Zero Trust & The Flaming Sword of Justice

Dave Lewis, Global Advisory CISO

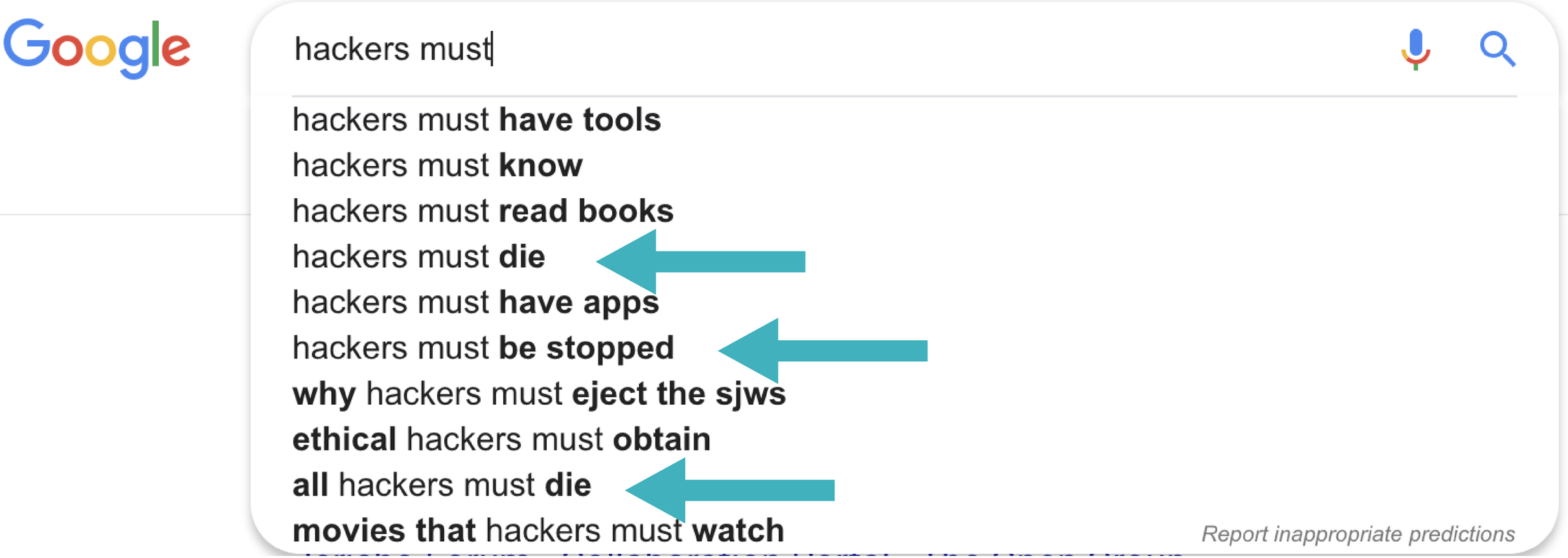
Duo Security, Cisco

@gattaca

Please Allow Me To Introduce Myself..

#WHOAMI

Dave Lewis, Global Advisory CISO


Google
hackers must
hackers must have tools
hackers must know
hackers must read books
hackers must die
hackers must have apps
hackers must be stopped
why hackers must eject the sjws
ethical hackers must obtain
all hackers must die
movies that hackers must watch
Report inappropriate predictions


MATTHEWS
34


CISCO

MENU

US EN

Products & Services / Security /

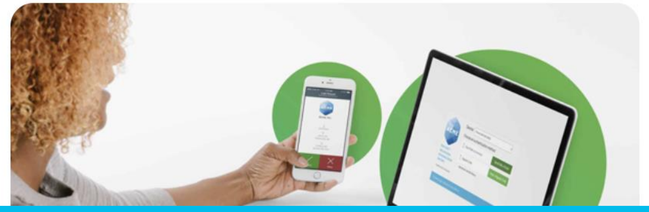
Adaptive Multi-Factor Authentication (MFA)

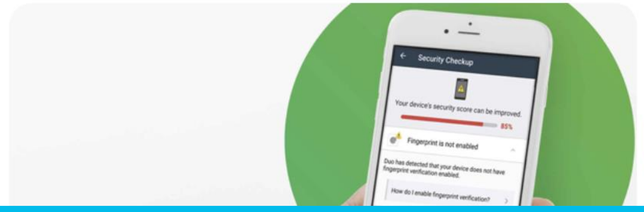
Proactively reduce the risk of a data breach with Duo. Verify users' identities, gain visibility into every device, and enforce adaptive policies to secure access to every application.

Learn more about Duo

Try Duo for free

User and device trust for every application






Our mission
is to protect
your mission.

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

ZTN

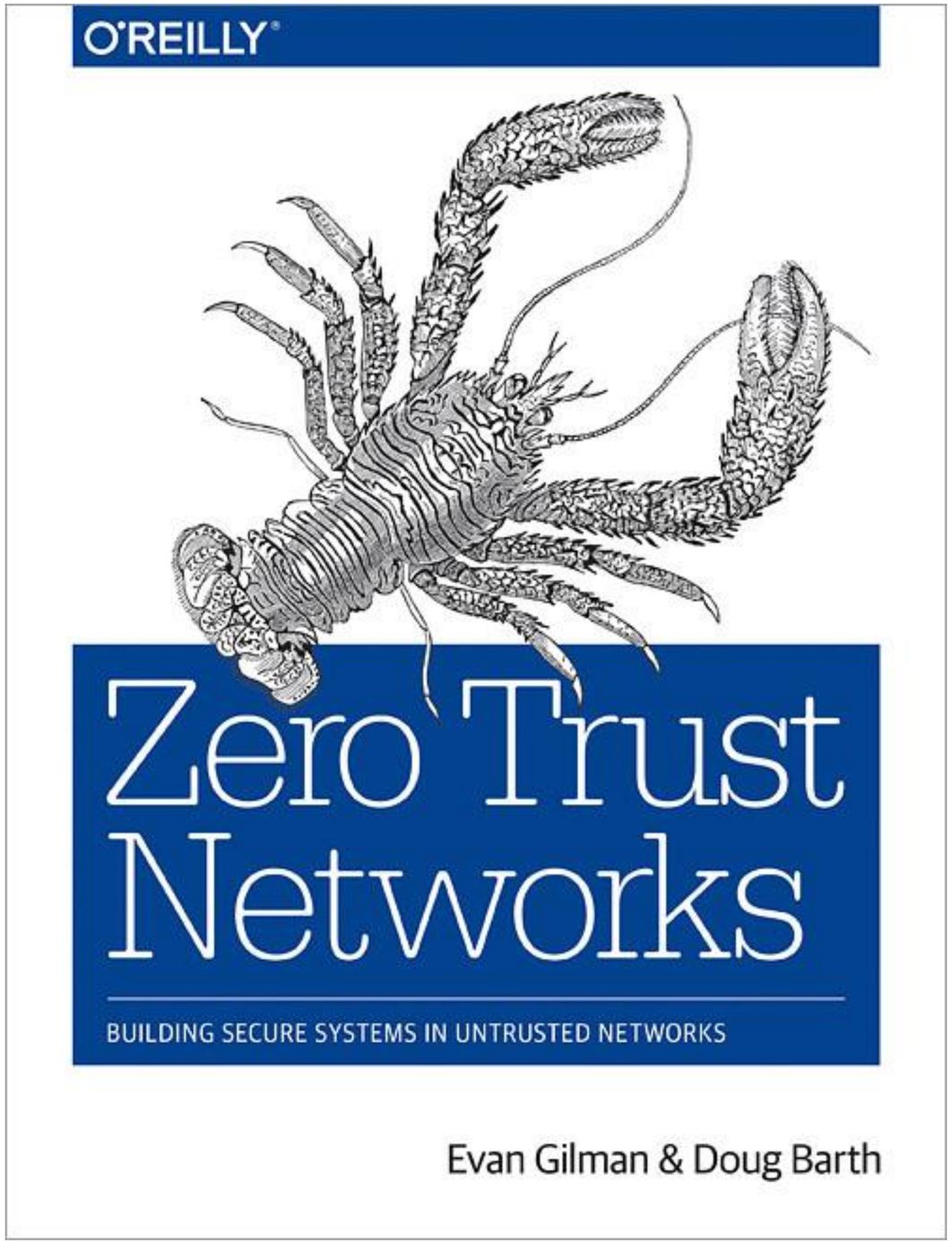
DUO


It’s On Fire Yo!


WORKED FINE IN DEV
OPS PROBLEM NOW
memegenerator.net

What is Zero Trust?

- 2004(ish) - Jericho Forum
- 2010 - John Kindervag, coined term ‘Zero Trust’
- 2014 - Google BeyondCorp
- 2017 - O’Reilly Zero Trust Networks


O'REILLY
Zero Trust Networks
BUILDING SECURE SYSTEMS IN UNTRUSTED NETWORKS
Evan Gilman & Doug Barth

Change in IT Landscape

With a shift to cloud and mobile-first world, a new approach to security is needed.

Cloud

Mobile

Anywhere

Shift to Zero Trust Trends

Security/IT teams need to enable user access, from any device and anywhere, while preventing breaches.

Enable Multi- Cloud Access

- Cloud infrastructure
- SaaS apps

Enable BYOD

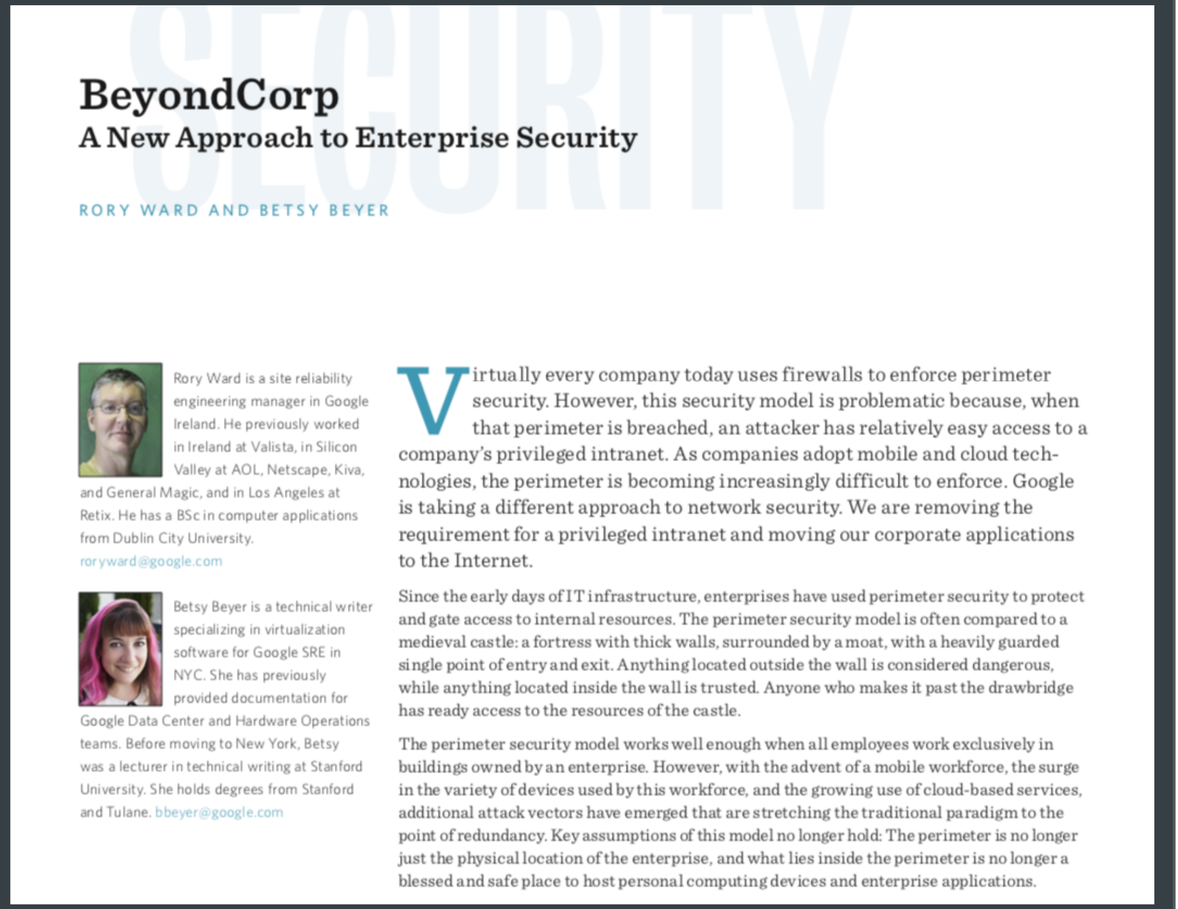
- Work from anywhere using personal devices
- Third-parties, contractors, etc.

Breach Prevention

- Compromised credentials
- Phishing

What is BeyondCorp?

- 2014 - Google BeyondCorp paper
- 2016 - Google BeyondCorp progress update
- 2017 - BeyondCorp migration, user experience and lessons learned



SECURITY

BeyondCorp
A New Approach to Enterprise Security

RORY WARD AND BETSY BEYER

Rory Ward is a site reliability engineering manager in Google Ireland. He previously worked in Ireland at Valista, in Silicon Valley at AOL, Netscape, Kiva, and General Magic, and in Los Angeles at Retix. He has a BSc in computer applications from Dublin City University. roryward@google.com

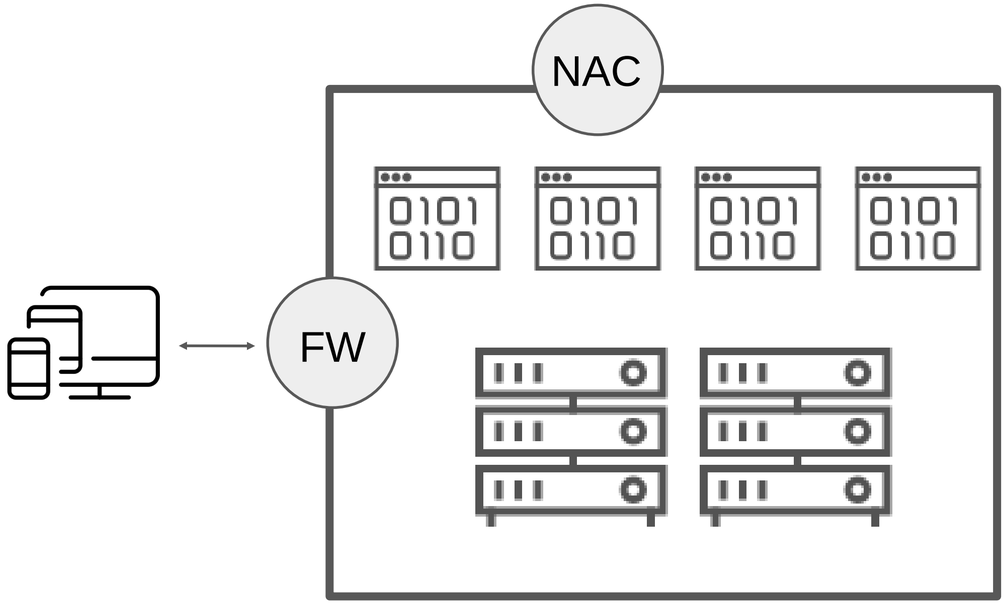
Betsy Beyer is a technical writer specializing in virtualization software for Google SRE in NYC. She has previously provided documentation for Google Data Center and Hardware Operations teams. Before moving to New York, Betsy was a lecturer in technical writing at Stanford University. She holds degrees from Stanford and Tulane. bbeyer@google.com

Virtually every company today uses firewalls to enforce perimeter security. However, this security model is problematic because, when that perimeter is breached, an attacker has relatively easy access to a company's privileged intranet. As companies adopt mobile and cloud technologies, the perimeter is becoming increasingly difficult to enforce. Google is taking a different approach to network security. We are removing the requirement for a privileged intranet and moving our corporate applications to the Internet.

Since the early days of IT infrastructure, enterprises have used perimeter security to protect and gate access to internal resources. The perimeter security model is often compared to a medieval castle: a fortress with thick walls, surrounded by a moat, with a heavily guarded single point of entry and exit. Anything located outside the wall is considered dangerous, while anything located inside the wall is trusted. Anyone who makes it past the drawbridge has ready access to the resources of the castle.

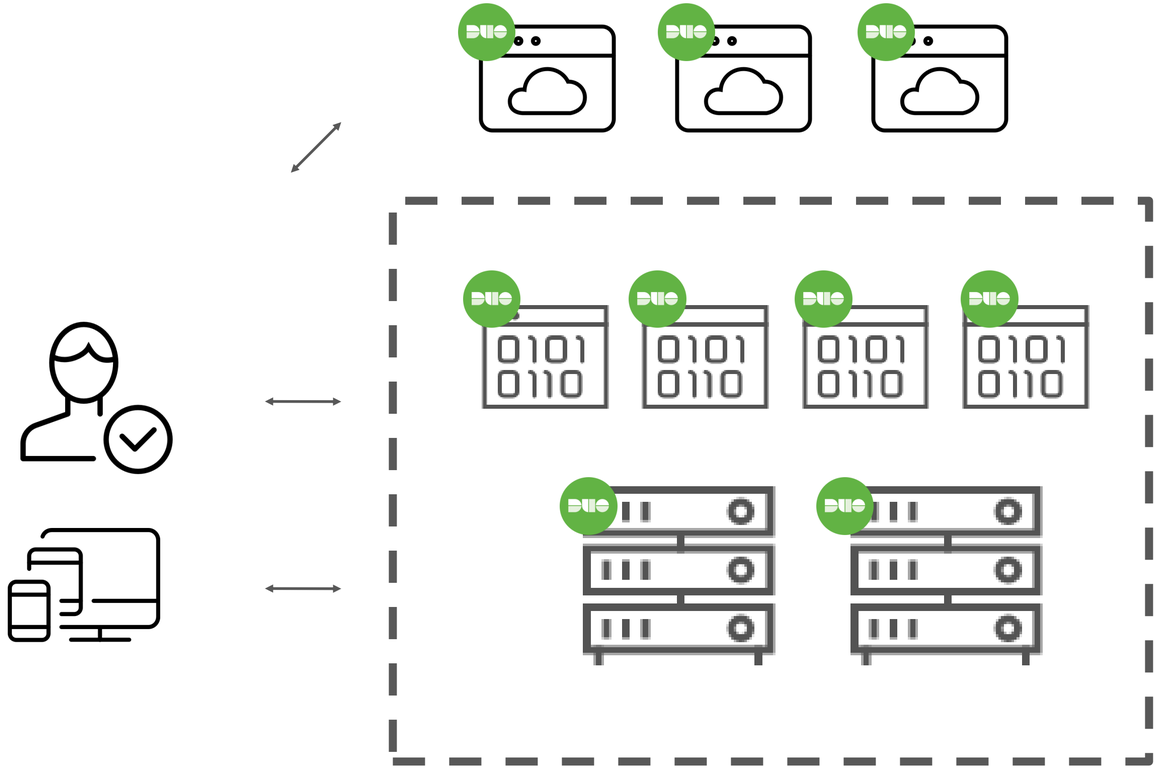
The perimeter security model works well enough when all employees work exclusively in buildings owned by an enterprise. However, with the advent of a mobile workforce, the surge in the variety of devices used by this workforce, and the growing use of cloud-based services, additional attack vectors have emerged that are stretching the traditional paradigm to the point of redundancy. Key assumptions of this model no longer hold: The perimeter is no longer just the physical location of the enterprise, and what lies inside the perimeter is no longer a blessed and safe place to host personal computing devices and enterprise applications.

Traditional perimeter approach



Focus on securing **access to the network** by inspecting the device.

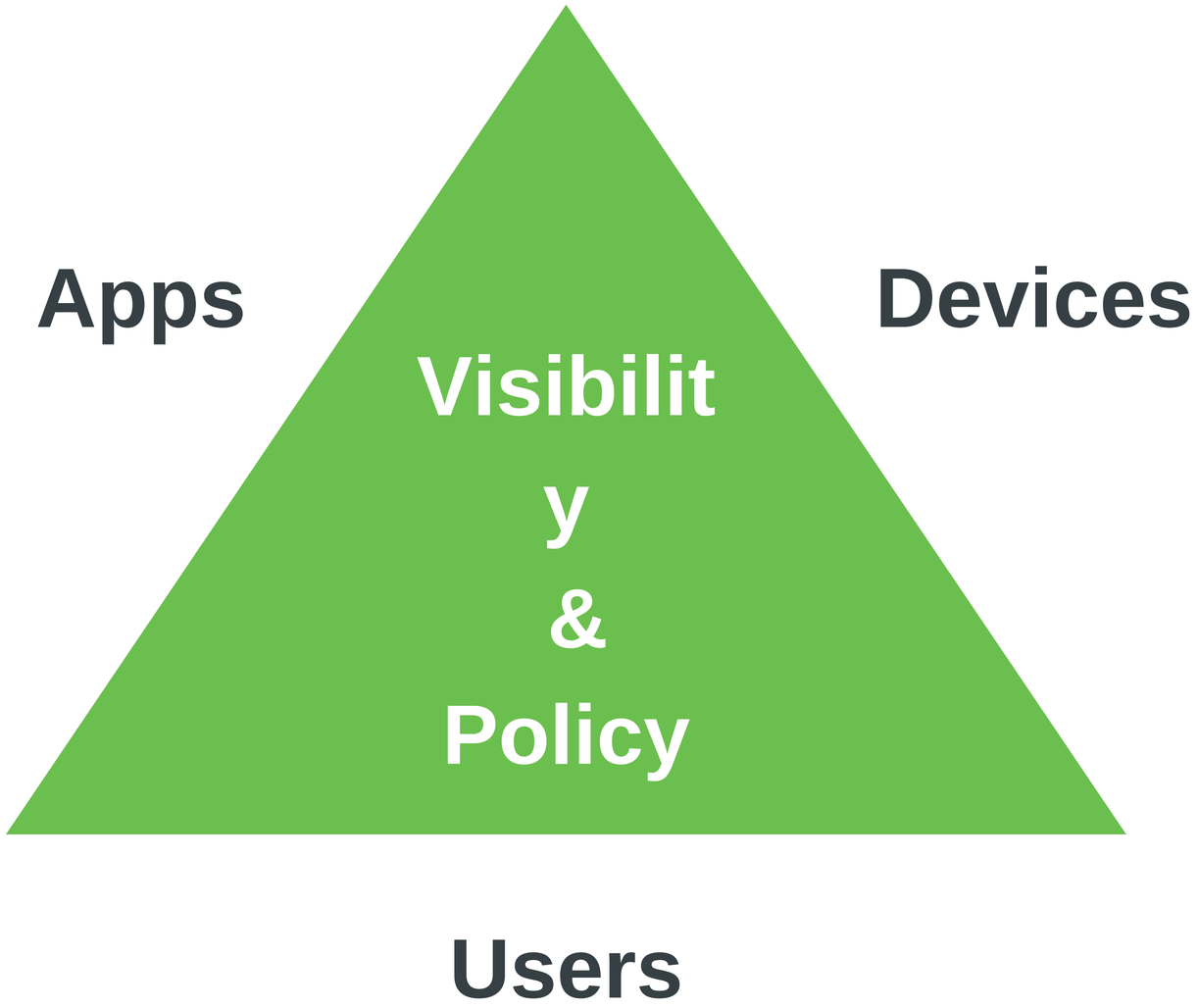
“Zero Trust” approach



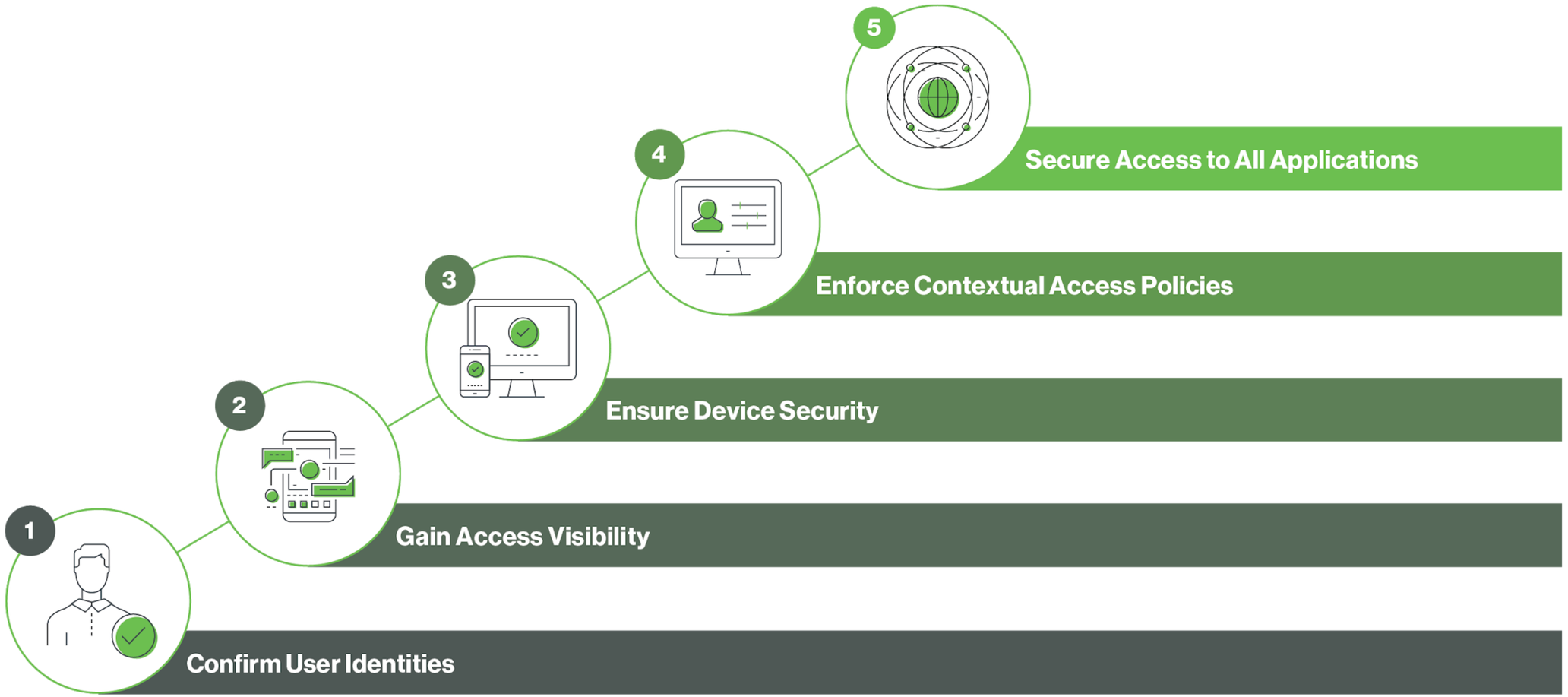
Focus on securing **access to the application** by **verifying the user**, **inspecting the device** and **context**

Coverage for all apps including SaaS apps outside the corporate network.

The Magic Triad



How Do You Establish Trust Easily and Effectively?



Castles Don’t Scale

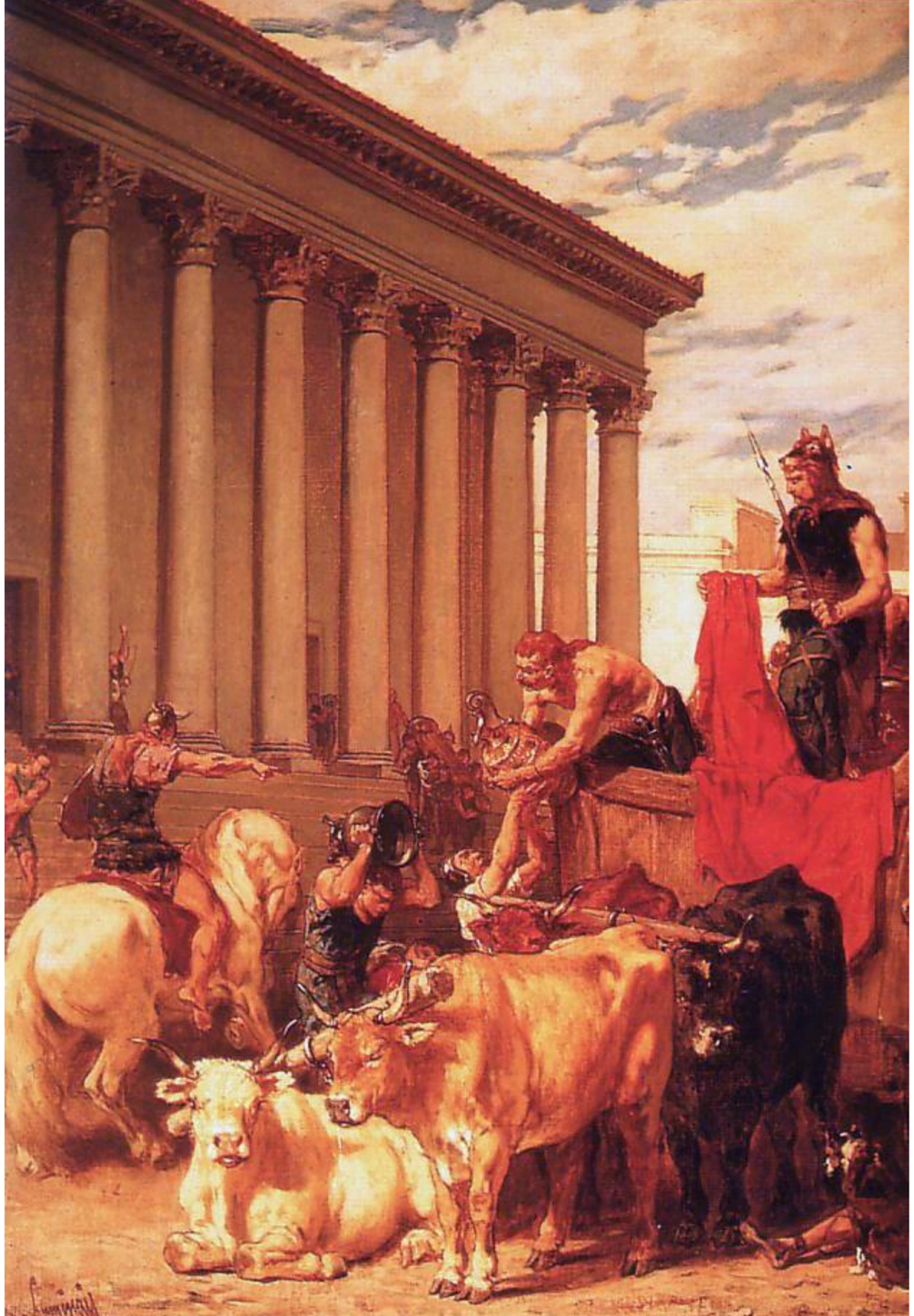
Don’t trust something just because it’s on the “inside” of your firewall

Is the password…password?

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

Lessons From History

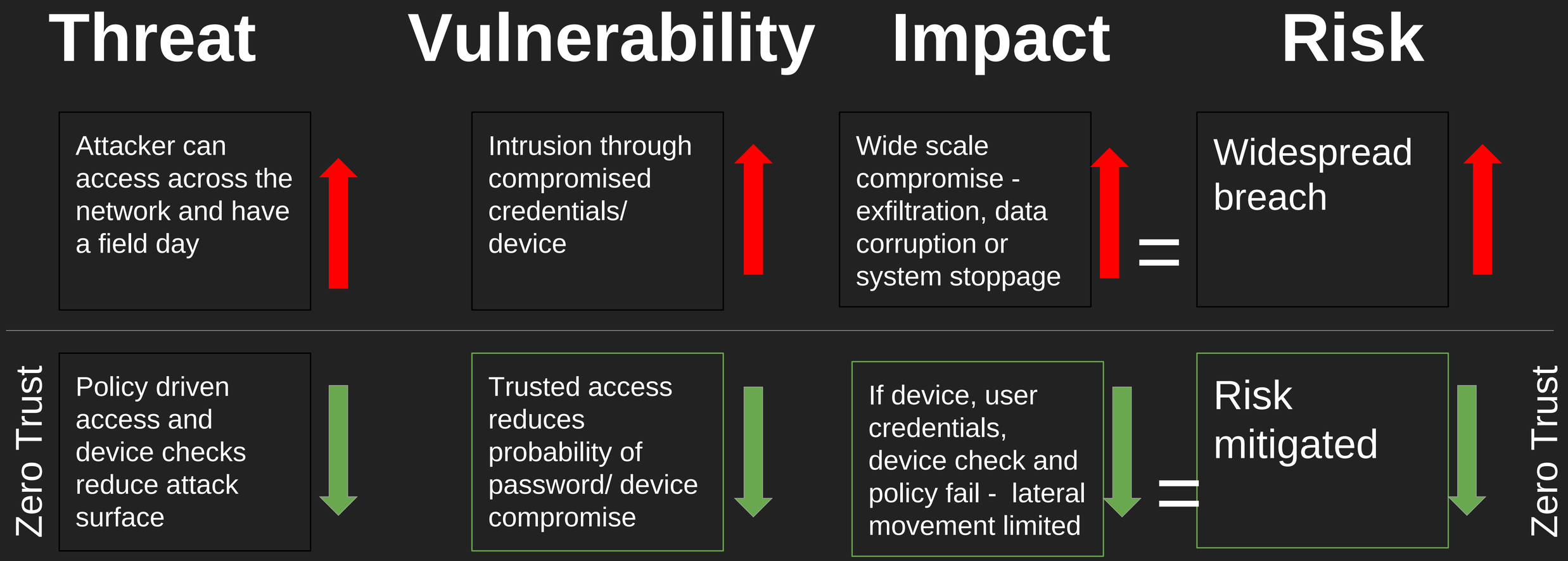
The sack of Rome in 410 AD




Remember when you only had to outrun the other hiker?

Now there’s more than enough bear to go around

Reducing the Risk



The Flaming Sword of Justice

Data Breaches

In The News

THE GLOBE AND MAIL

REPORT ON B

M
ha

JIM FI
REUTE
PUBLIS
UPDAT
CO

A Marr
on No

Adam D'A
don't happ
Matthew St

By

Dec. 4, 2018

DARKReading | Join us live at Interop

Authors Slideshows Video Tech Library University Radio Calendar Black Hat News

ANALYTICS | ATTACKS / BREACHES | APP SEC | CAREERS & PEOPLE | CLOUD | ENDPOINT | IoT | MOBILE | OPERATION

APPLICATION SECURITY

3/12/2019
05:55 PM

Robert Lemos
News

2 COMMENTS
COMMENT NOW

Login

50% 50%

Like

Citrix Breach Underscores Password Perils

Attackers used a short list of passwords to knock on every digital door to find vulnerable systems in the vendor's network.

The recent cyberattack on enterprise technology provider Citrix Systems using a technique known as password spraying highlights a major problem that passwords pose for companies: Users who select weak passwords or reuse their login credentials on different sites expose their organizations to compromise.

On March 8, Citrix posted a statement confirming that the company's internal network had been breached by hackers who had used password spraying, successfully using a short list of passwords on a wide swath of systems to eventually find a digital key that worked. The company began investigating after being contacted by the FBI on March 6, confirming that the attackers

81%

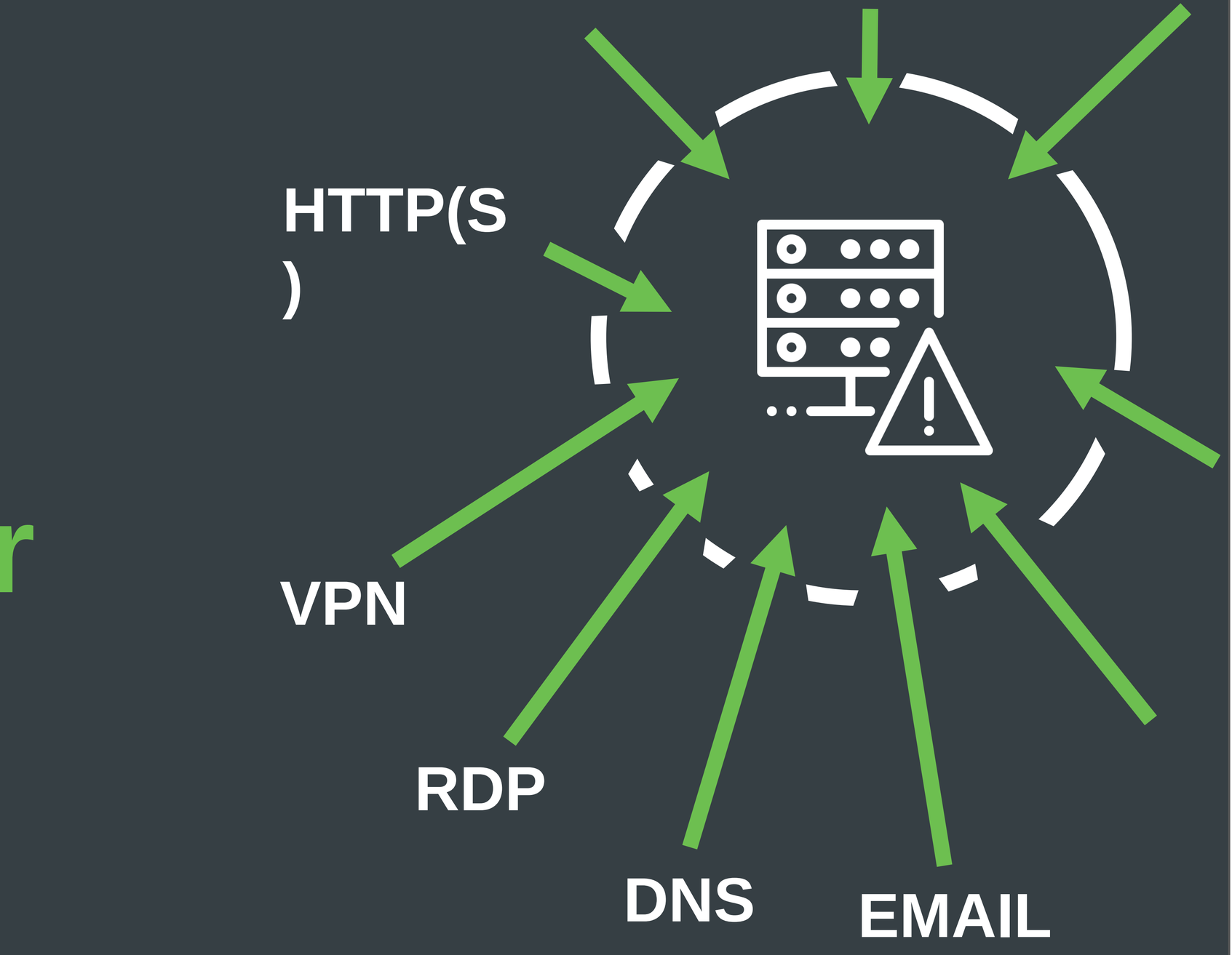
Of breaches involve stolen or weak **credentials**

70%

Of breaches involve compromised **devices**

Sources: 2017 Verizon DBIR, 2016 IDC Research

Porous Perimeter




Are You
My
Perimeter?

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

New Perimeter

Remote Employees

Hybrid Cloud

Old Perimeter

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

Cloud Applications

Personal Devices

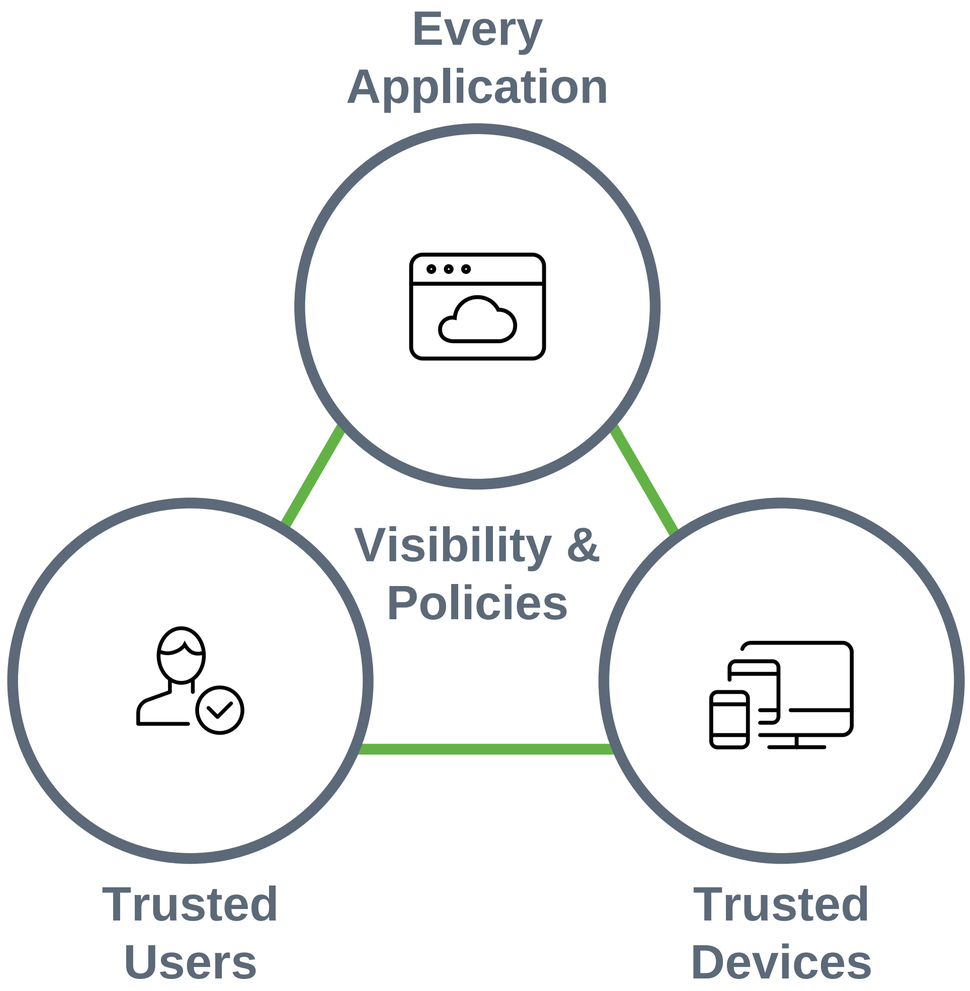
Mobile Devices

Vendors & Contractors

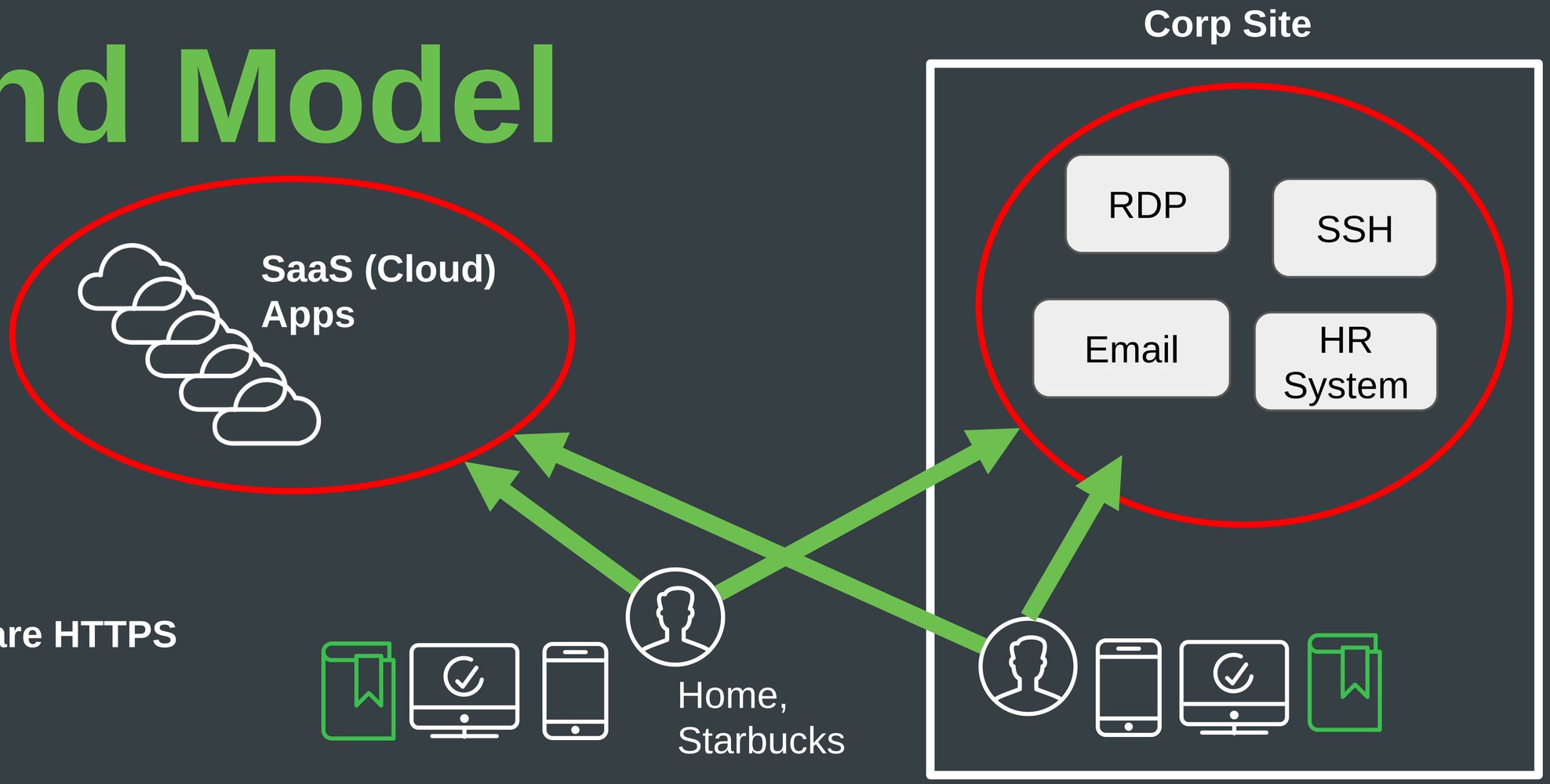
DUO

Zero-Trust Model: Focus on Access

Protect organizations by verifying the identity of **users** and the health of their **devices** before connecting to the **applications** they need.



Beyond Model



All connections are HTTPS

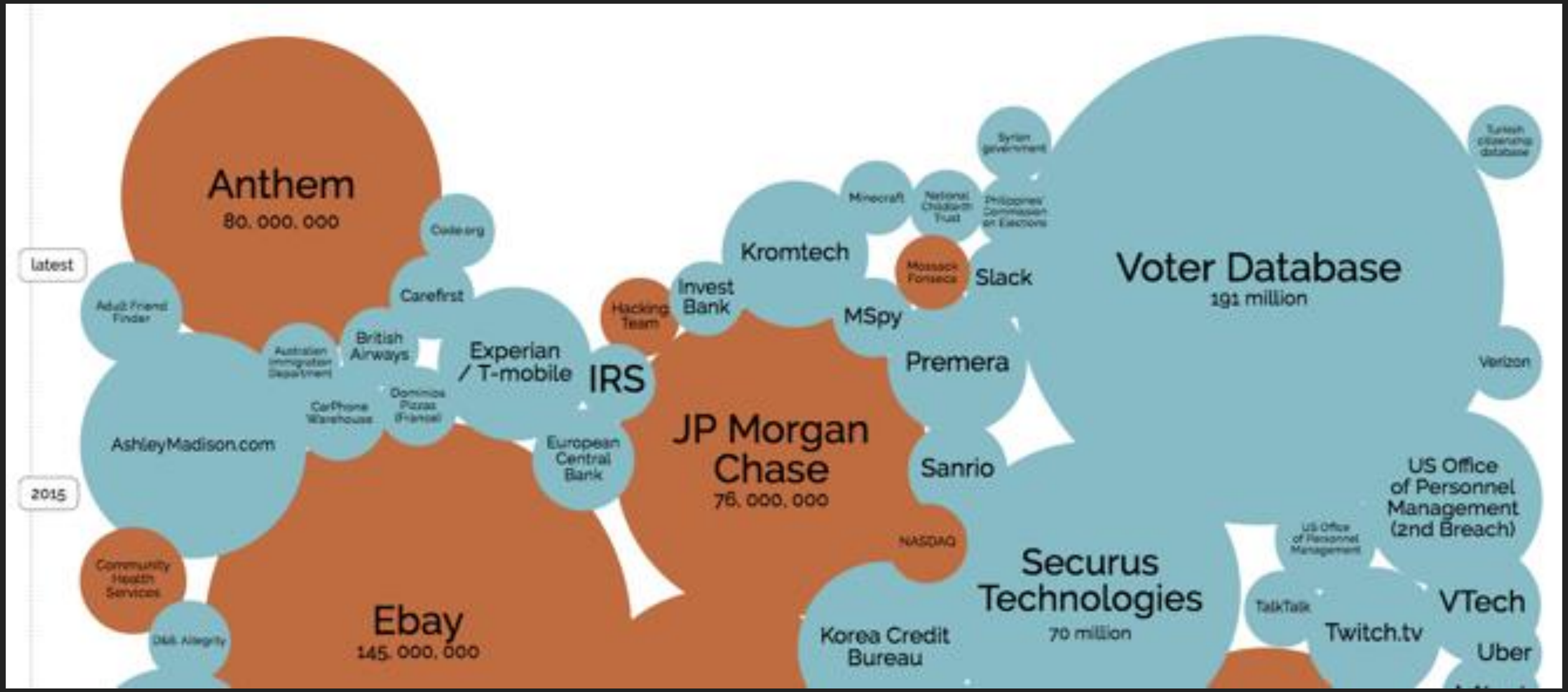
Lets you protect your assets the same way using the same policies, whether they are accessed internally or externally

The Summer of Breach 2012

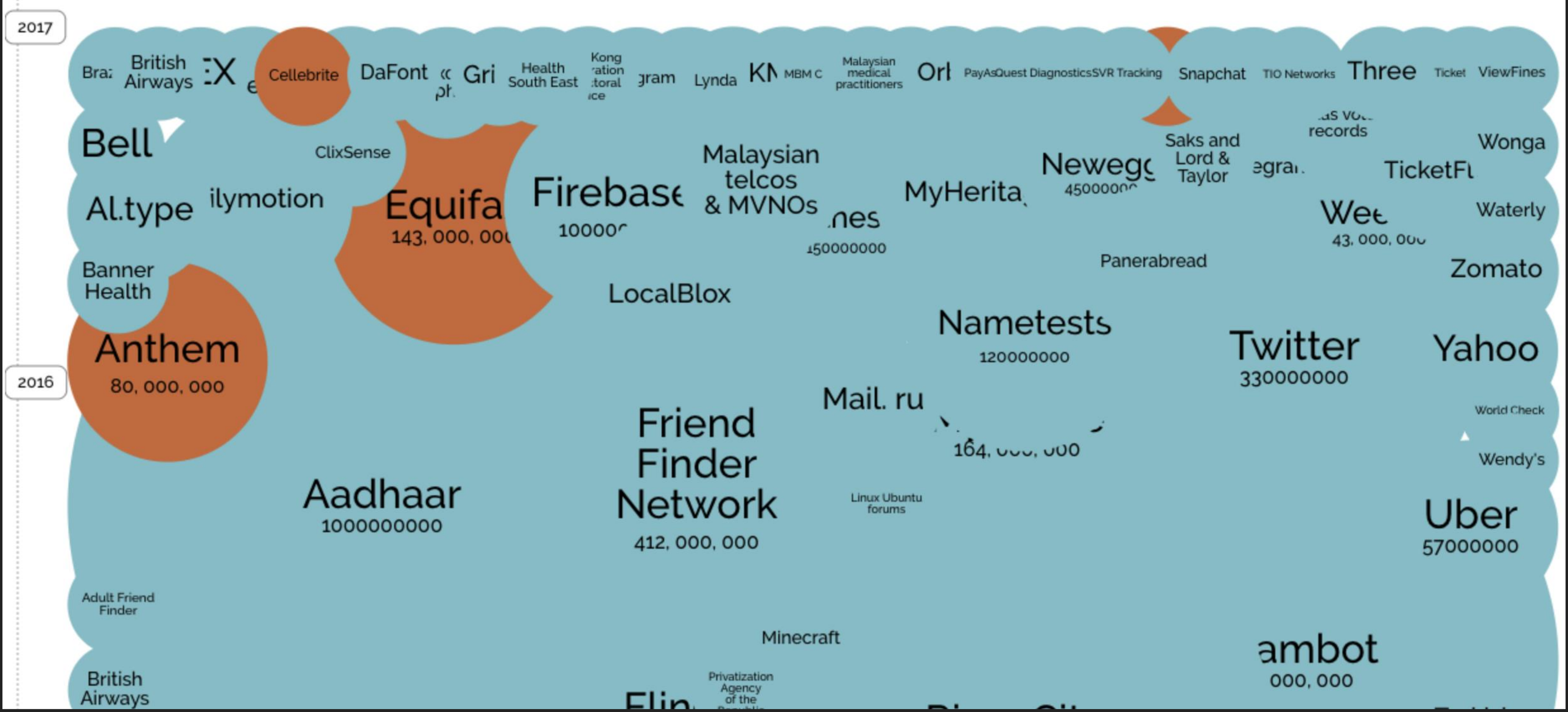
Site Breached	Users Affected	Link	Confirmed
Yahoo	453,000	CNN	Yes
Formspring	420,000	Securityweek	Yes
Phandroid	1,000,000	Securityweek	Yes
Billabong	21,485	IT News AU	Yes
Nvidia	800	PCWorld	Yes
LinkedIn	6,460,000	Globe and Mail	Yes
eHarmony	1,500,000	ZDNet	Yes
Consumerist	TBD	Consumerist	Yes/TBD

Been There…

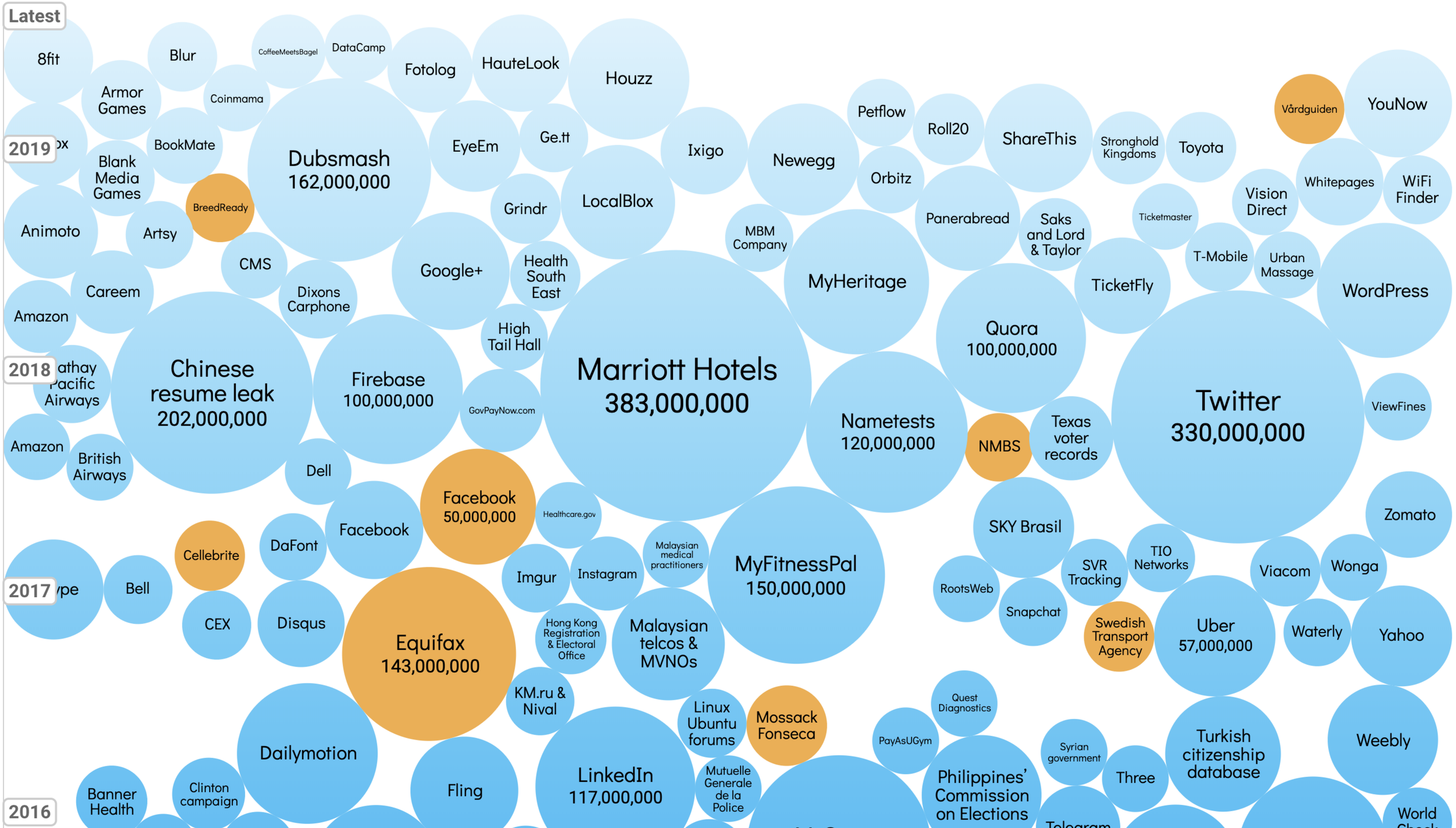
Hades_ - Eriksson - Akira - Taz
r00tBeer Security Team



THREE YEARS AGO



TWO YEARS AGO - AND NOW


Latest
2019
2018
2017
2016
8fit
Blur
CoffeeMeetsBagel
DataCamp
Fotolog
HauteLook
Houzz
Armor Games
Coinmama
Dubsmash
162,000,000
EyeEm
Ge.tt
Ixigo
Newegg
Petflow
Roll20
ShareThis
Stronghold Kingdoms
Toyota
Vårdguiden
YouNow
BookMate
Blank Media Games
BreedReady
Grindr
LocalBlox
Orbitz
Panerabread
Saks and Lord & Taylor
Ticketmaster
Vision Direct
Whitepages
WiFi Finder
Animoto
Artsy
CMS
Google+
Health South East
MBM Company
MyHeritage
T-Mobile
Urban Massage
WordPress
Careem
Dixons Carphone
TicketFly
Amazon
High Tail Hall
Marriott Hotels
383,000,000
Quora
100,000,000
Chinese resume leak
202,000,000
Firebase
100,000,000
GovPayNow.com
Nametests
120,000,000
Twitter
330,000,000
ViewFines
athay Pacific Airways
Amazon
British Airways
Dell
NMBS
Texas voter records
Facebook
50,000,000
Healthcare.gov
Facebook
DaFont
Cellebrite
SKY Brasil
Zomato
Bell
CEX
Disqus
Imgur
Instagram
Malaysian medical practitioners
MyFitnessPal
150,000,000
RootsWeb
Snapchat
SVR Tracking
TIO Networks
Viacom
Wonga
Equifax
143,000,000
Hong Kong Registration & Electoral Office
Malaysian telcos & MVNOs
Swedish Transport Agency
Uber
57,000,000
Waterly
Yahoo
KM.ru & Nival
Linux Ubuntu forums
Mossack Fonseca
Quest Diagnostics
Weebly
Dailymotion
PayAsUGym
Syrian government
Turkish citizenship database
Banner Health
Clinton campaign
Fling
LinkedIn
117,000,000
Mutuelle Generale de la Police
Philippines' Commission on Elections
Three
World

What’s Open In USA?

178,404,301

Meanwhile, In Texas

7,106,429

Systems Vulnerable to Eternal Blue

1,233

Systems Vulnerable To Heartbleed

18,137

Systems Vulnerable to Bluekeep

43,415

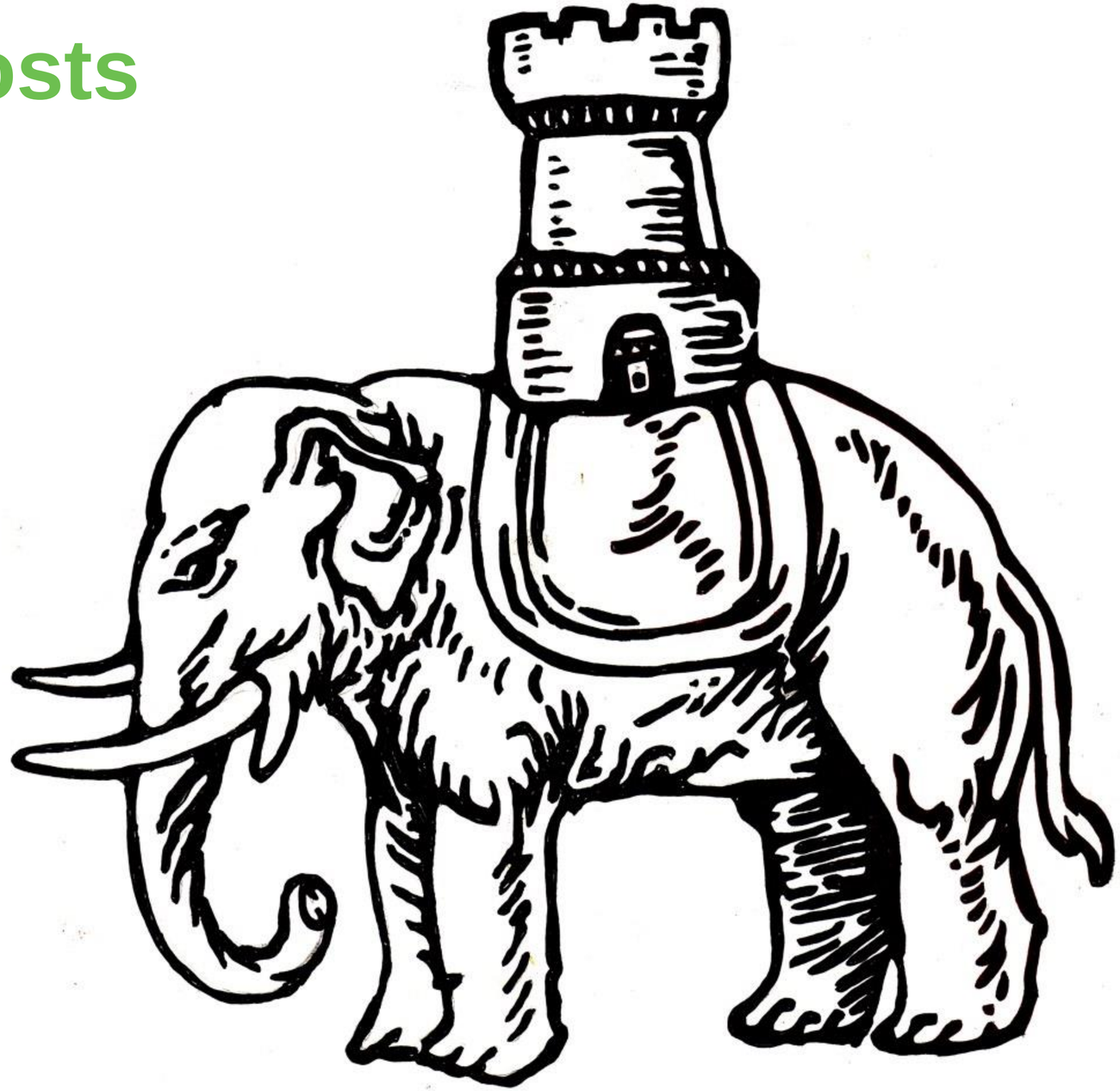
ZTN Value Proposition

- Devaluation of stolen credentials
- Low hanging fruit sours.
- Complicates lateral movement through uniform security policy.
- Attackers have to work that much harder.

Trusted Access Security, Value Proposition

- Devaluation of stolen credentials
- Low hanging fruit sours.
- Complicates lateral movement through uniform security policy.
- Attackers have to work that much harder.

Bastion Hosts



From DMZ To The Soft Chewy Centre

Setting Expectations

Aspire to a Zero Trust Network

A Game of Increments

Determining Priorities

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

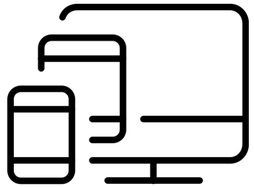
How do you prevent devices with poor security hygiene from accessing critical apps?

Security Best Practices

Policies Are Unique to Each User and Device

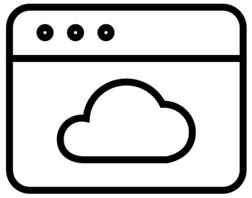
Verify Your Users

- Strong Authentication
- Intuitive Authentication
- User Risk Assessment



Verify Their Devices

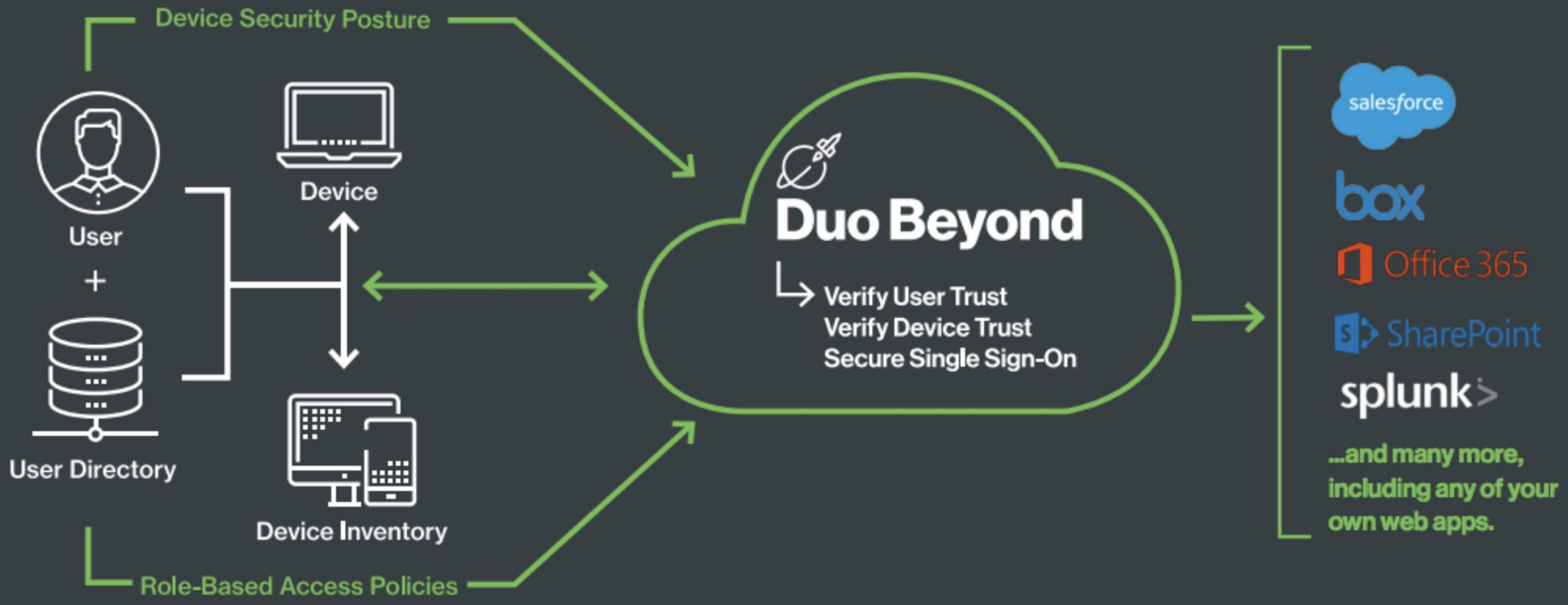
- Up-to-date Devices
- Well-configured Devices
- Managed Devices
- Device Authentication



Protect Every Application

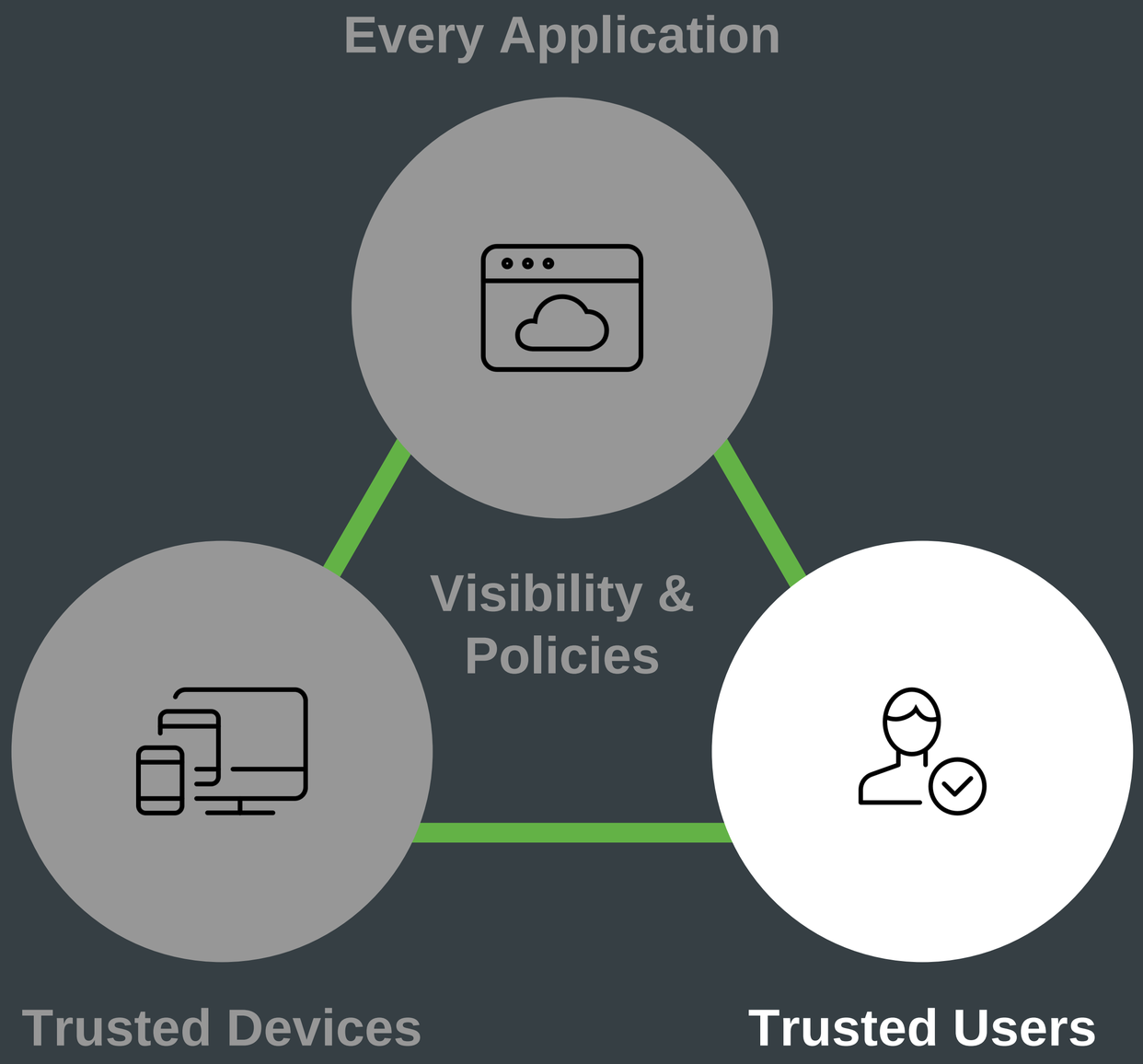
- All Cloud Apps
- All On-Prem Apps
- Consistent End User Experience & Security

Security Beyond the Perimeter

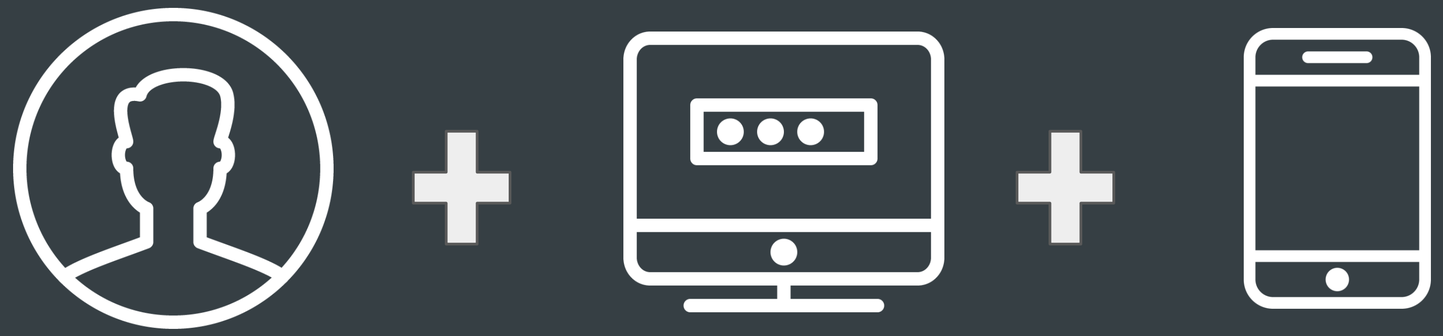


Trusted Users:

- ➔Allow only known users
- ➔Verify identity with strong authentication
- ➔Regardless of location
- ➔On every access
- ➔For every application



Example: Stolen Credentials



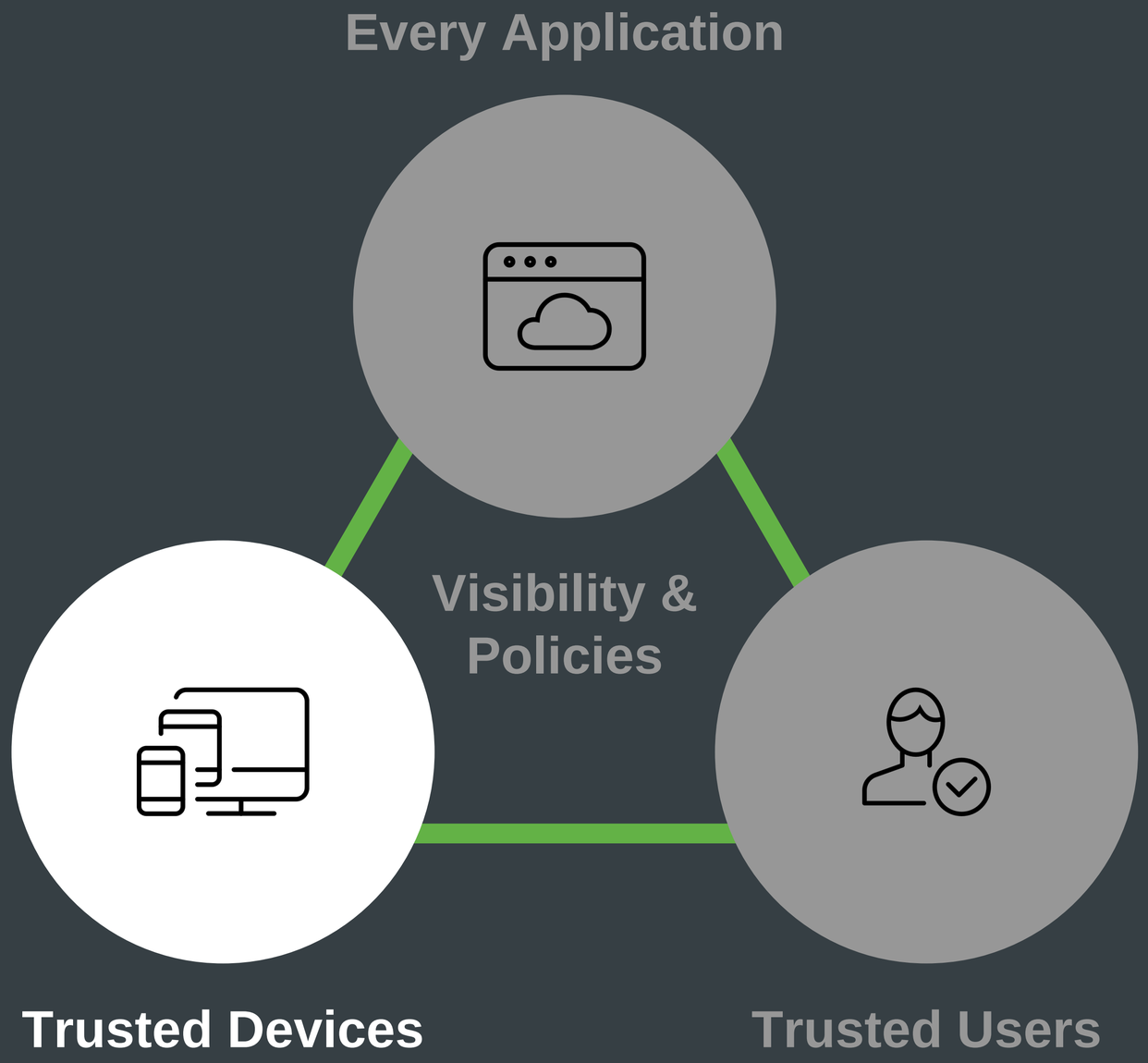
Attackers must compromise:

- Username
- Password
- 2nd auth factor

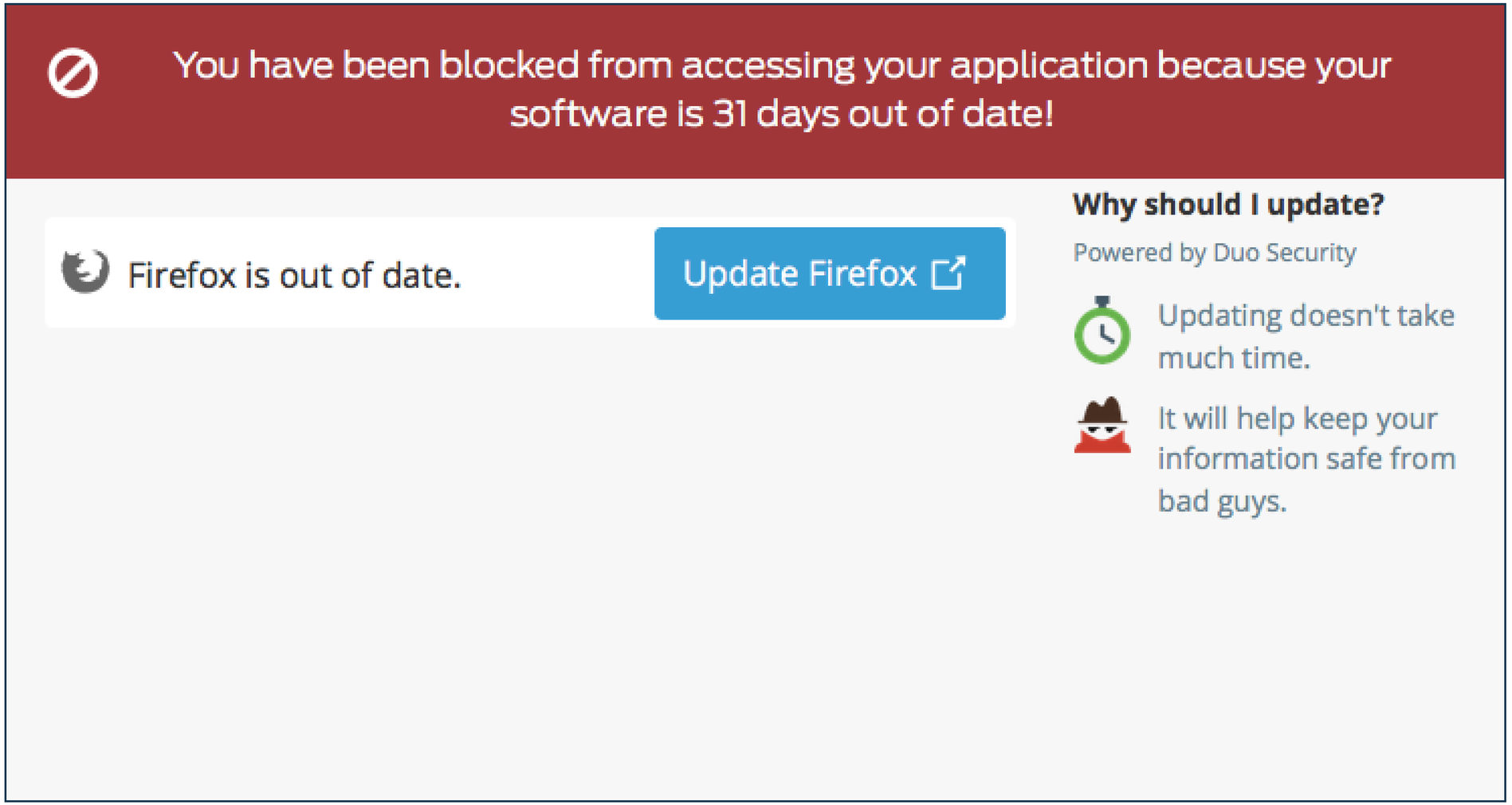
- Trusted device

Trusted Devices:

- ➔Allow only known devices
- ➔Distinguish user- vs. corp-managed
- ➔Enforce device hygiene
- ➔Regardless of location
- ➔On every access
- ➔For every application



Protect Sensitive Apps From Risky Devices



Example: Devices with Poor Security Hygiene

BYOD

Enforce Device Policy:

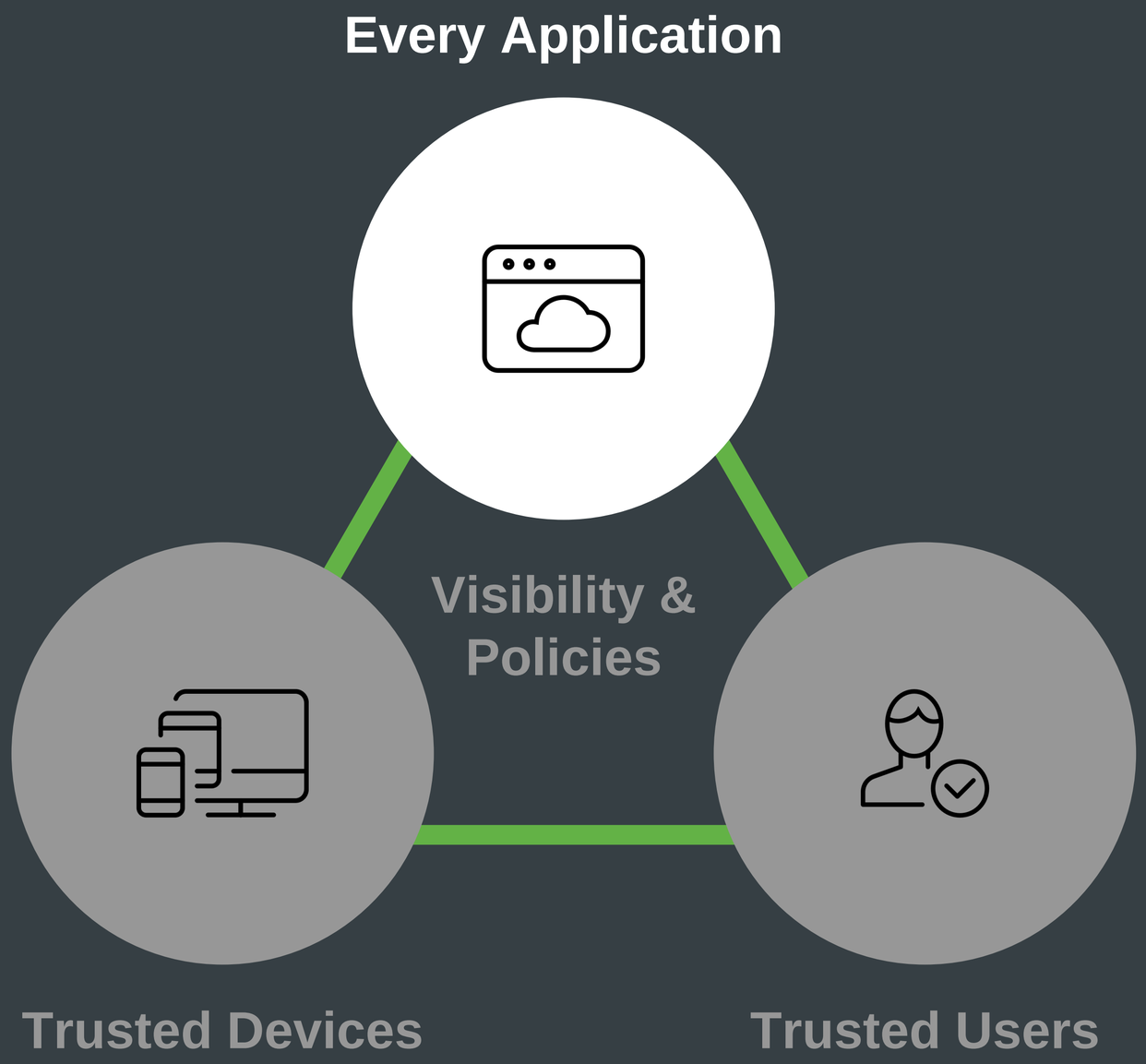
- Known device
- Up-to-date software
- Security configuration
- Device risk

Cloud Apps

On-Premises Apps

Every Application:

- ➔Cloud-based or on-prem
- ➔Regardless of access location
- ➔For every user
- ➔On every access
- ➔For every device



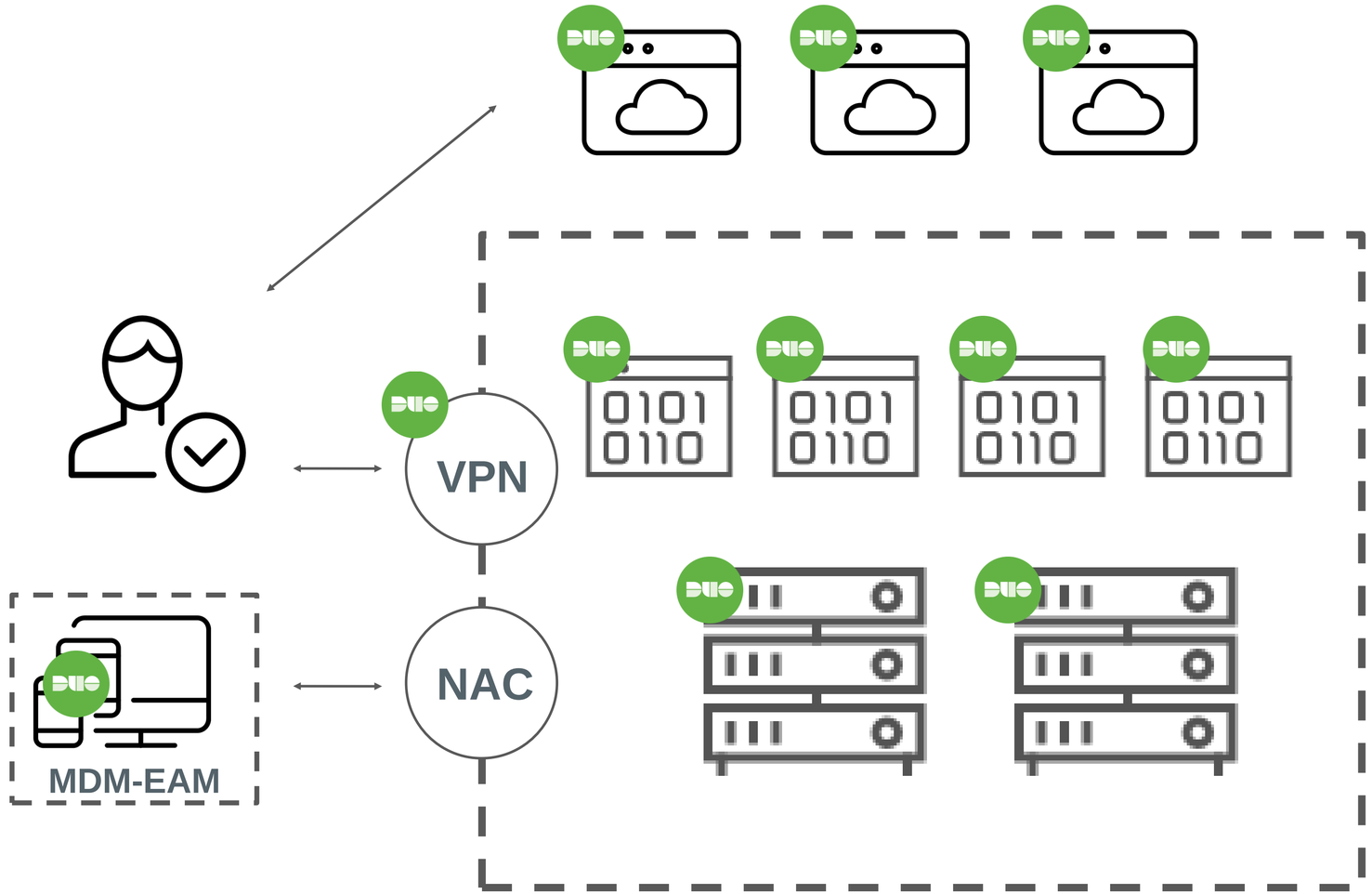
Enforce Policy Based Controls

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

BeyondCorp Journey leverages 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



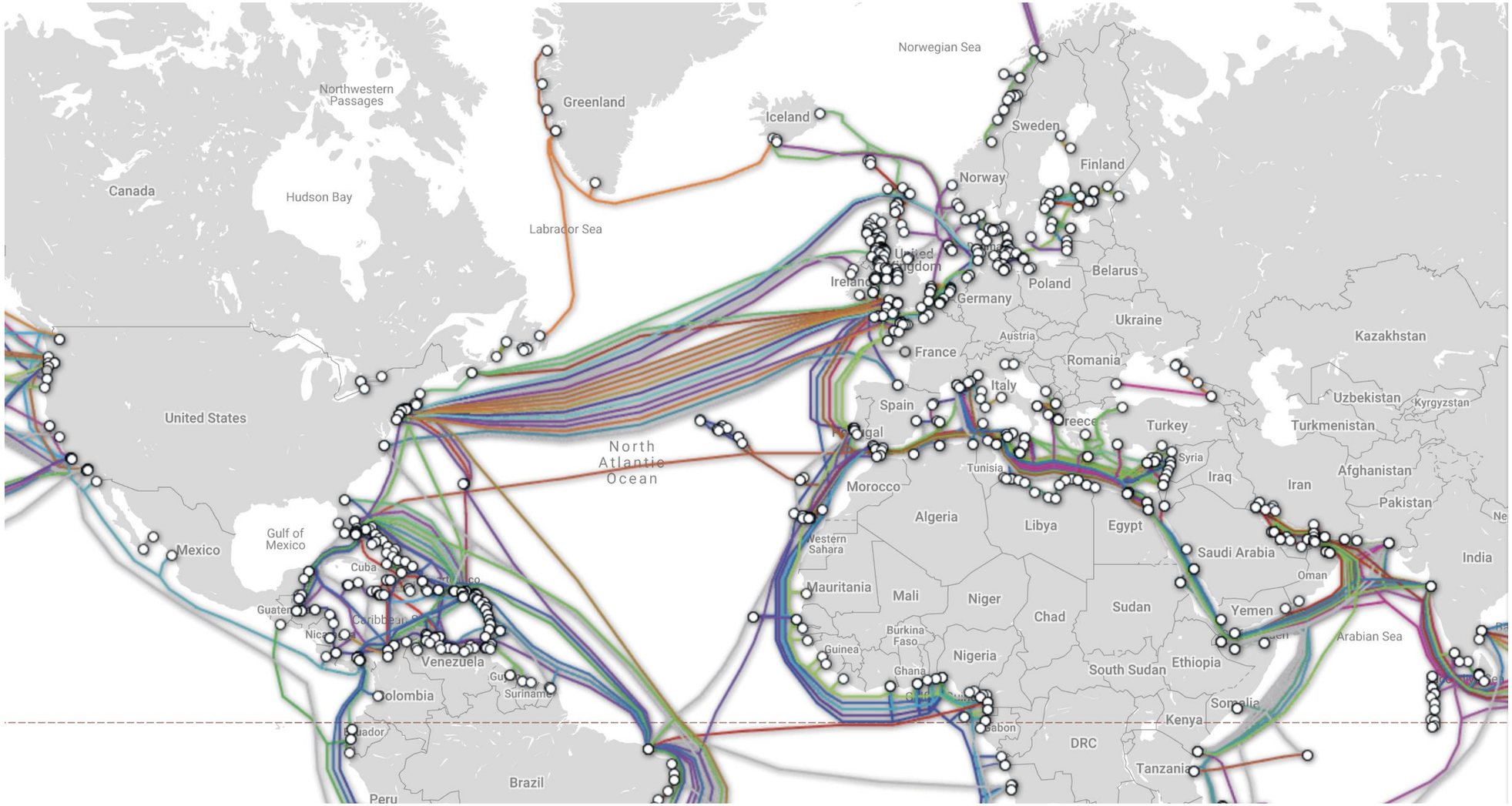
Note: No agents required

Zero Trust Shopping List

- Asset Inventory.
- User Management.
- Device Management through uniform security policy.
- Defined Repeatable Process.
- User and Entity Behavior Analytics.
- Network Zone Segmentation.

The Authentications Must Flow

Supply Chain Security



Partner Network, Meet The Pentest

SSH

22
tcp
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
```

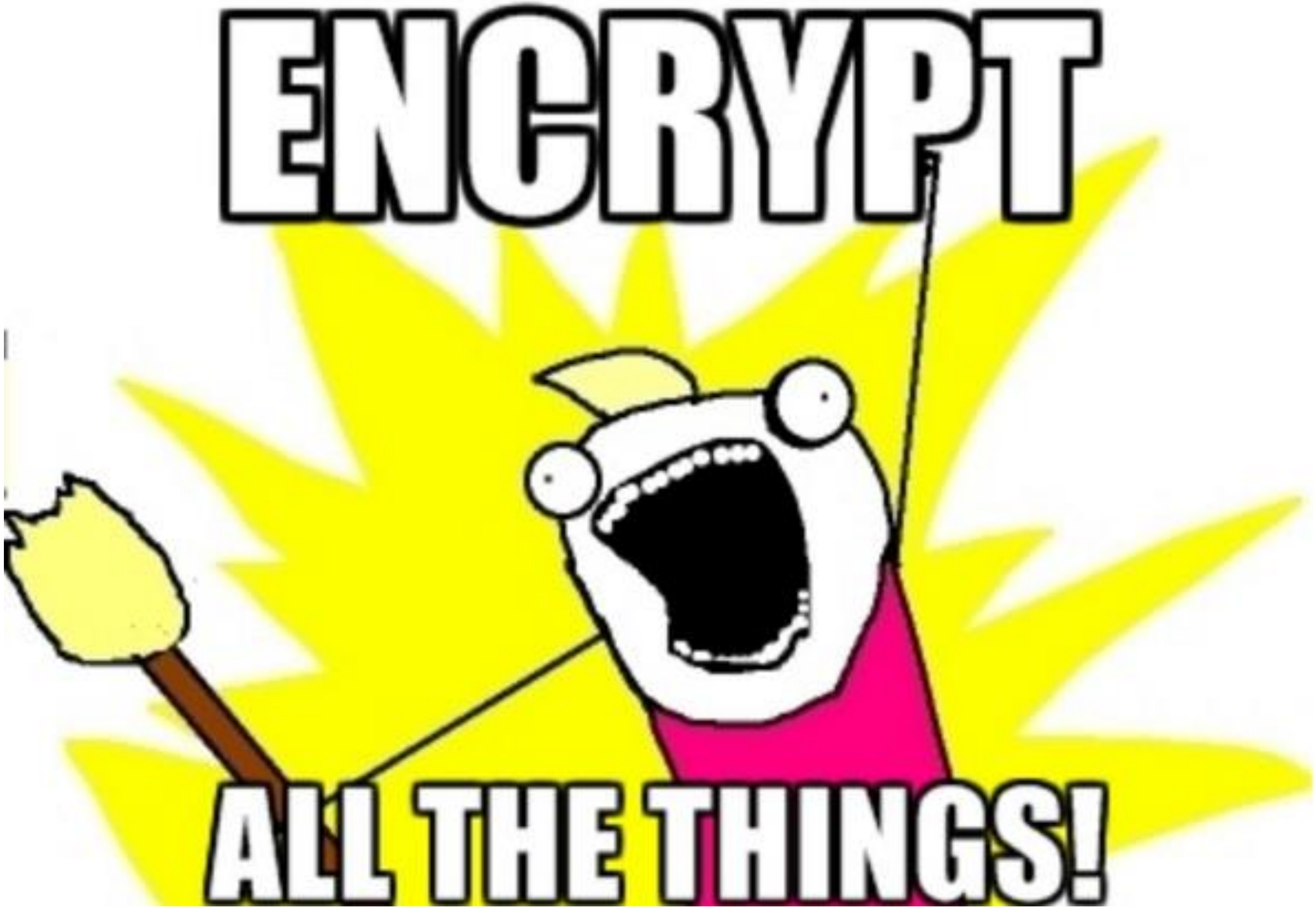
47.593

⚠ Vulnerabilities

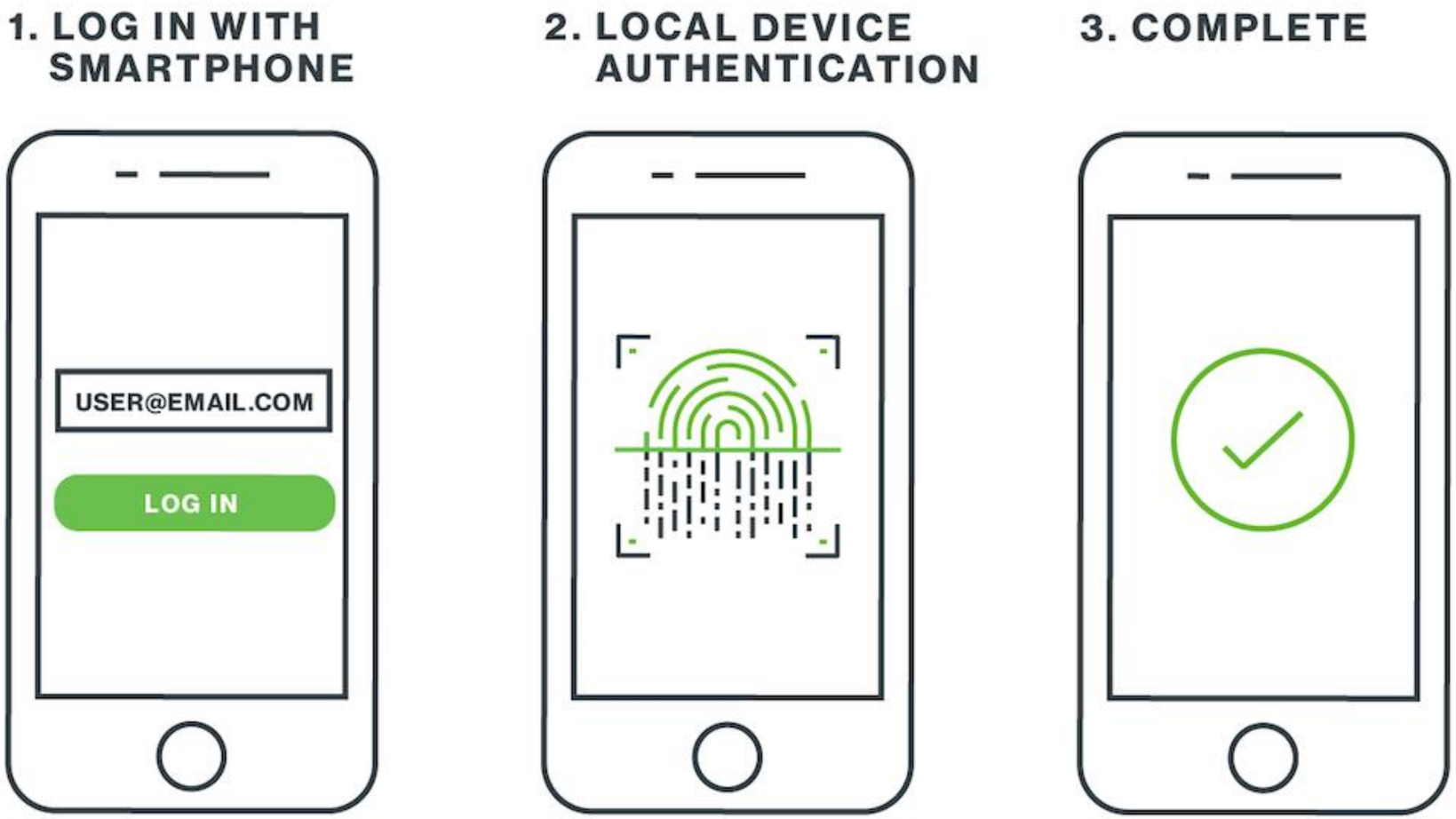
Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

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 ing a login, which makes it easier for remote attackers to cause a denial haustion) by periodically making many new TCP connections.
	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.

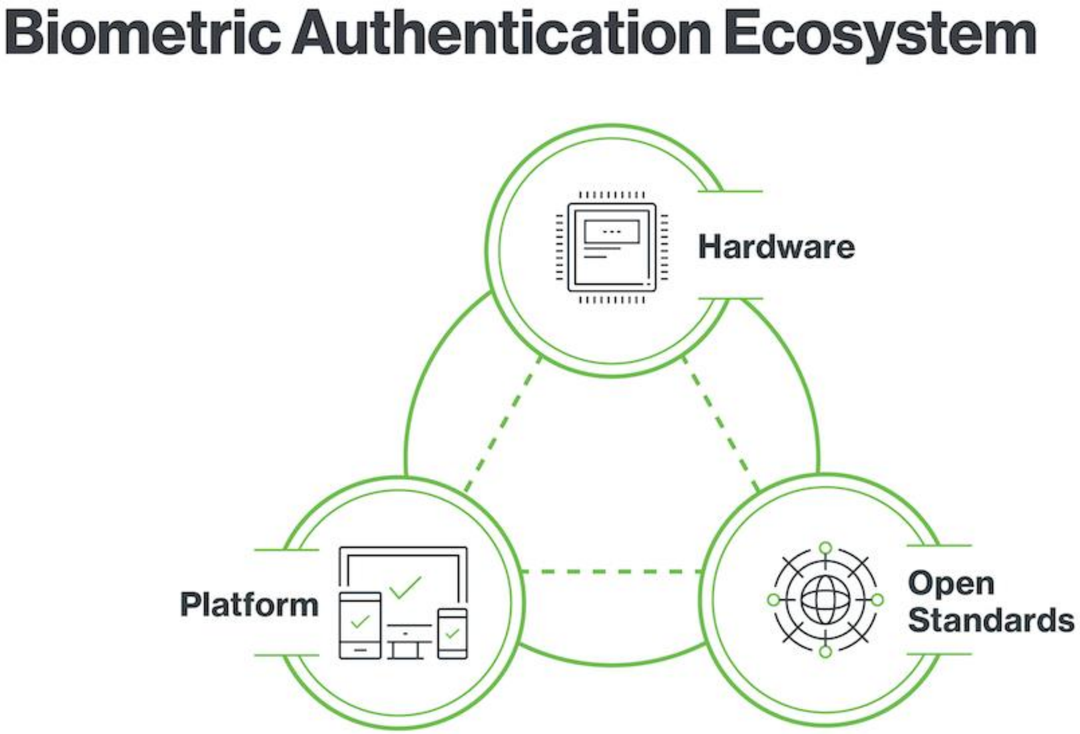
DUO

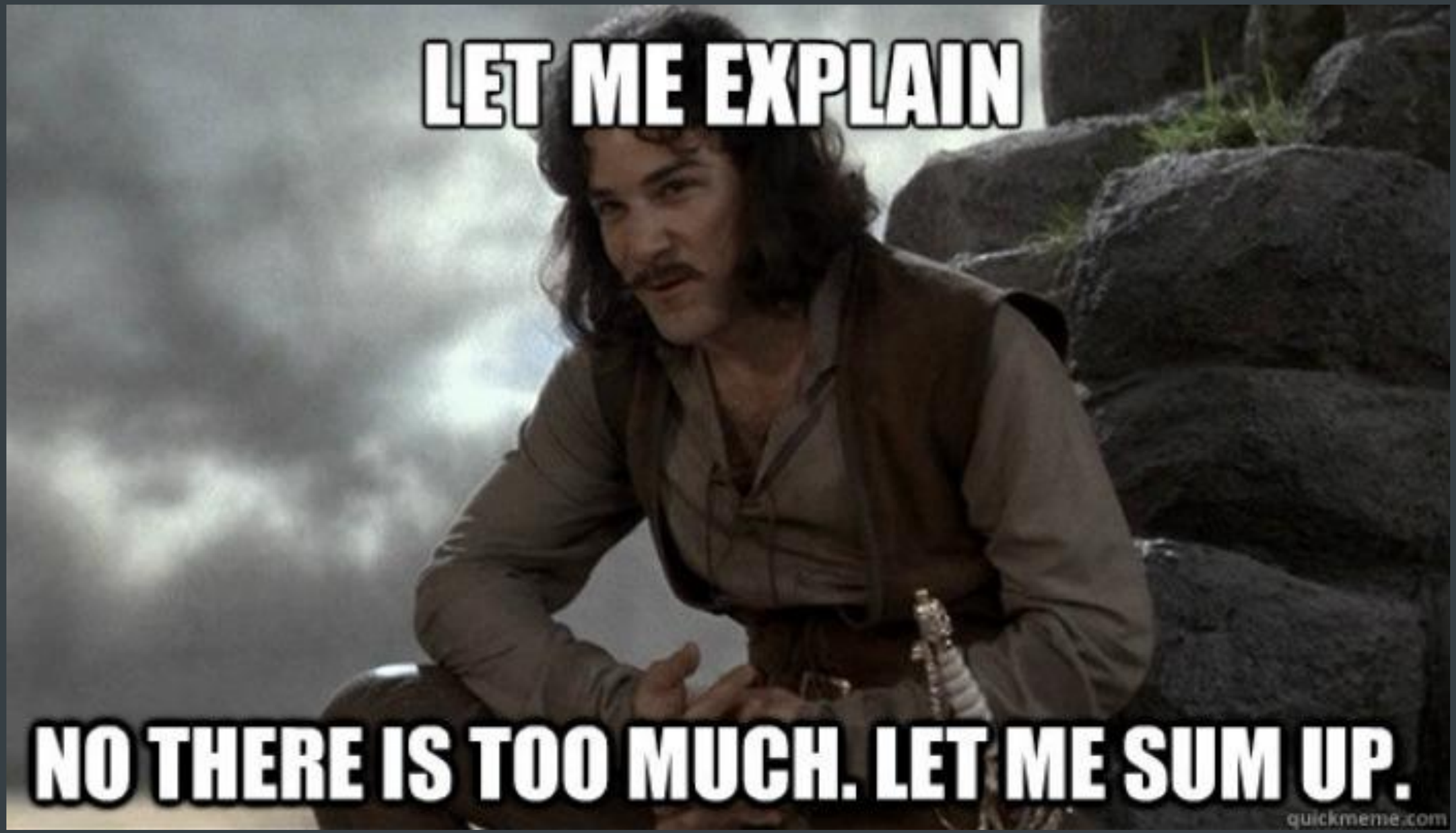

ENCRYPT
ALL THE THINGS!

A Better Way Forward



Webauthn


Biometric Authentication Ecosystem
Hardware
Platform
Open
Standards


LET ME EXPLAIN
NO THERE IS TOO MUCH. LET ME SUM UP.
quickmeme.com

Zero Trust True-isms

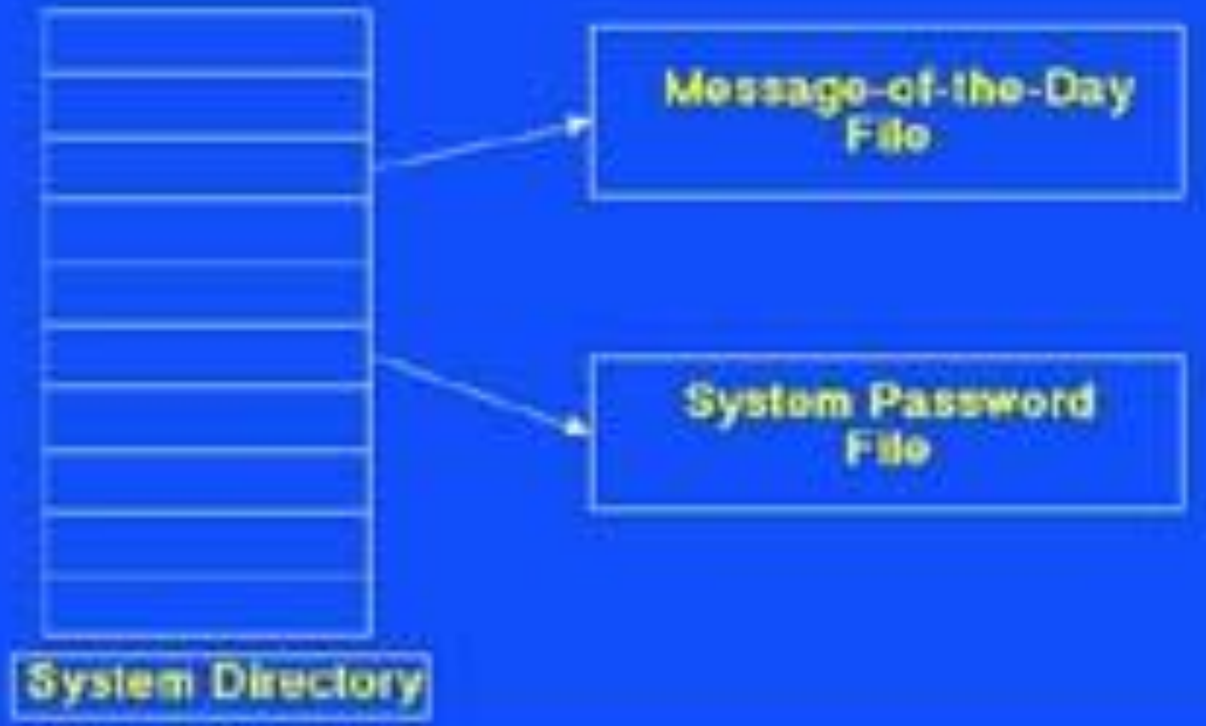
- Assume the network is hostile
- Establish a trust engine
- Reduce threat surface
- Continuously validate for authorization
- KISS

ZTN Summary

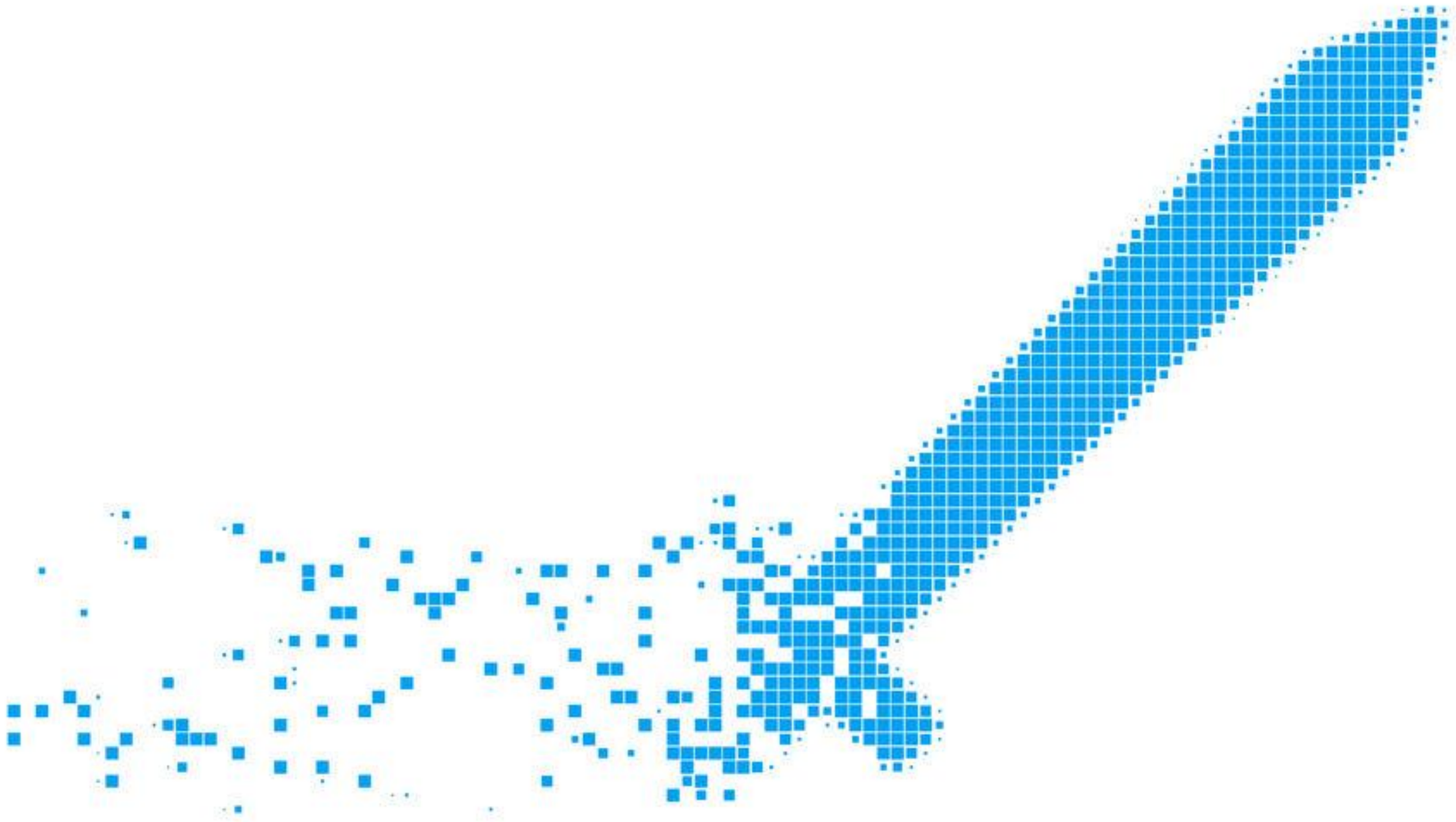
- Build an asset inventory.
- Get a solid hold on user management.
- What’s on your network?
- Defined Repeatable Process
- User and Entity Behavior Analytics.
- Network Zone Segmentation.

CTSS: A Mishap

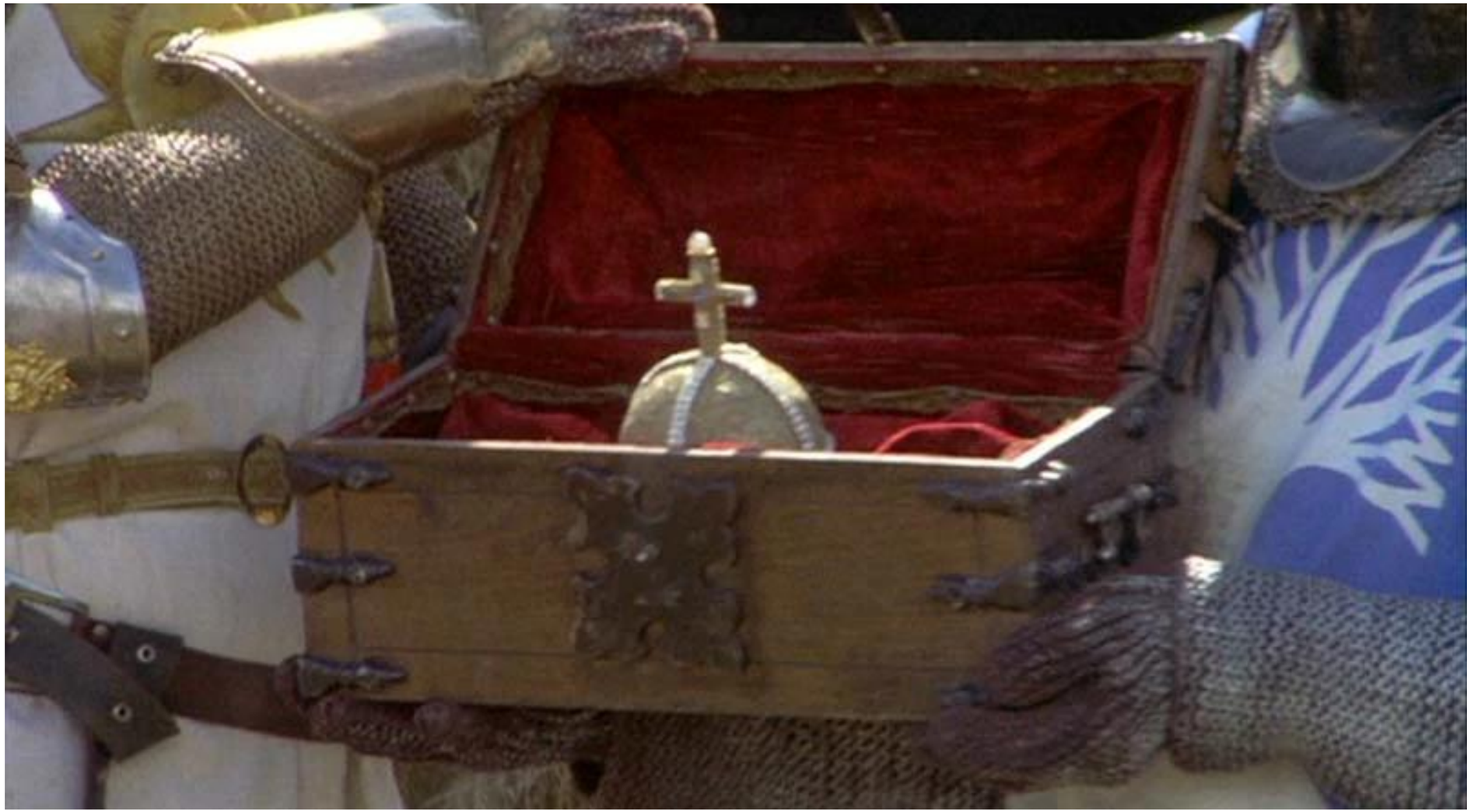
- System Password File became the Message-of-Day



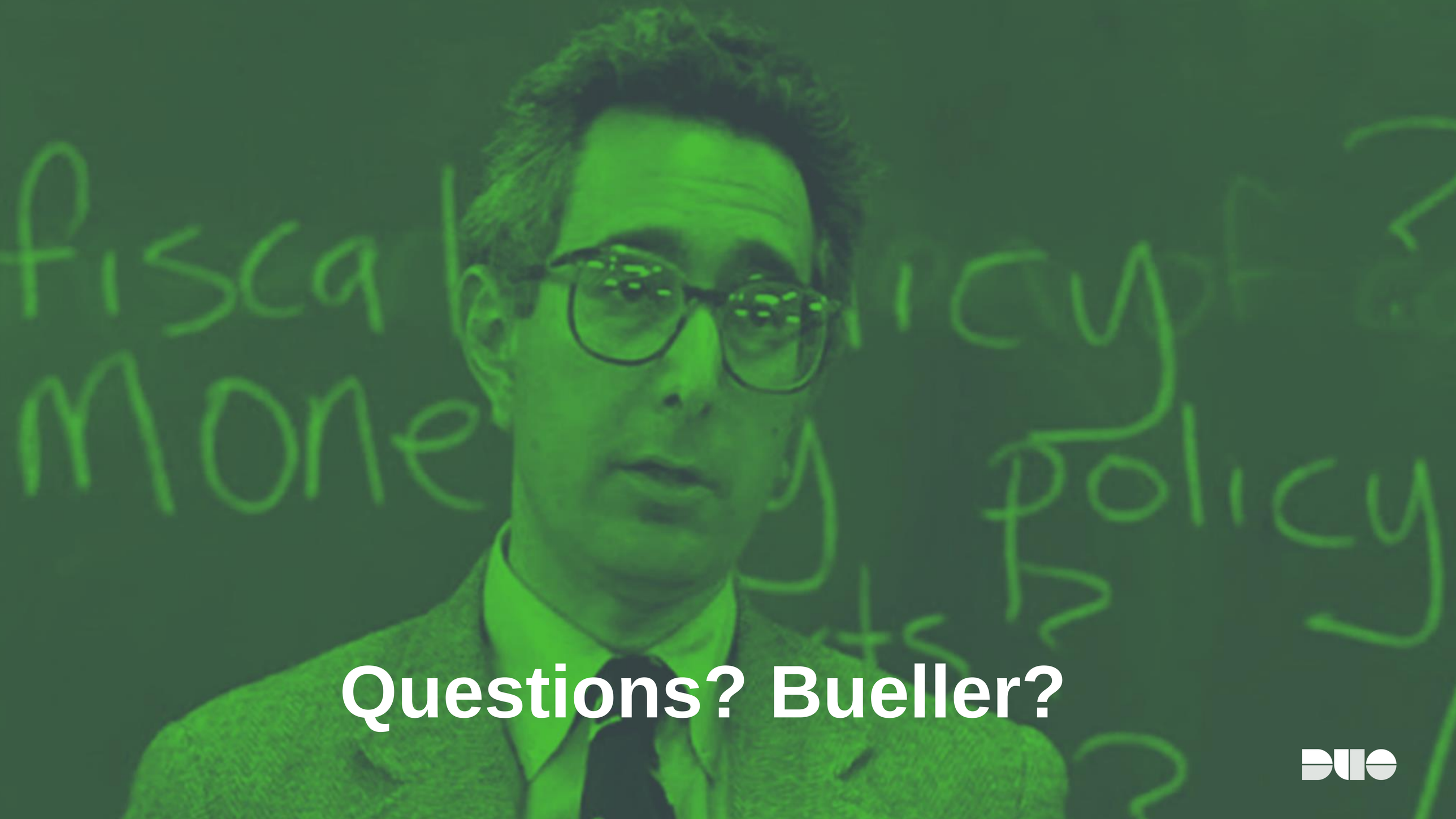
The Sword Is Dissolving



No Need For The Holy Hand Grenade



Thanks For Listening!



Questions? Bueller?

Thanks!

gattaca@cisco.com
gattaca@duo.com
@gattaca

www.cisco.com

www.duo.com