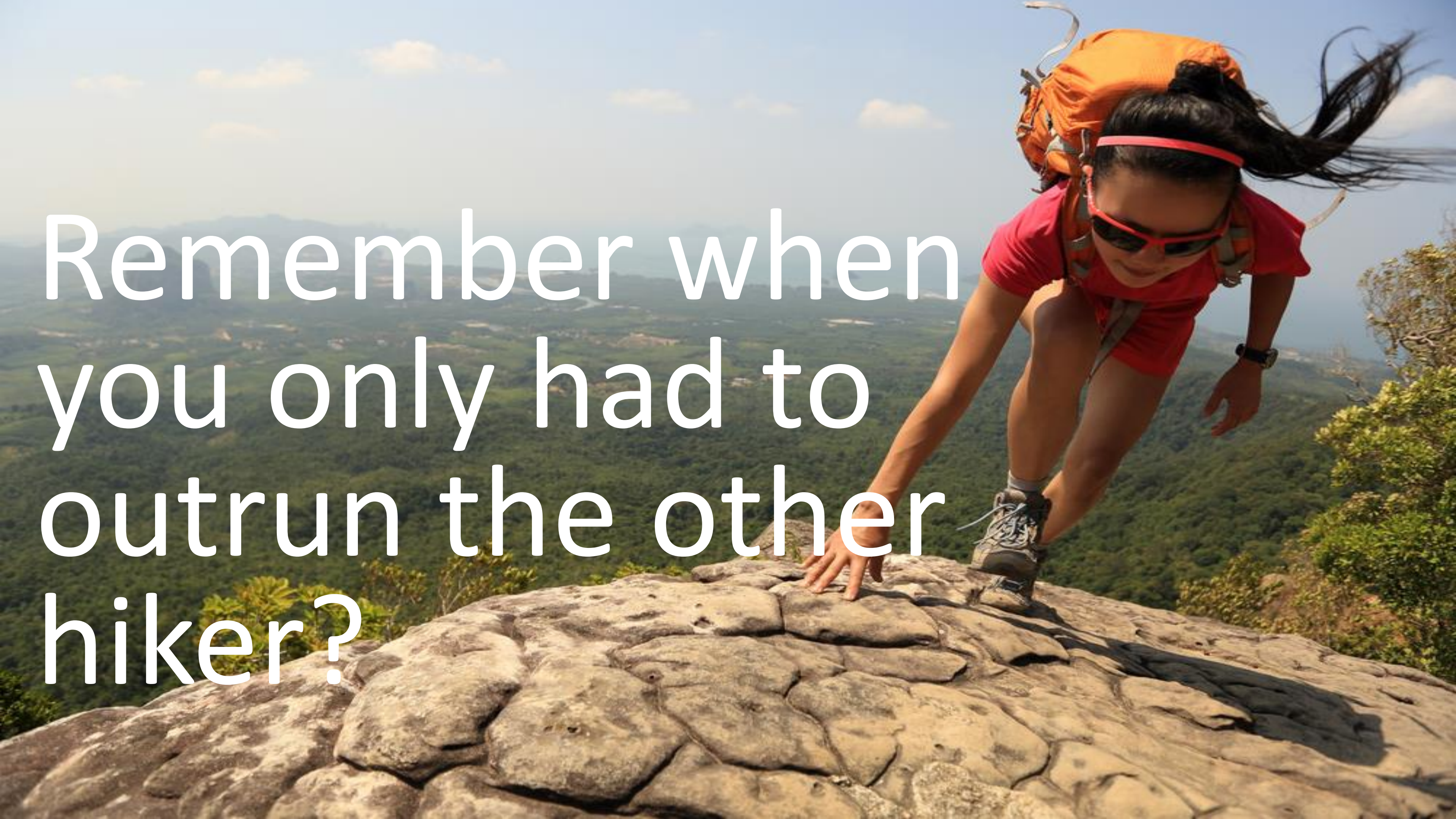
No!! Now go away, or I shall taunt you a second time!

Castles Don’t Scale

Lessons From History

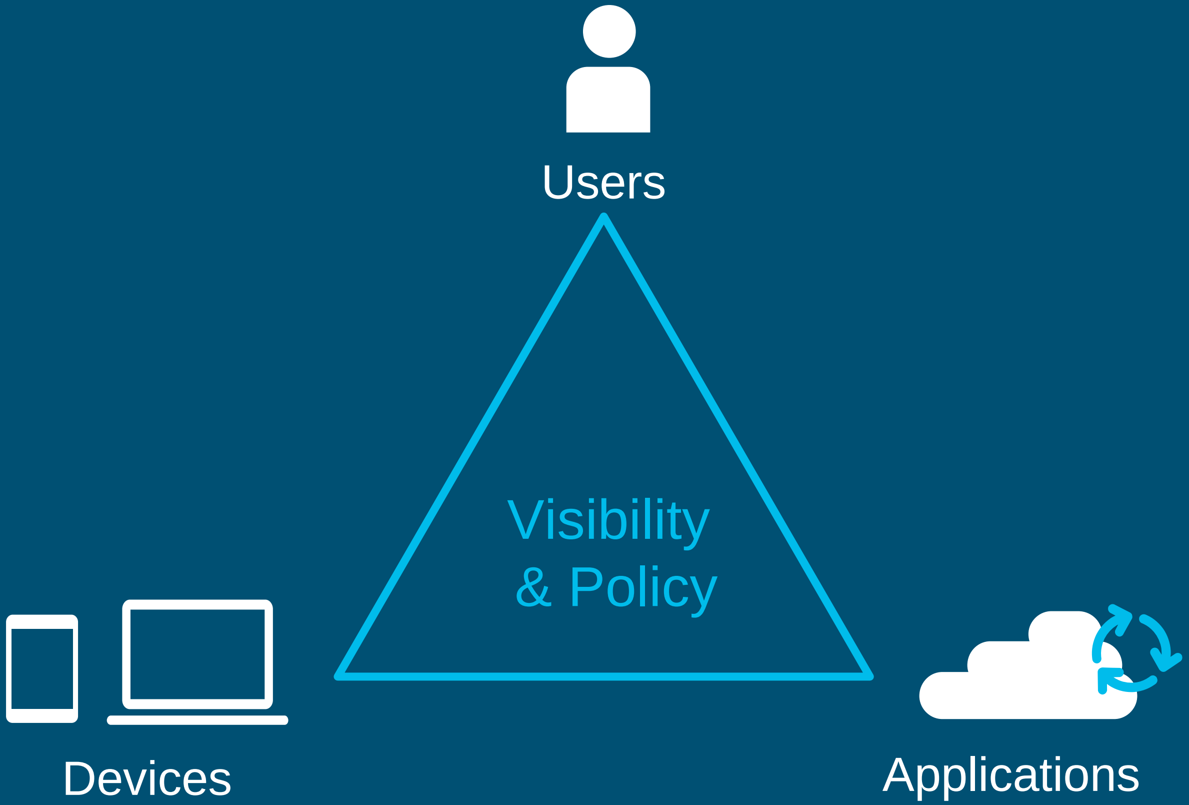
The sack of Rome in 410 AD





Remember when you only had to outrun the other hiker?

Now there’s more than enough bear to go around



Users

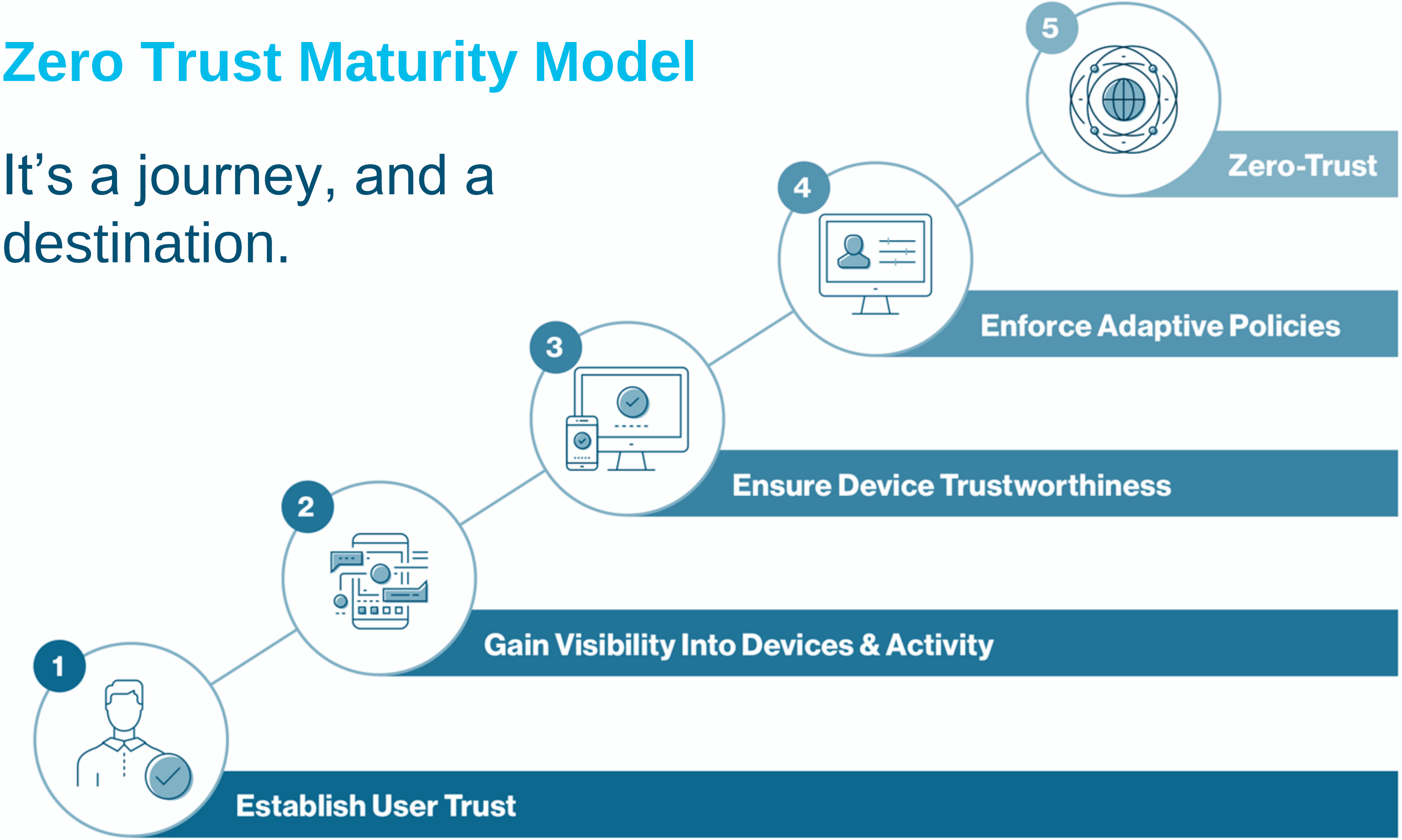
Visibility
& Policy

Devices

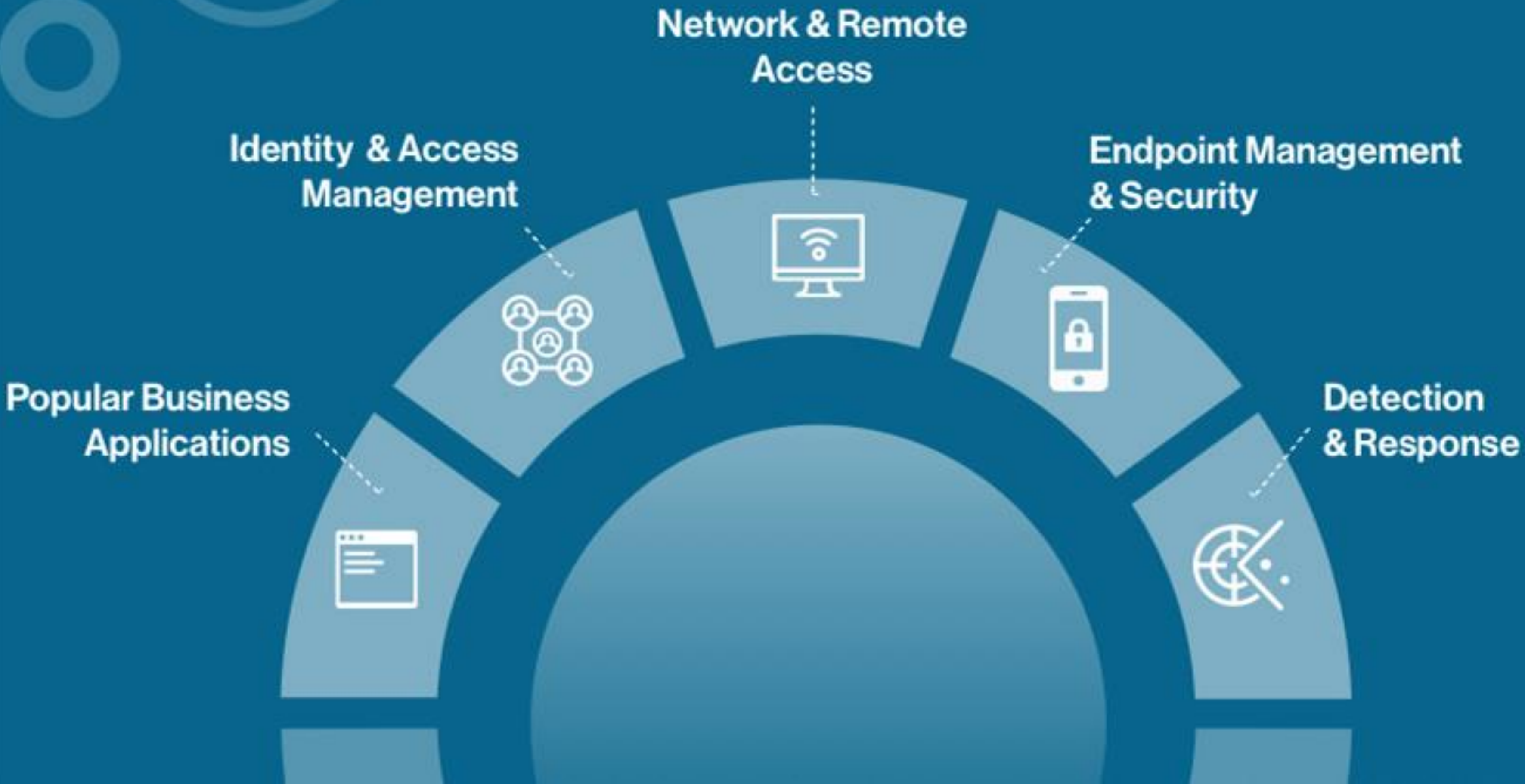
Applications

Zero Trust Maturity Model

It’s a journey, and a destination.


5
Zero-Trust
4
Enforce Adaptive Policies
3
Ensure Device Trustworthiness
2
Gain Visibility Into Devices & Activity
1
Establish User Trust

The Ecosystem

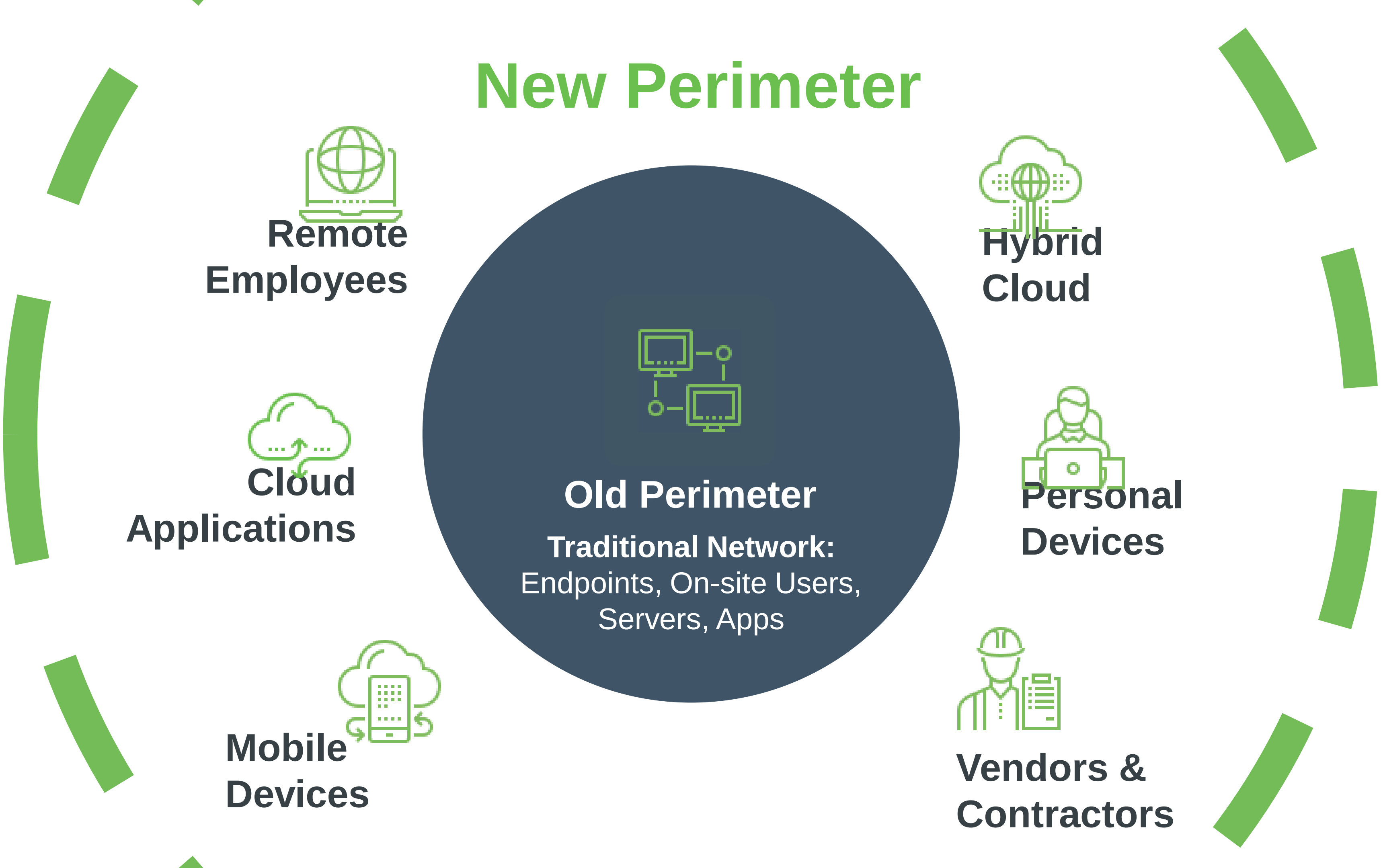


Popular Business Applications
Identity & Access Management
Network & Remote Access
Endpoint Management & Security
Detection & Response

The Flaming Sword of Justice

“The perimeter is anywhere an access decision is being made.”

New Perimeter



Remote Employees

Cloud Applications

Mobile Devices

Old Perimeter

Traditional Network: Endpoints, On-site Users, Servers, Apps

Hybrid Cloud

Personal Devices

Vendors & Contractors

Data Breaches

81%

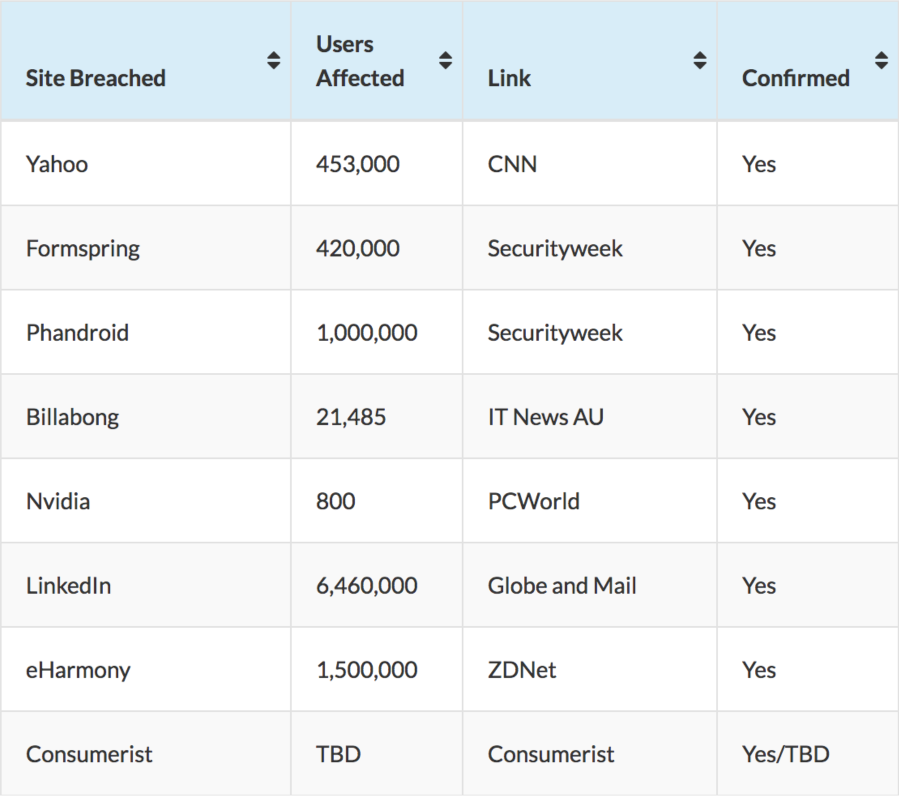
Of breaches involve stolen or weak **credentials**

70%

Of breaches involve compromised **devices**

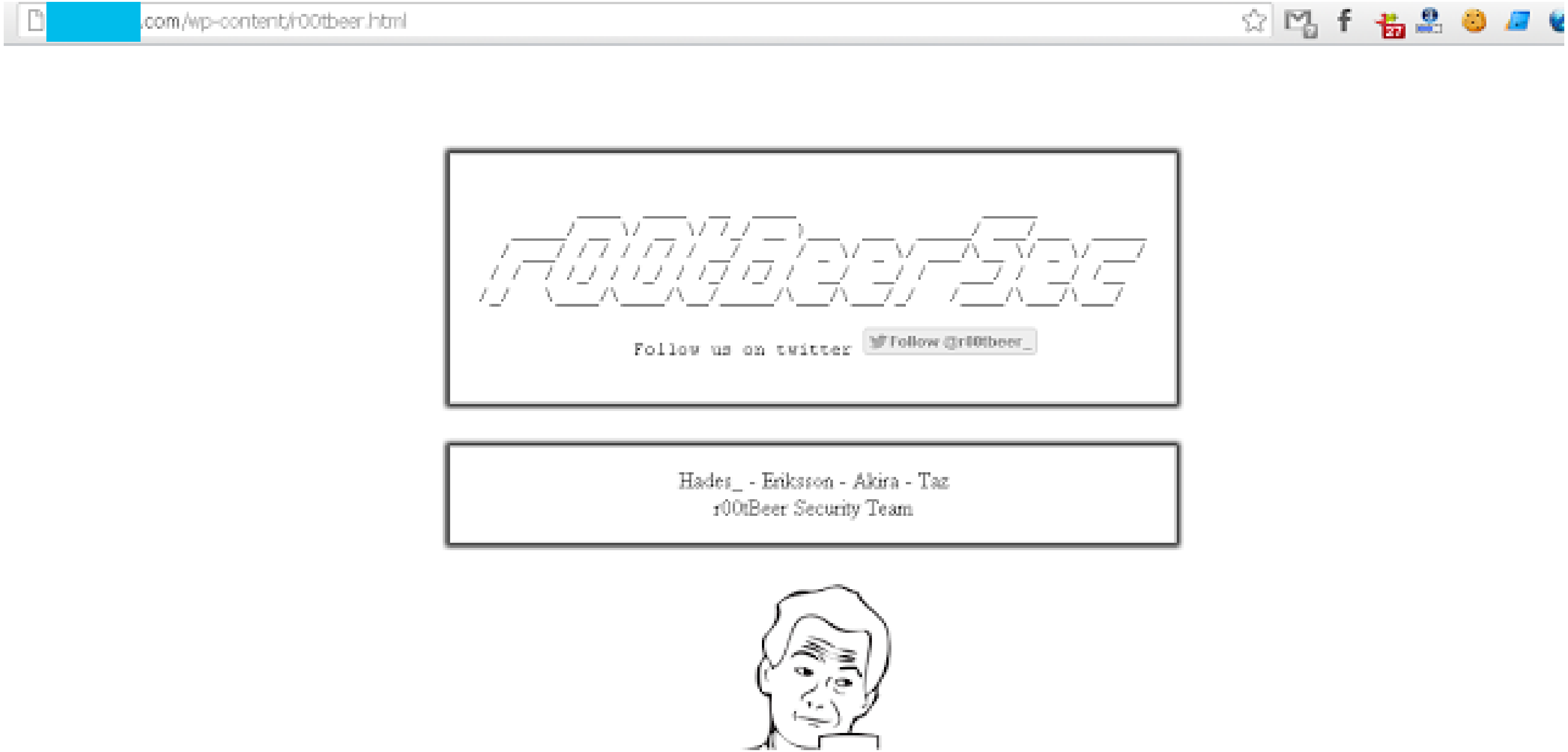
Sources: Verizon DBIR, IDC Research

The Summer of Breach 2012



Site Breached	Users Affected	Link	Confirmed
Yahoo	453,000	CNN	Yes
Formspring	420,000	Securityweek	Yes
Phandroid	1,000,000	Securityweek	Yes
Billabong	21,485	IT News AU	Yes
Nvidia	800	PCWorld	Yes
LinkedIn	6,460,000	Globe and Mail	Yes
eHarmony	1,500,000	ZDNet	Yes
Consumerist	TBD	Consumerist	Yes/TBD

Been There...

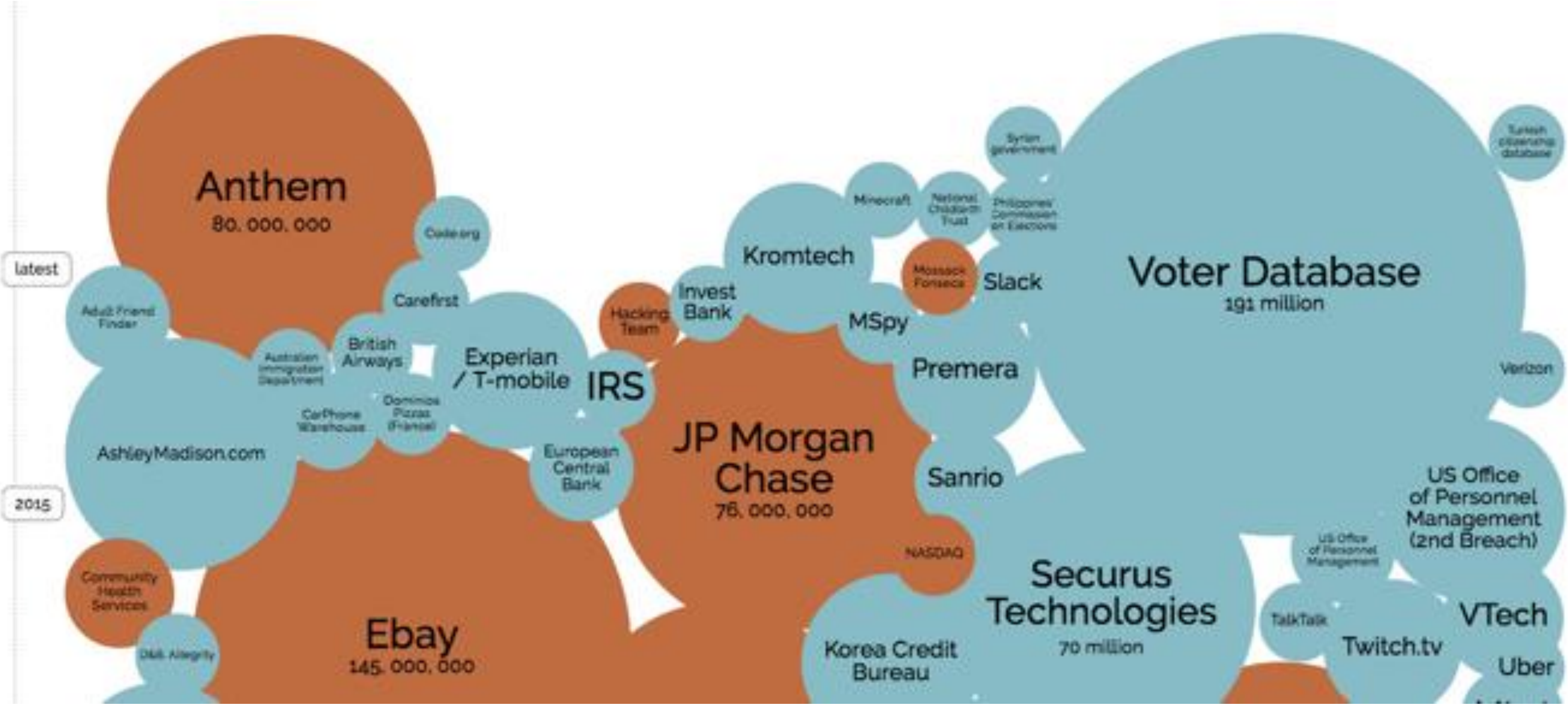


[redacted].com/wp-content/r00tbeer.html

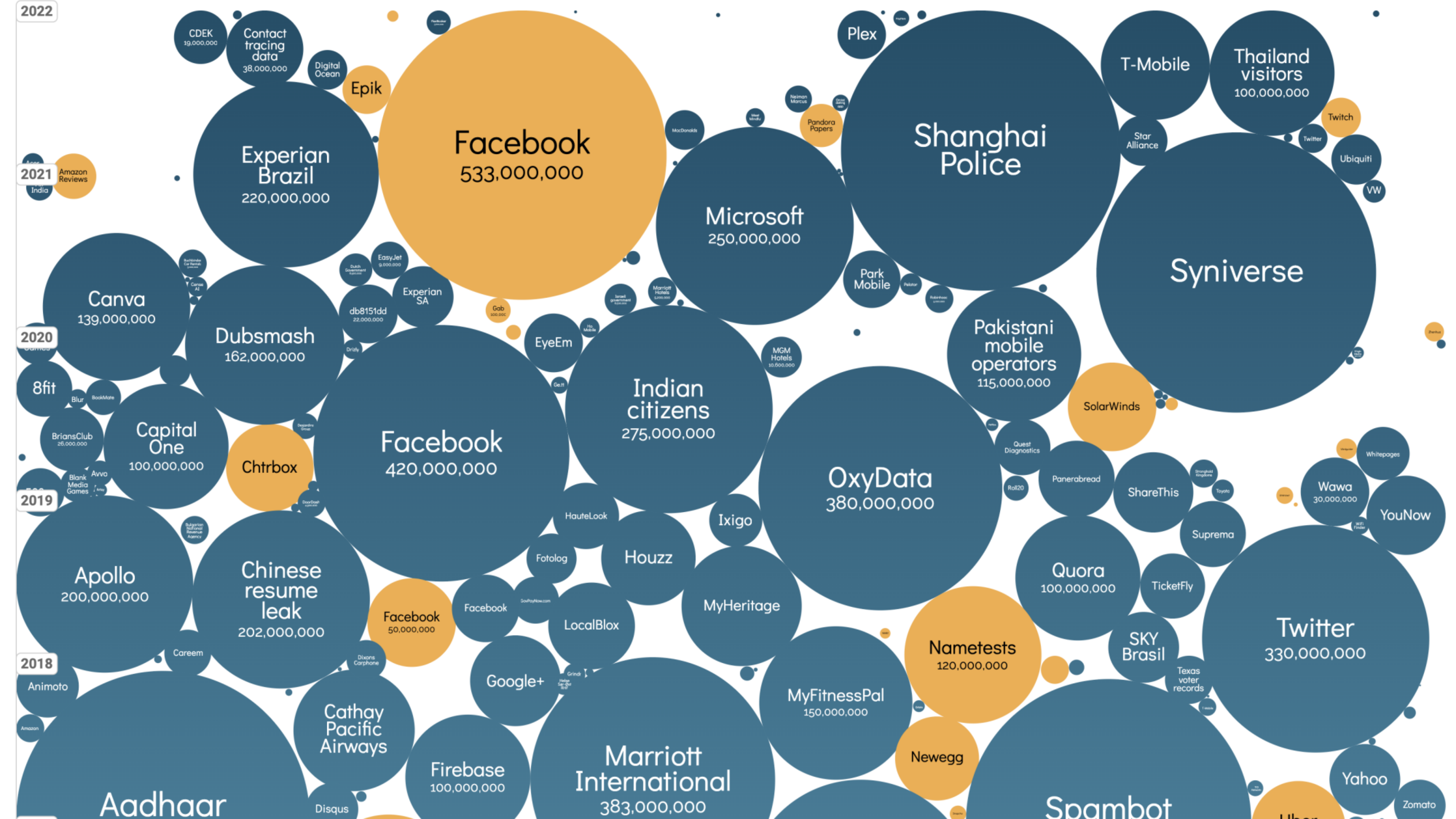
r00tBeerSec

Follow us on twitter

Hades_ - Eriksson - Akira - Taz
r00tBeer Security Team


latest
2015
Anthem
80. 000. 000
Code.org
Adult Friend Finder
Carefirst
British Airways
Australian Immigration Department
Experian / T-mobile
IRS
Hacking Team
Invest Bank
Kromtech
Minecraft
National Childbirth Trust
Syrian government
Philippines' Commission on Elections
Mossack Fonseca
Slack
MSpy
Premera
Voter Database
191 million
Turkish citizenship database
Verizon
CarPhone Warehouse
Dominos Pizzas (France)
AshleyMadison.com
European Central Bank
JP Morgan Chase
76. 000. 000
Sanrio
NASDAQ
US Office of Personnel Management (2nd Breach)
US Office of Personnel Management
Community Health Services
D&B. Allegrity
Ebay
145. 000. 000
Korea Credit Bureau
Securus Technologies
70 million
TalkTalk
Twitch.tv
VTech
Uber

YEARS AGO...


2022
CDEK 19,000,000
Contact tracing data 38,000,000
Digital Ocean
Epik
Facebook 533,000,000
Plex
Shanghai Police
T-Mobile
Thailand visitors 100,000,000
Twitch
Star Alliance
Twitter
Ubiquiti
VW
Neiman Marcus
Pandora Papers
MacDonalds
Microsoft 250,000,000
2021
Amazon Reviews
India
Experian Brazil 220,000,000
Syniverse
Canva 139,000,000
EasyJet 9,000,000
Dutch Government
Experian SA
db8151dd 22,000,000
Gab
Israeli government
Marriott Hotels
Park Mobile
Peloton
Robinhood
Dubsmash 162,000,000
2020
EyeEm
Drizly
MGM Hotels 10,600,000
Pakistani mobile operators 115,000,000
8fit
Blur
BookMate
Indian citizens 275,000,000
SolarWinds
Facebook 420,000,000
Ge.tt
BriansClub 26,000,000
Capital One 100,000,000
Desjardins Group
Chtrbox
OxyData 380,000,000
Quest Diagnostics
Whitepages
Roll20
Panerabread
ShareThis
Wawa 30,000,000
Blank Media Games
Avvo
DoorDash
2019
HauteLook
Ixigo
Suprema
YouNow
Bulgarian National Revenue Agency
Apollo 200,000,000
Chinese resume leak 202,000,000
Fotolog
Houzz
Quora 100,000,000
TicketFly
Facebook 50,000,000
Facebook
LocalBlox
MyHeritage
Twitter 330,000,000
Nametests 120,000,000
Careem
Dixons Carphone
SKY Brasil
2018
Animoto
Google+
Grindr
Texas voter records
MyFitnessPal 150,000,000
Amazon
Cathay Pacific Airways
Newegg
Yahoo
Firebase 100,000,000
Marriott International 383,000,000
Aadhaar
Disqus
Spambot
Zomato

What’s Open In Portugal?

1,000,276

So, Why Should We Be Concerned?

418

Vulnerable to Heartbleed

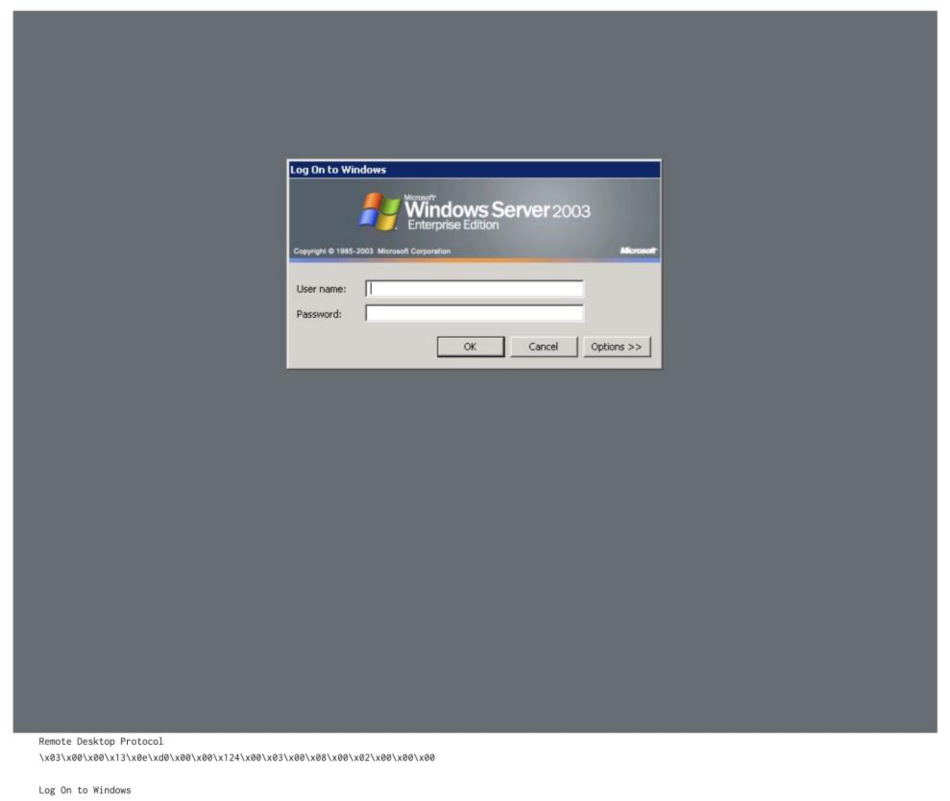
4

Compromised Databases

602

Industrial Control Systems

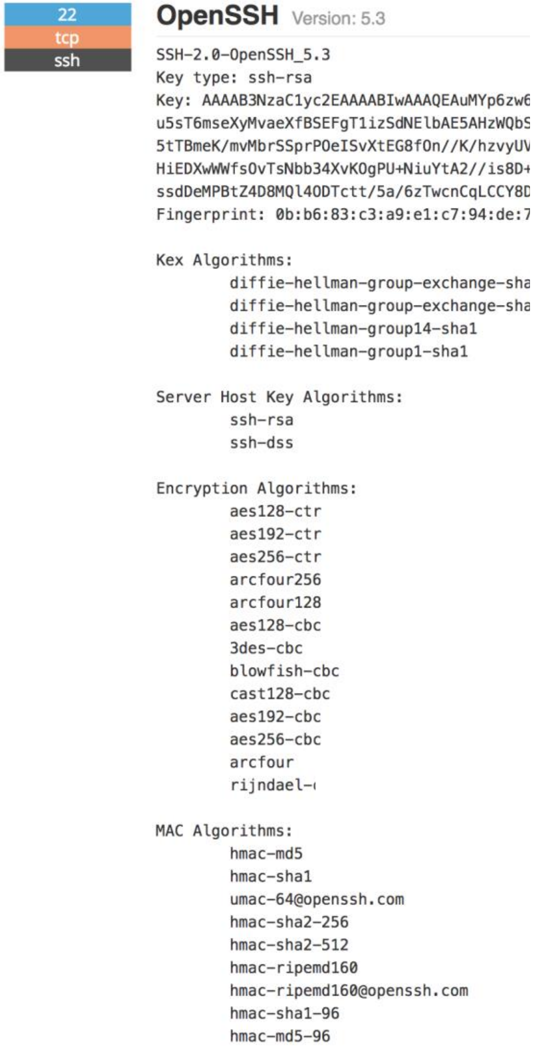
Hi There!



```
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x03\x00\x08\x00\x02\x00\x00\x00

Log On to Windows
```

SSH



OpenSSH Version: 5.3

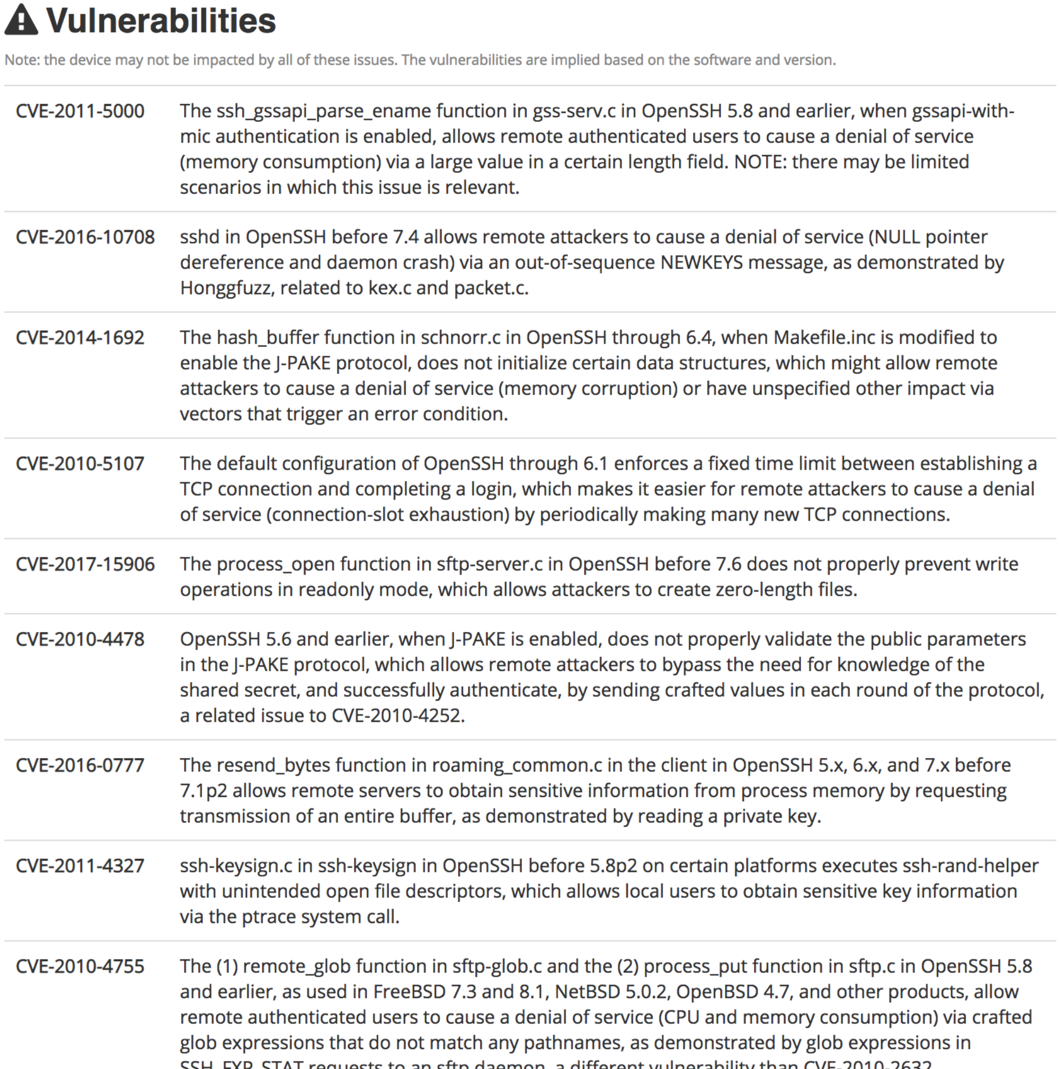
```
SSH-2.0-OpenSSH_5.3
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAABIwAAAQEAuMYp6zw6
u5sT6mseXyMvaeXfBSEFgT1izSdNElbAE5AHzWQbS
5tTBmeK/mvMbrSSprPOeISvXtEG8fOn//K/hzvyUV
HiEDXwWWfsOvTsNbb34XvKOgPU+NiuYtA2//is8D+
ssdDeMPBtZ4D8MQl4ODTctt/5a/6zTwcnCqLCCY8D
Fingerprint: 0b:b6:83:c3:a9:e1:c7:94:de:7

Kex Algorithms:
        diffie-hellman-group-exchange-sha
        diffie-hellman-group-exchange-sha
        diffie-hellman-group14-sha1
        diffie-hellman-group1-sha1

Server Host Key Algorithms:
        ssh-rsa
        ssh-dss

Encryption Algorithms:
        aes128-ctr
        aes192-ctr
        aes256-ctr
        arcfour256
        arcfour128
        aes128-cbc
        3des-cbc
        blowfish-cbc
        cast128-cbc
        aes192-cbc
        aes256-cbc
        arcfour
        rijndael-

MAC Algorithms:
        hmac-md5
        hmac-sha1
        umac-64@openssh.com
        hmac-sha2-256
        hmac-sha2-512
        hmac-ripemd160
        hmac-ripemd160@openssh.com
        hmac-sha1-96
        hmac-md5-96
```

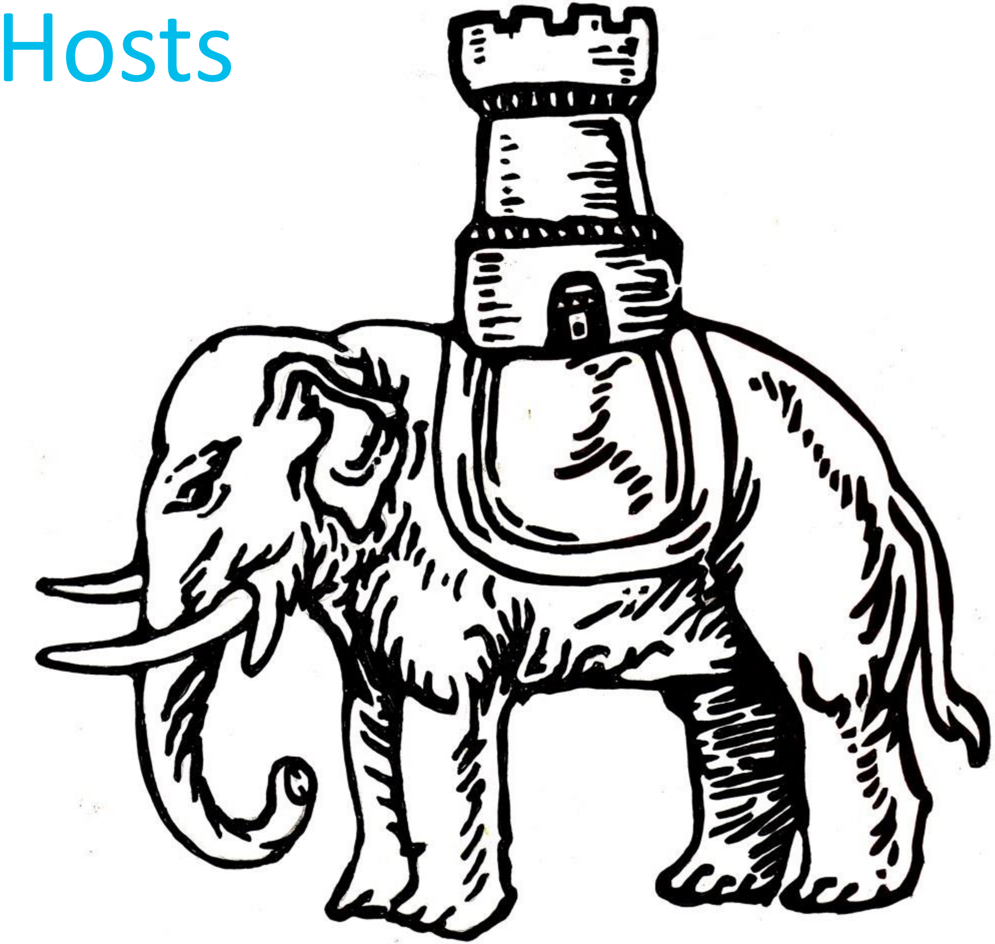


⚠ Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2011-5000	The ssh_gssapi_parse_ename function in gss-serv.c in OpenSSH 5.8 and earlier, when gssapi-with-mic authentication is enabled, allows remote authenticated users to cause a denial of service (memory consumption) via a large value in a certain length field. NOTE: there may be limited scenarios in which this issue is relevant.
CVE-2016-10708	sshd in OpenSSH before 7.4 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence NEWKEYS message, as demonstrated by Honggfuzz, related to kex.c and packet.c.
CVE-2014-1692	The hash_buffer function in schnorr.c in OpenSSH through 6.4, when Makefile.inc is modified to enable the J-PAKE protocol, does not initialize certain data structures, which might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition.
CVE-2010-5107	The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.
CVE-2017-15906	The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.
CVE-2010-4478	OpenSSH 5.6 and earlier, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol, a related issue to CVE-2010-4252.
CVE-2016-0777	The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.
CVE-2011-4327	ssh-keysign.c in ssh-keysign in OpenSSH before 5.8p2 on certain platforms executes ssh-rand-helper with unintended open file descriptors, which allows local users to obtain sensitive key information via the ptrace system call.
CVE-2010-4755	The (1) remote_glob function in sftp-glob.c and the (2) process_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH_FXP_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632

Bastion Hosts



From DMZ To The Soft Chewy Centre

A Game of Increments

Determining Priorities

1

How do you stop attacks that use stolen (yet legitimate) credentials?

2

How do you prevent devices with poor security hygiene from accessing critical apps?

Security Best Practices

Policies Are Unique to Each User and Device

Verify Your Users

- Strong Authentication
- Intuitive Authentication
- User Risk Assessment

Verify Their Devices

- Up-to-date Devices
- Well-configured Devices
- Managed Devices
- Device Authentication

Protect Every Application

- All Cloud Apps
- All On-Prem Apps
- Consistent End User Experience & Security

Example: Stolen Credentials

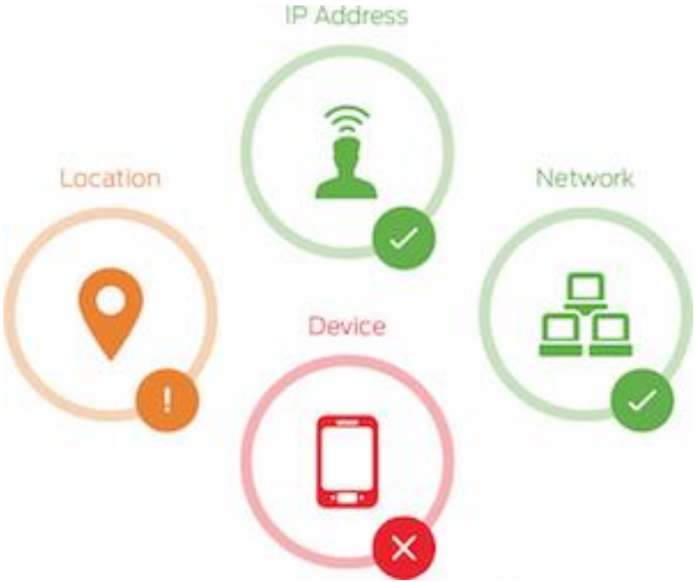
Attackers must compromise:

- Username
- Password
- 2nd auth factor
- Trusted device

Enforce Policy Based Controls

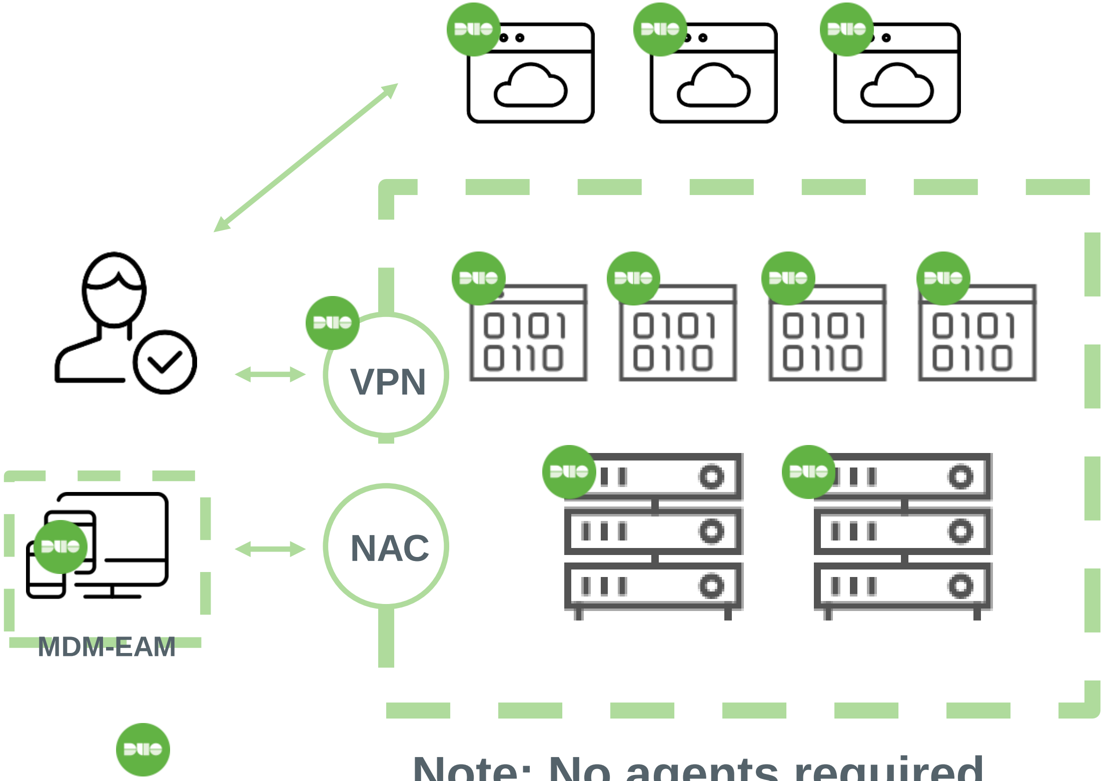
Get Granular

- Block anonymous networks, out-of-date browsers and plugins, and rooted or jailbroken devices
- Require users to enable screen-lock and use U2F or push authentication
- Ensure all systems are up-to-date

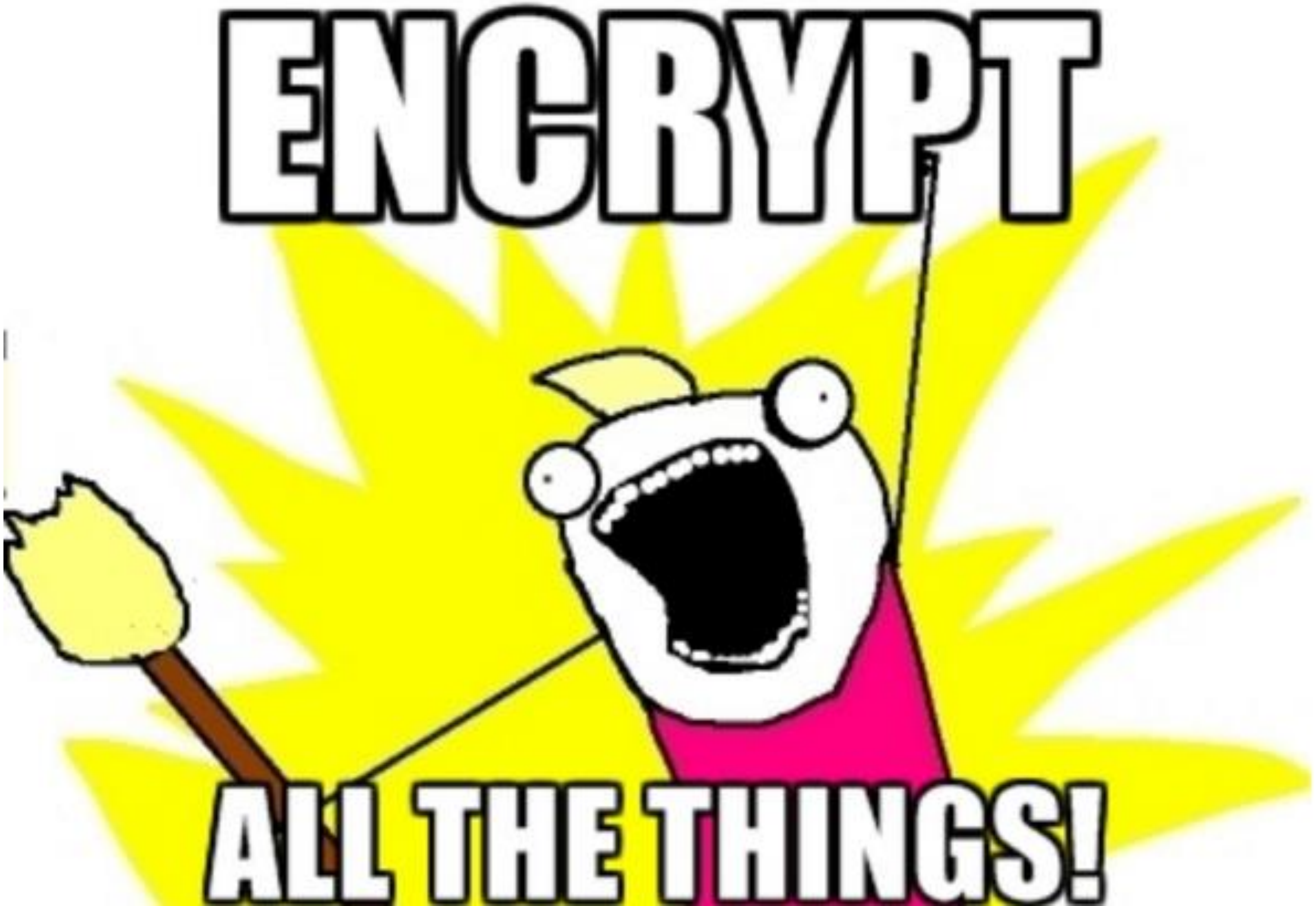


Trusted Access: leverage your existing investments

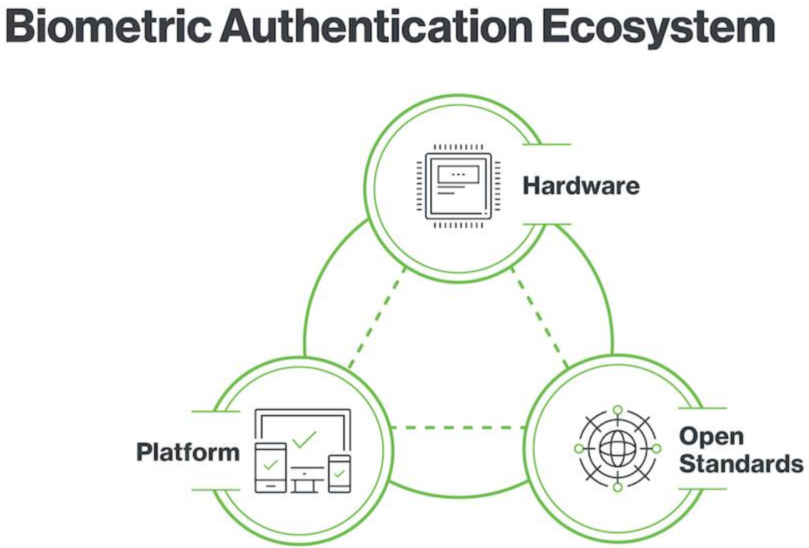
- Secure VPNs with MFA and device-level hygiene
- Ensure only managed devices can access network or cloud apps leveraging MDM agents
- Easily add protection for cloud apps in addition to your on-prem NAC



Note: No agents required


ENCRYPT
ALL THE THINGS!

Webauthn


Biometric Authentication Ecosystem
Hardware
Platform
Open Standards

ZTN Summary

Build an asset inventory.

Get a solid hold on user management.

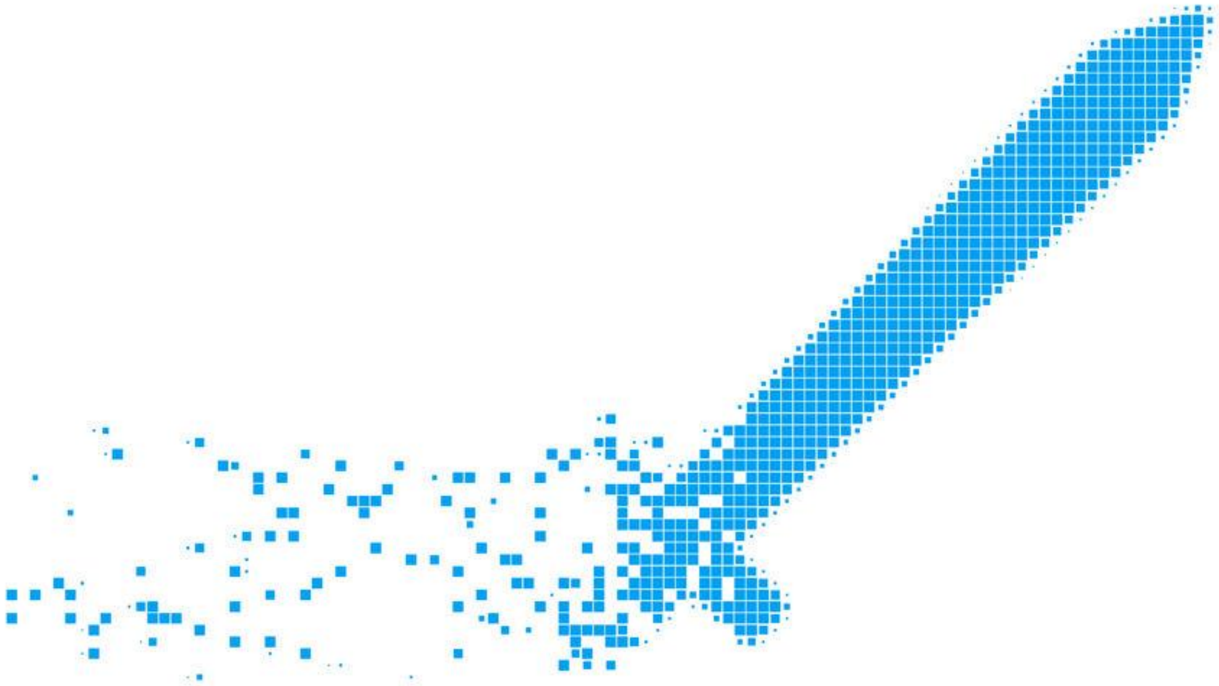
What’s on your network?

Defined Repeatable Process

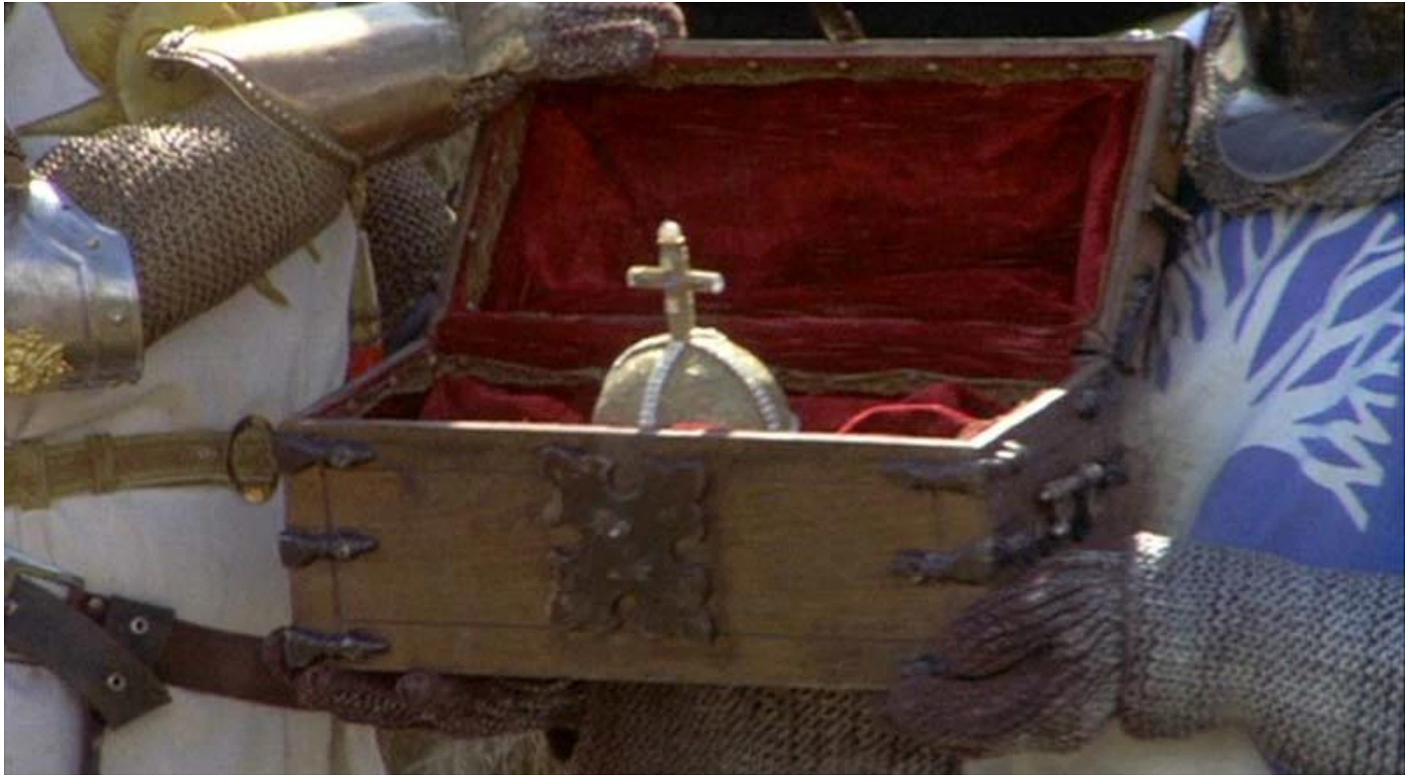
User and Entity Behavior Analytics.

Network Zone Segmentation.

The Sword Is Dissolving



No Need For The Holy Hand Grenade



Thanks!

gattaca@cisco.com
@gattaca@infosec.exchange

cisco