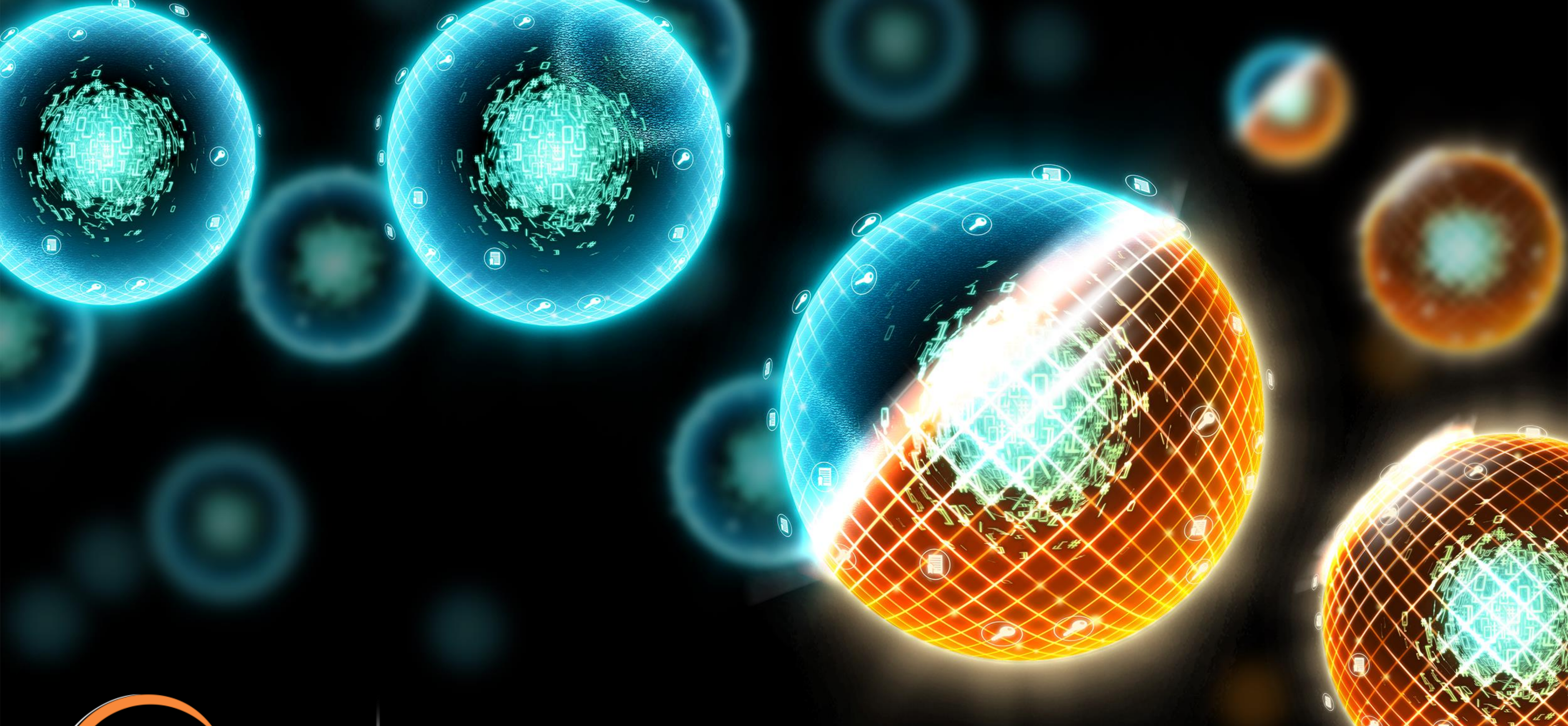
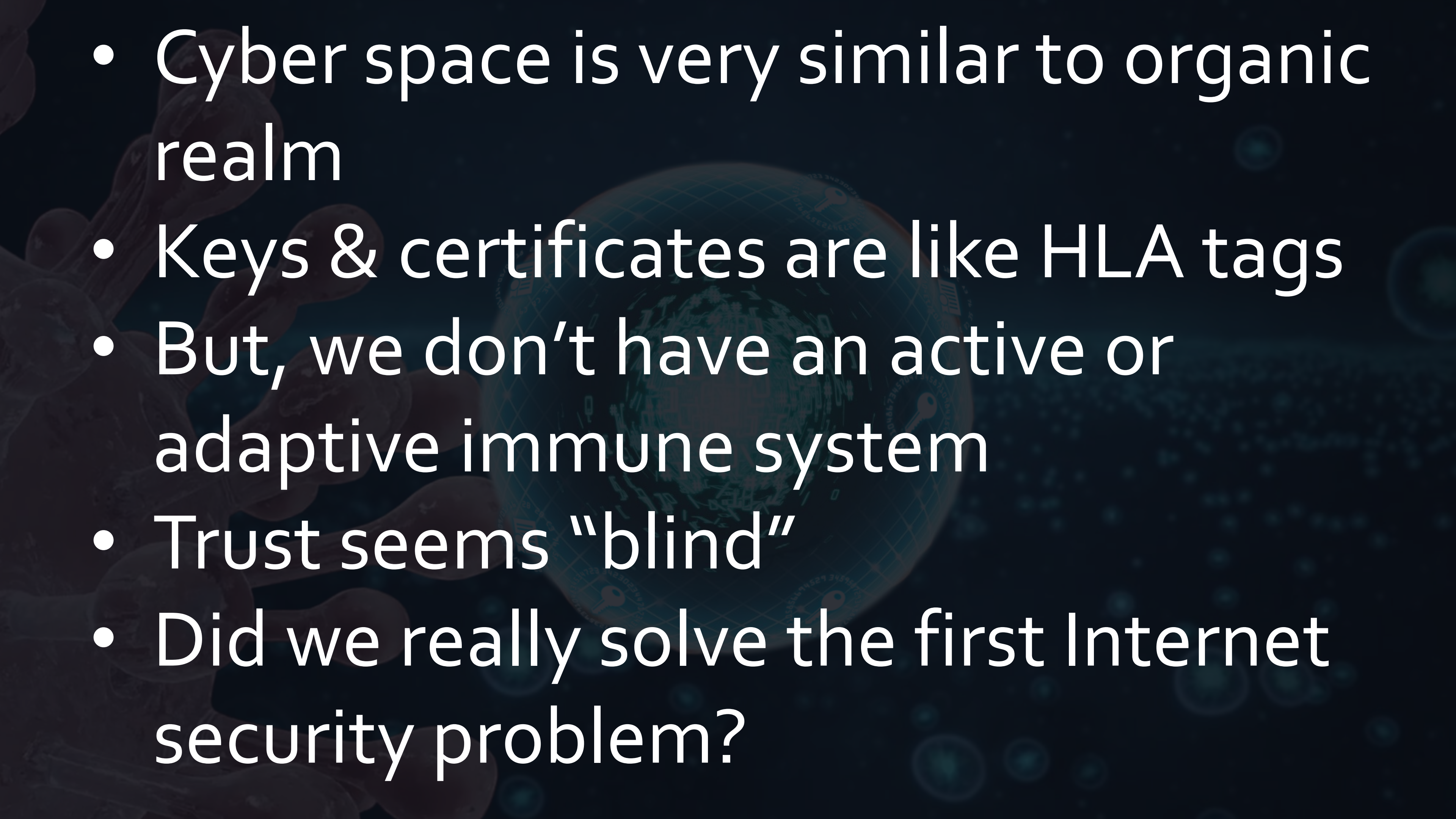
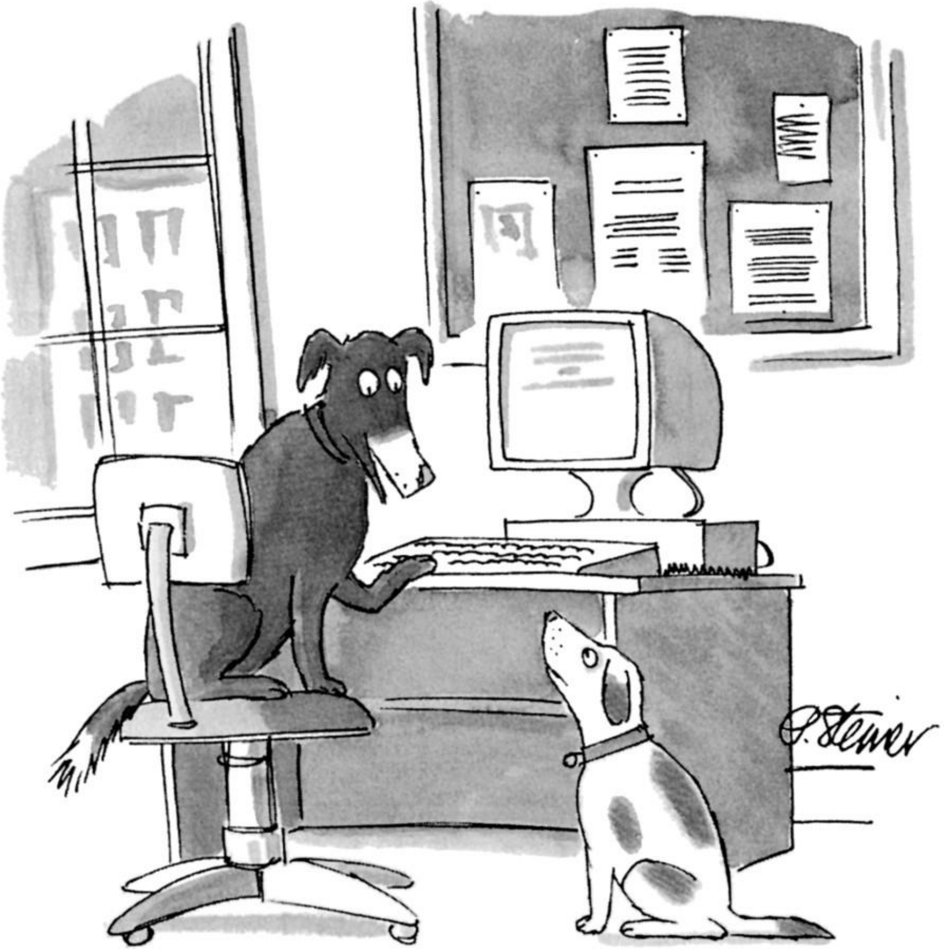


Lessons from the Human Immune System

Gavin Hill, Director Threat Intelligence



- Cyber space is very similar to organic realm
- Keys & certificates are like HLA tags
- But, we don’t have an active or adaptive immune system
- Trust seems “blind”
- Did we really solve the first Internet security problem?



"On the Internet, nobody knows you're a dog."

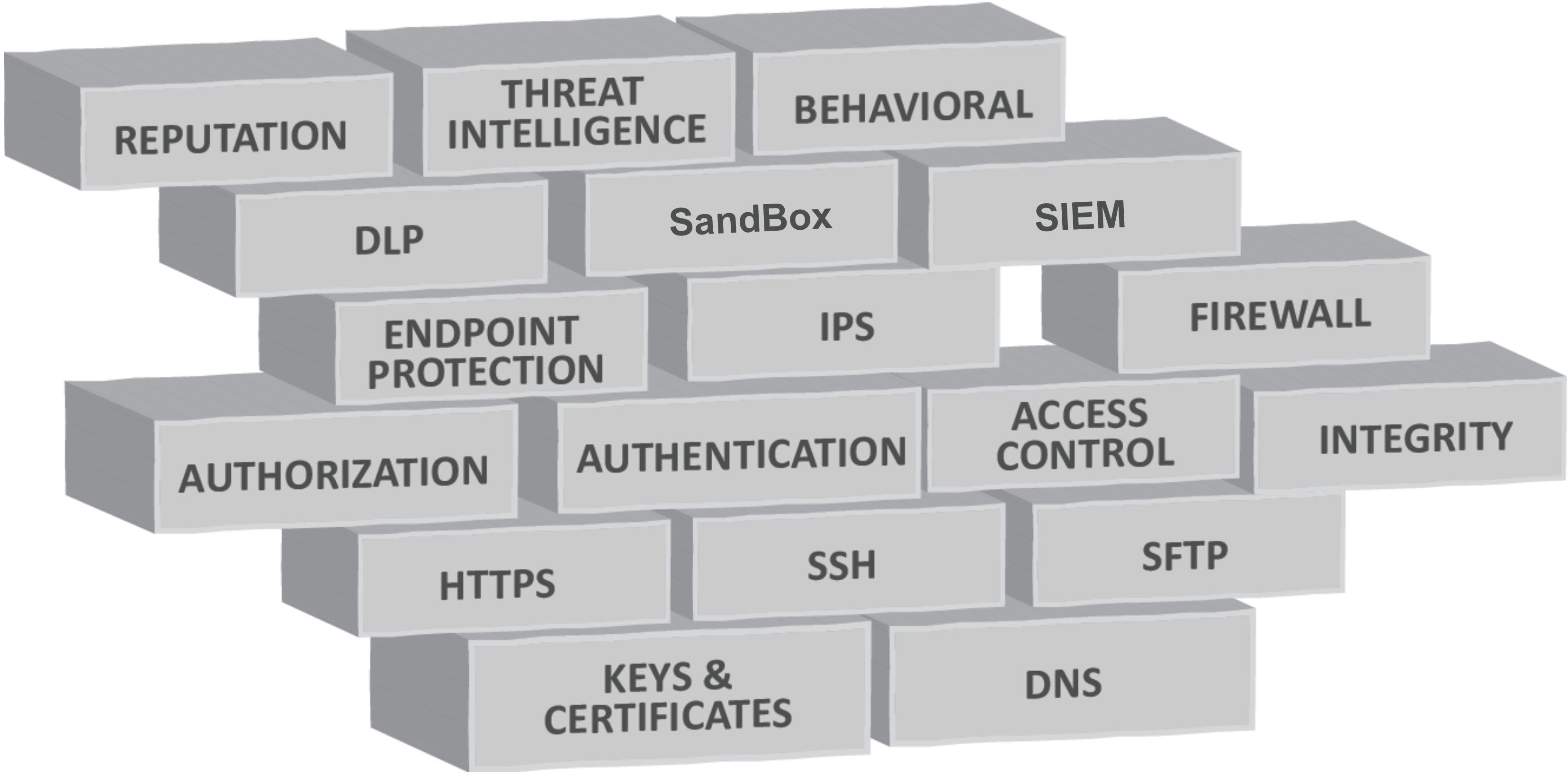
5 July 1993, *New Yorker Magazine*

Foundation of Online Security

KEYS & CERTIFICATES

DNS

Building Layered Security



REPUTATION

THREAT INTELLIGENCE

BEHAVIORAL

DLP

SandBox

SIEM

ENDPOINT PROTECTION

IPS

FIREWALL

AUTHORIZATION

AUTHENTICATION

ACCESS CONTROL

INTEGRITY

HTTPS

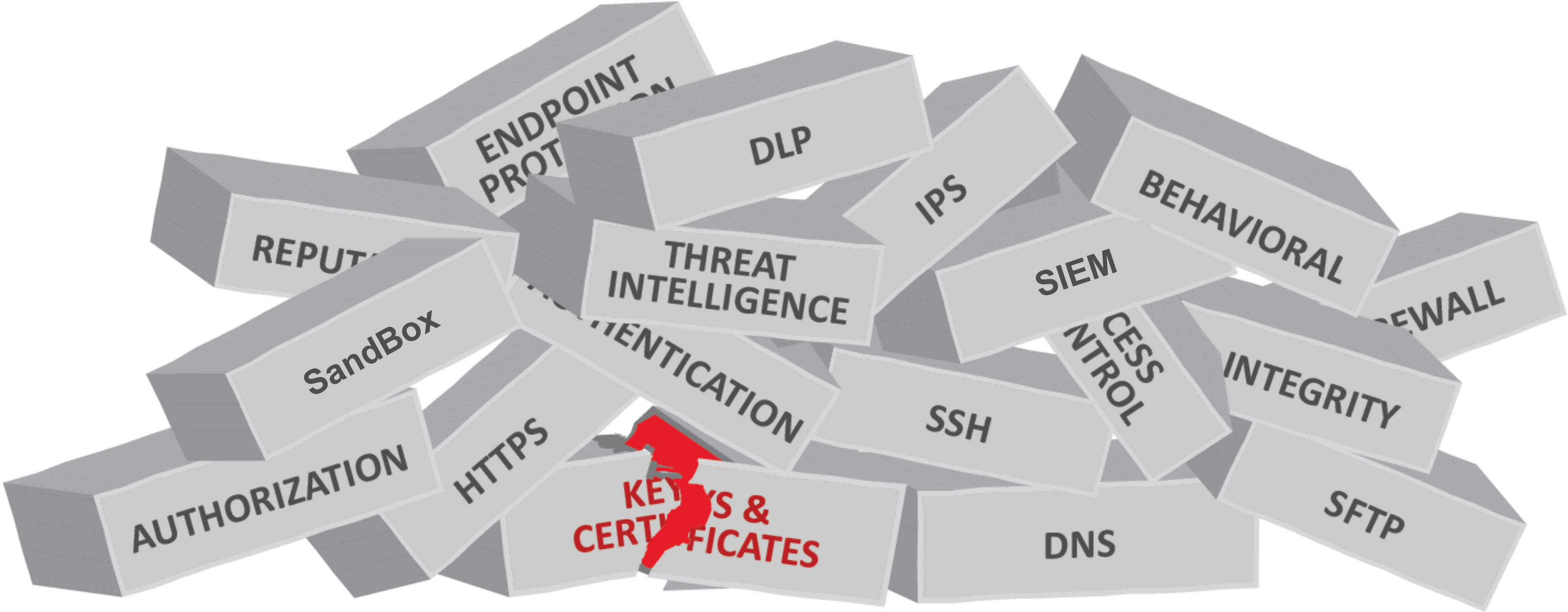
SSH

SFTP

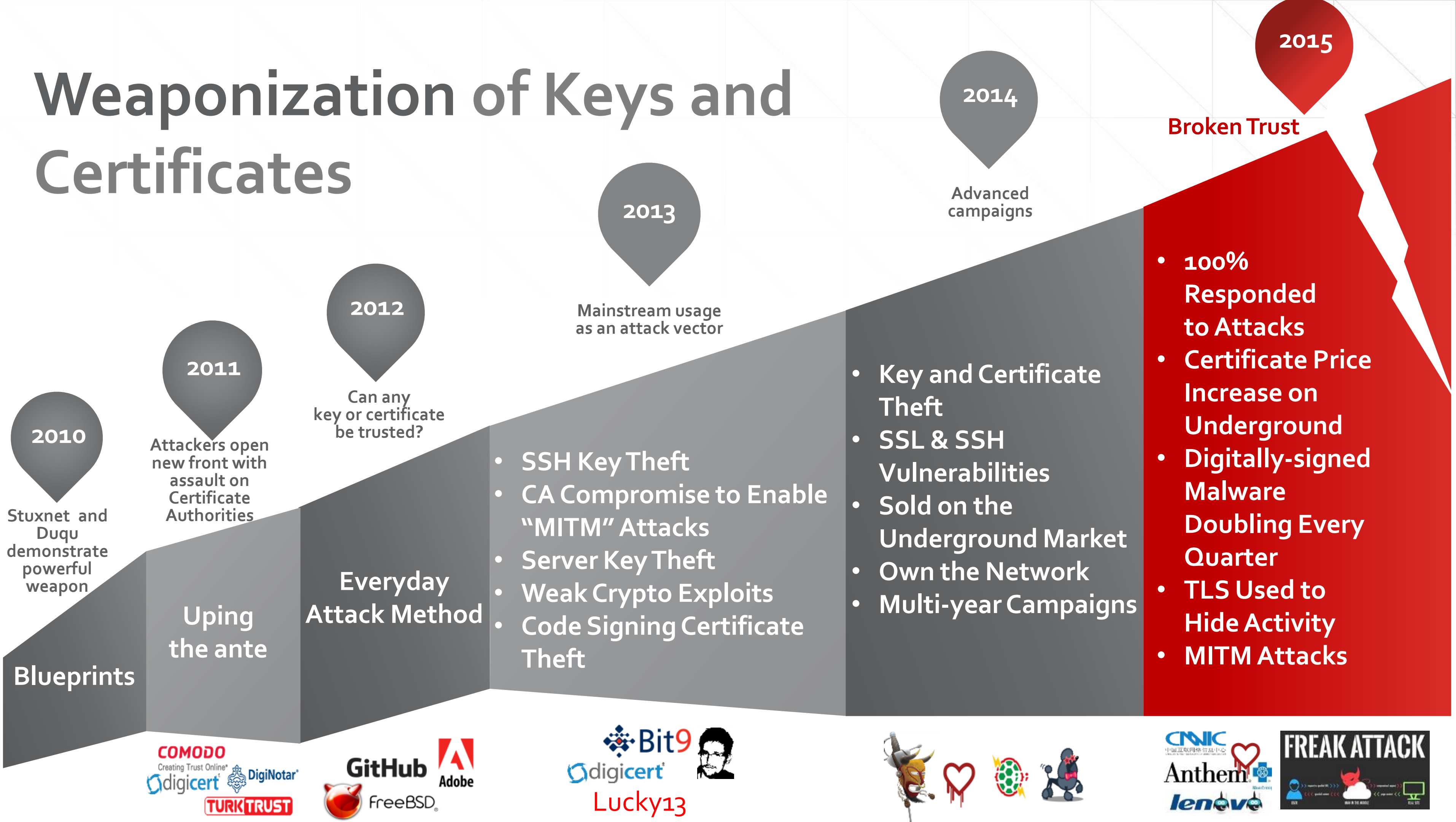
KEYS & CERTIFICATES

DNS

When the Foundation Isn’t Protected



Weaponization of Keys and Certificates



2010

Stuxnet and Duqu demonstrate powerful weapon

Blueprints

2011

Attackers open new front with assault on Certificate Authorities

Uping the ante

COMODO Creating Trust Online

digicert

DigiNotar

TURKTRUST

2012

Can any key or certificate be trusted?

Everyday Attack Method

GitHub

Adobe

FreeBSD

2013

Mainstream usage as an attack vector

- SSH Key Theft
- CA Compromise to Enable “MITM” Attacks
- Server Key Theft
- Weak Crypto Exploits
- Code Signing Certificate Theft

Bit9

digicert

Lucky13

2014

Advanced campaigns

- Key and Certificate Theft
- SSL & SSH Vulnerabilities
- Sold on the Underground Market
- Own the Network
- Multi-year Campaigns

2015

Broken Trust

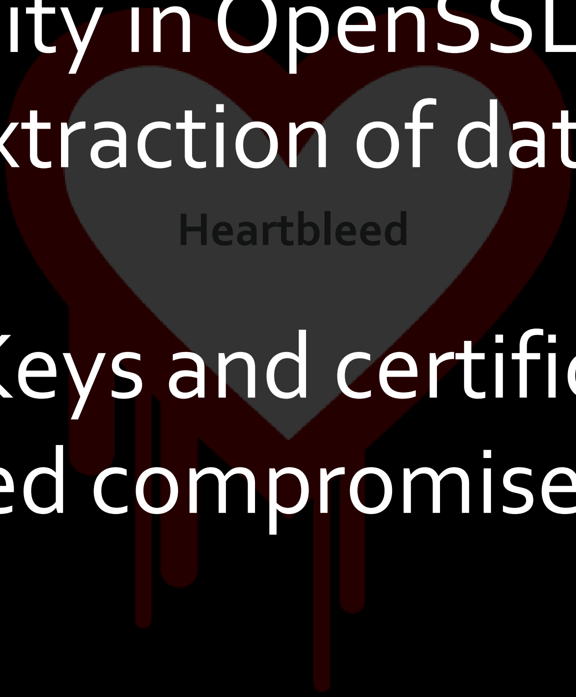
- 100% Responded to Attacks
- Certificate Price Increase on Underground
- Digitally-signed Malware Doubling Every Quarter
- TLS Used to Hide Activity
- MITM Attacks

CNNIC

Anthem

lenovo

FREAK ATTACK



- Vulnerability in OpenSSL
- Enables extraction of data without a breach
- SSL/TLS Keys and certificates **must** be assumed compromised

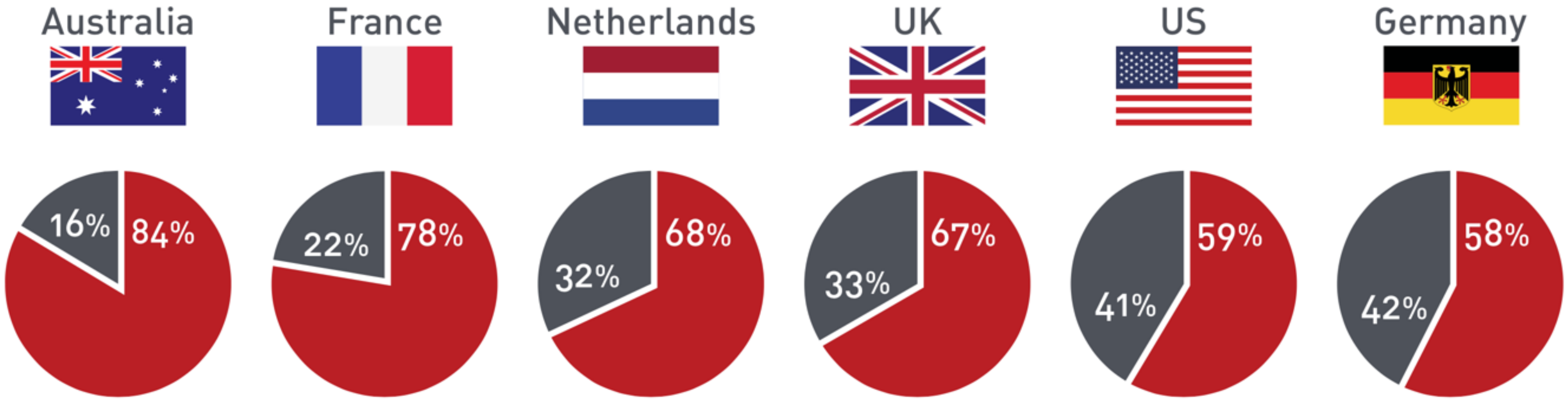
Patch vulnerable OpenSSL systems

Assume ALL keys and certificates compromised

Must generate new keys and certificates

Validate changes to demonstrate remediation

Global 2000: Heartbleed Remediation



April 2015

25,540 KEYS & CERTIFICATES

On average per company

UP 40% FROM 2013

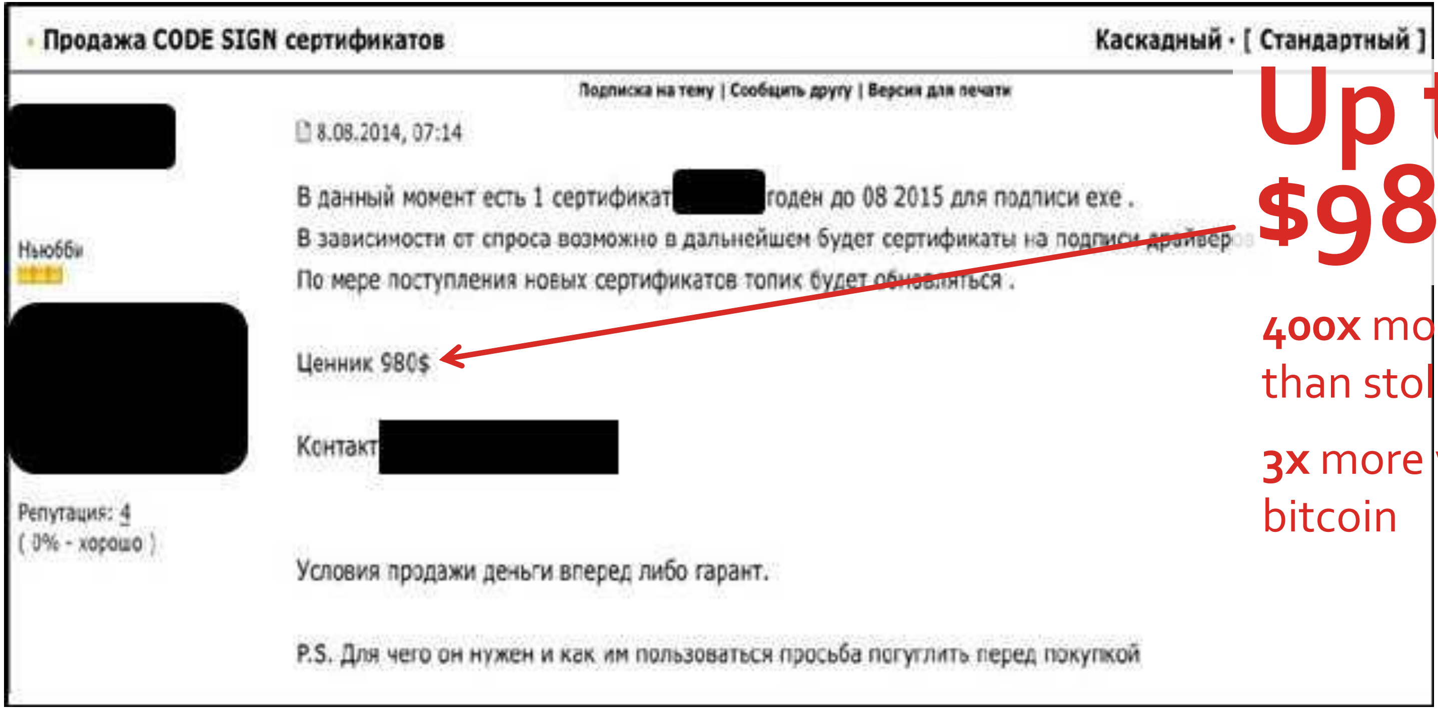
↑ 18,351

$1000 PRICE TAG

For a stolen certificate in the underground marketplace

“Stealing Certificates will be the Next Big Market for Hackers”

Marketplace for Stolen Certificates



Продажа CODE SIGN сертификатов

Каскадный · [Стандартный]

Подписка на тему | Сообщить другу | Версия для печати

[redacted]

8.08.2014, 07:14

В данный момент есть 1 сертификат [redacted] годен до 08 2015 для подписи exe .
В зависимости от спроса возможно в дальнейшем будет сертификаты на подписи драйвер
По мере поступления новых сертификатов топик будет обновляться .

Ньюбби

[redacted]

Ценник 980$

Контакт [redacted]

Репутация: 4
(0% - хорошо)

Условия продажи деньги вперед либо гарант.

P.S. Для чего он нужен и как им пользоваться просьба погуглить перед покупкой

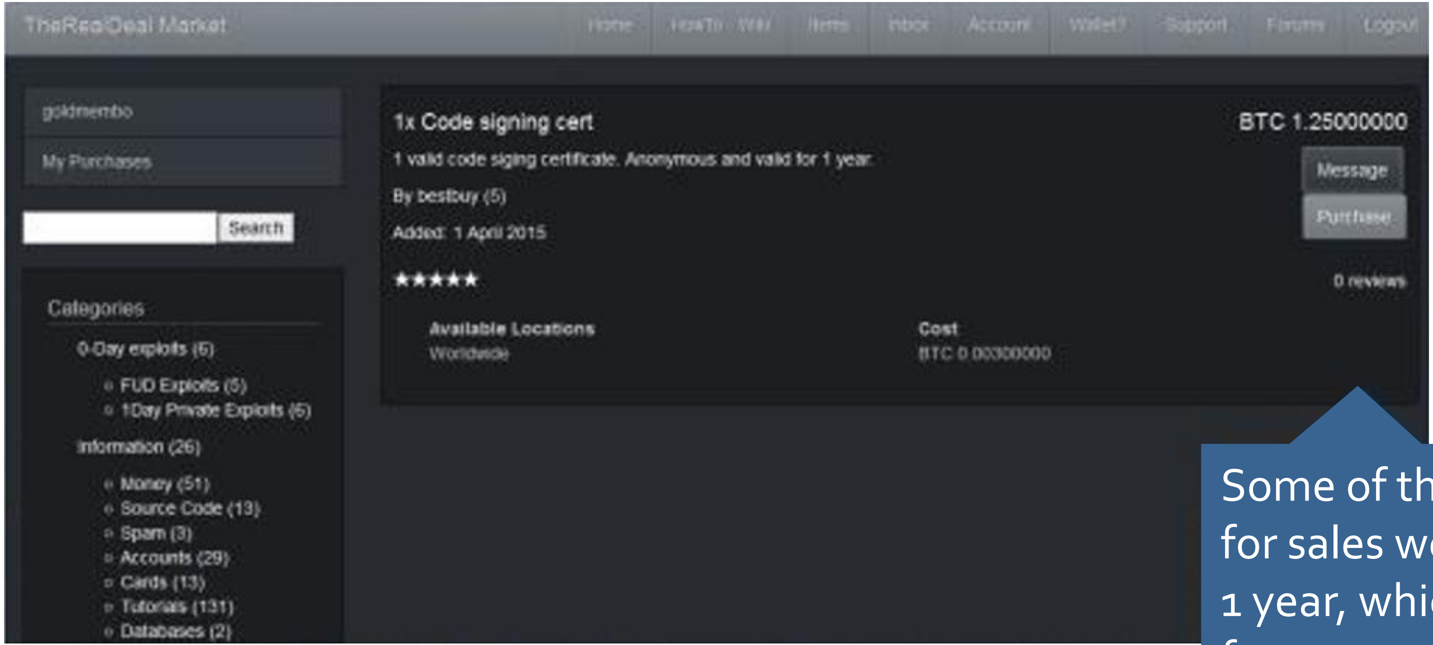
Up to $980/ea

400x more valuable than stolen credit card

3x more valuable than bitcoin

SenseCy
Sensing Cyber

Underground Certificates-as-a-service (CaaS)



Categories

- 0-Day exploits (6)
  - FUD Exploits (6)
  - 1Day Private Exploits (6)
- Information (26)
  - Money (51)
  - Source Code (13)
  - Spam (3)
  - Accounts (29)
  - Cards (13)
  - Tutorials (131)
  - Databases (2)

1x Code signing cert

BTC 1.25000000

1 valid code siging certificate. Anonymous and valid for 1 year.

By bestbuy (5)

Added: 1 April 2015

★★★★★

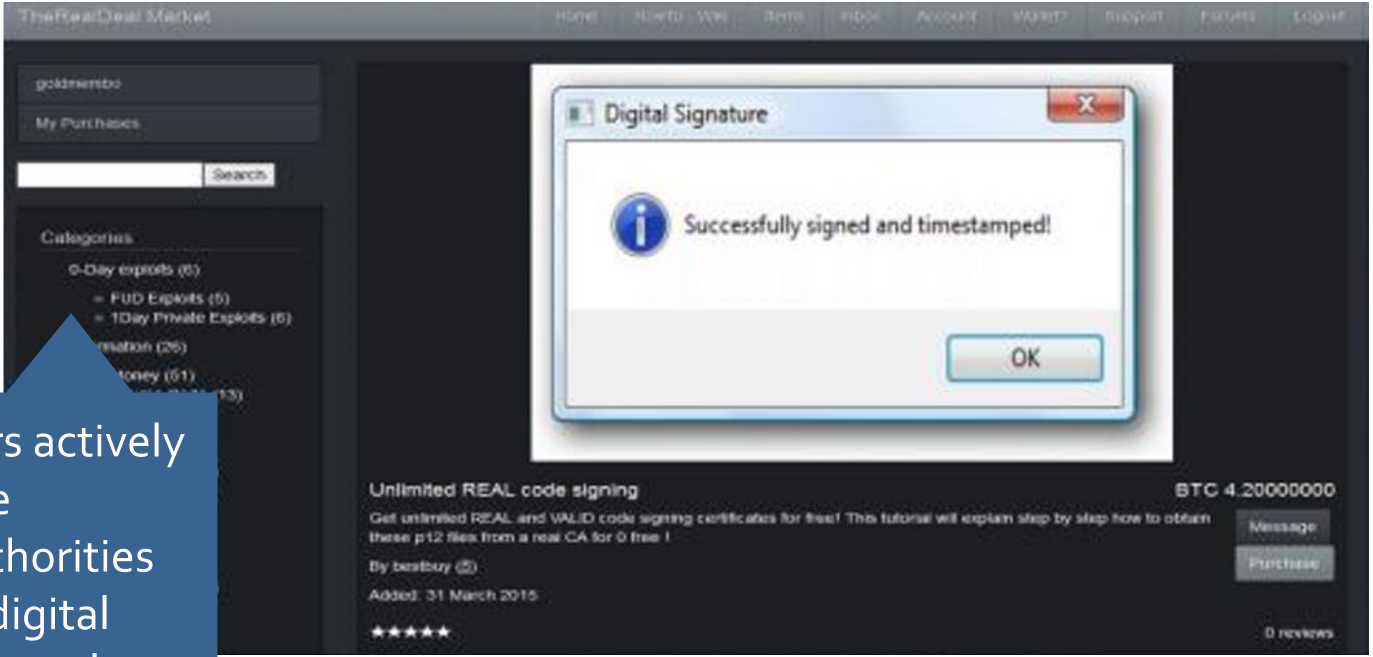
0 reviews

Available Locations	Cost
Worldwide	BTC 0.00000000

Some of the certificates for sales were issued for 1 year, which is enough for targeted APT

InfoArmor: GovRAT

Underground Certificates-as-a-service (CaaS)



Digital Signature

Successfully signed and timestamped!

OK

Unlimited REAL code signing BTC 4.20000000

Get unlimited REAL and VALID code signing certificates for free! This tutorial will explain step by step how to obtain these p12 files from a real CA for 0 free !

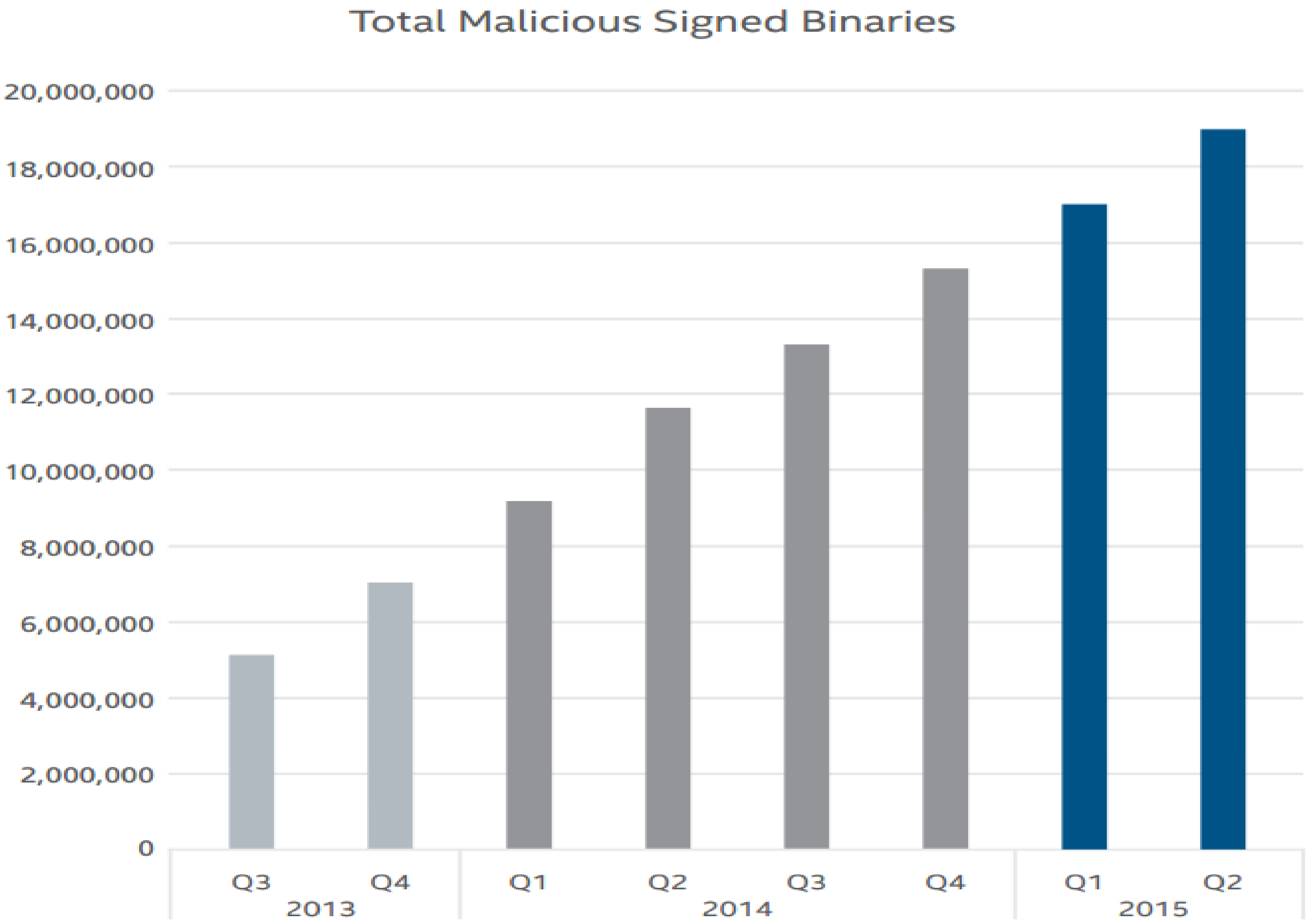
By bestbuy (5)

Added: 31 March 2015

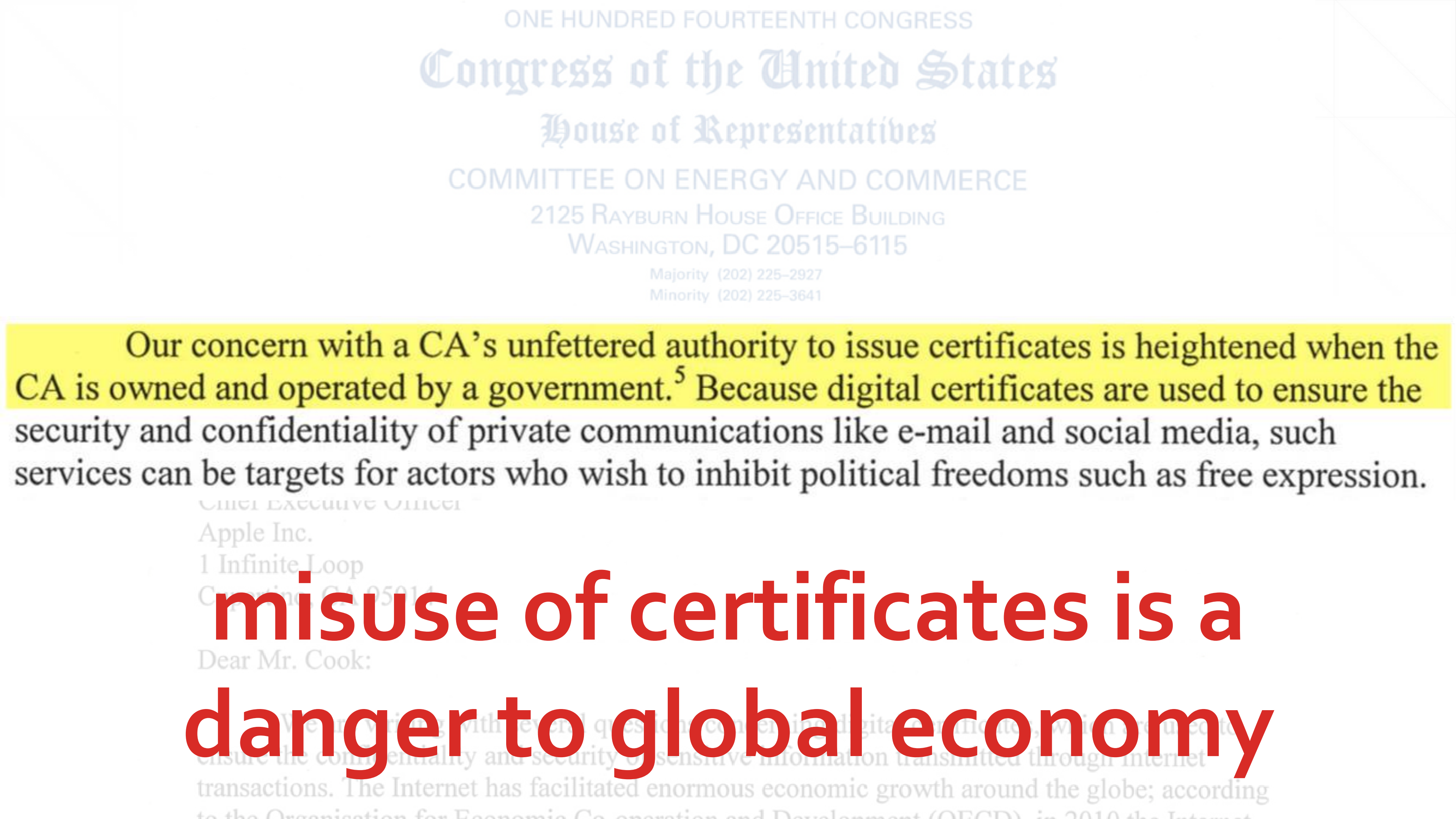
★★★★★ 0 reviews

ad actors actively
egitimate
icate authorities
to issue digital
icates for malware

InfoArmor: GovRAT



intel Security



ONE HUNDRED FOURTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 Rayburn House Office Building
Washington, DC 20515–6115

Majority (202) 225–2927
Minority (202) 225–3641

Our concern with a CA's unfettered authority to issue certificates is heightened when the CA is owned and operated by a government.[5] Because digital certificates are used to ensure the security and confidentiality of private communications like e-mail and social media, such services can be targets for actors who wish to inhibit political freedoms such as free expression.

Chief Executive Officer
Apple Inc.
1 Infinite Loop
Cupertino, CA 95014

Dear Mr. Cook:

We are writing with several questions concerning digital certificates, which are used to ensure the confidentiality and security of sensitive information transmitted through Internet transactions. The Internet has facilitated enormous economic growth around the globe; according to the Organization for Economic Co-operation and Development (OECD), in 2010 the Internet

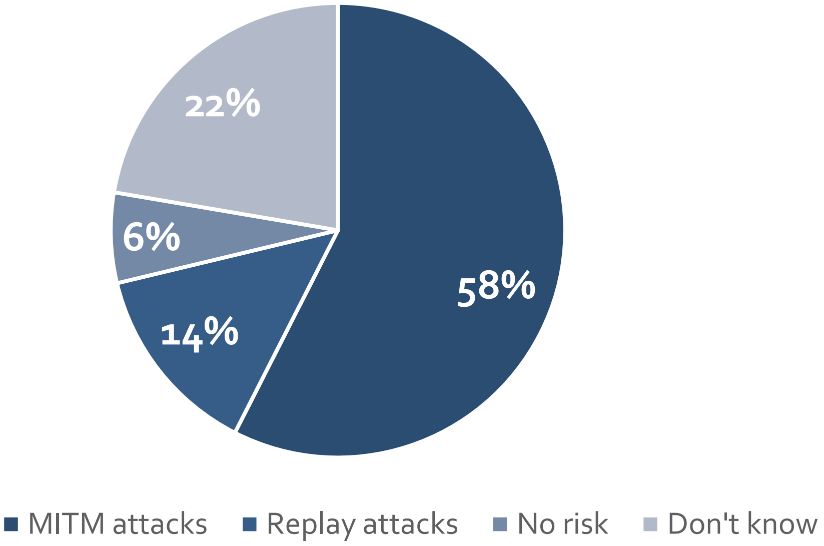
misuse of certificates is a danger to global economy

CNNIC
中国互联网络信息中心
CHINA INTERNET NETWORK INFORMATION CENTER
中华人民共和国国家互联网信息办公室
Cyberspace Administration of China
WWW.CAC.GOV.CN
请输入检索关键词
世界互联网大会
World Internet
Conference

trusted: in your
computer,
browser,
smartphone,
server

Example: MCS Holdings, an intermediate CA for CNNIC issued a fraudulent certificate for Google to perform Man-in-the-Middle

Security risks from untrustworthy CAs like CNNIC?



Venafi: Black Hat 2015 survey

Browser action to protect you

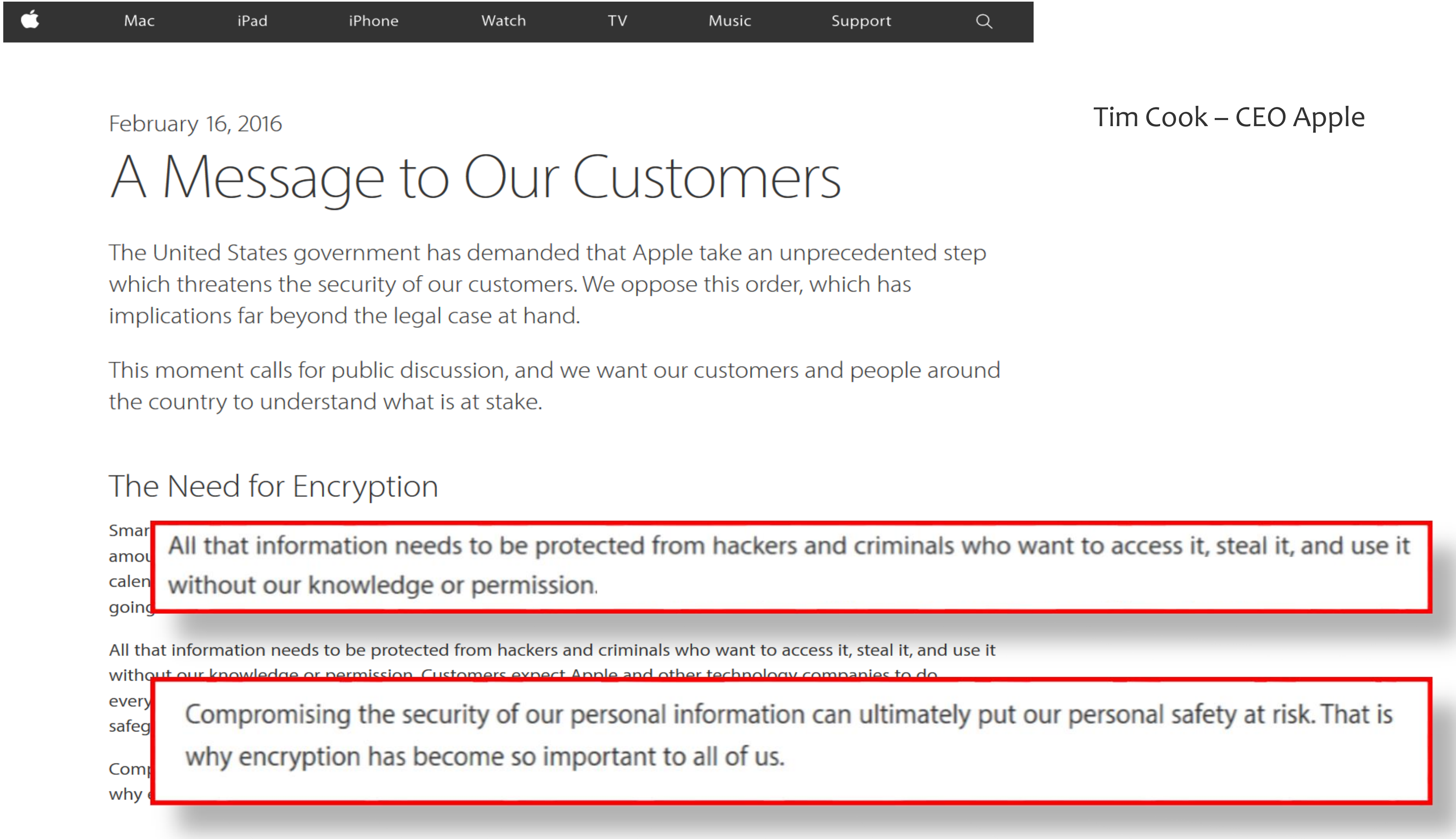
Untrusted by Google

Untrusted by Mozilla

Trusted by Apple

Trusted by Microsoft

Tim Cook – CEO Apple



February 16, 2016

A Message to Our Customers

The United States government has demanded that Apple take an unprecedented step which threatens the security of our customers. We oppose this order, which has implications far beyond the legal case at hand.

This moment calls for public discussion, and we want our customers and people around the country to understand what is at stake.

The Need for Encryption

Smar
amou
calen
going

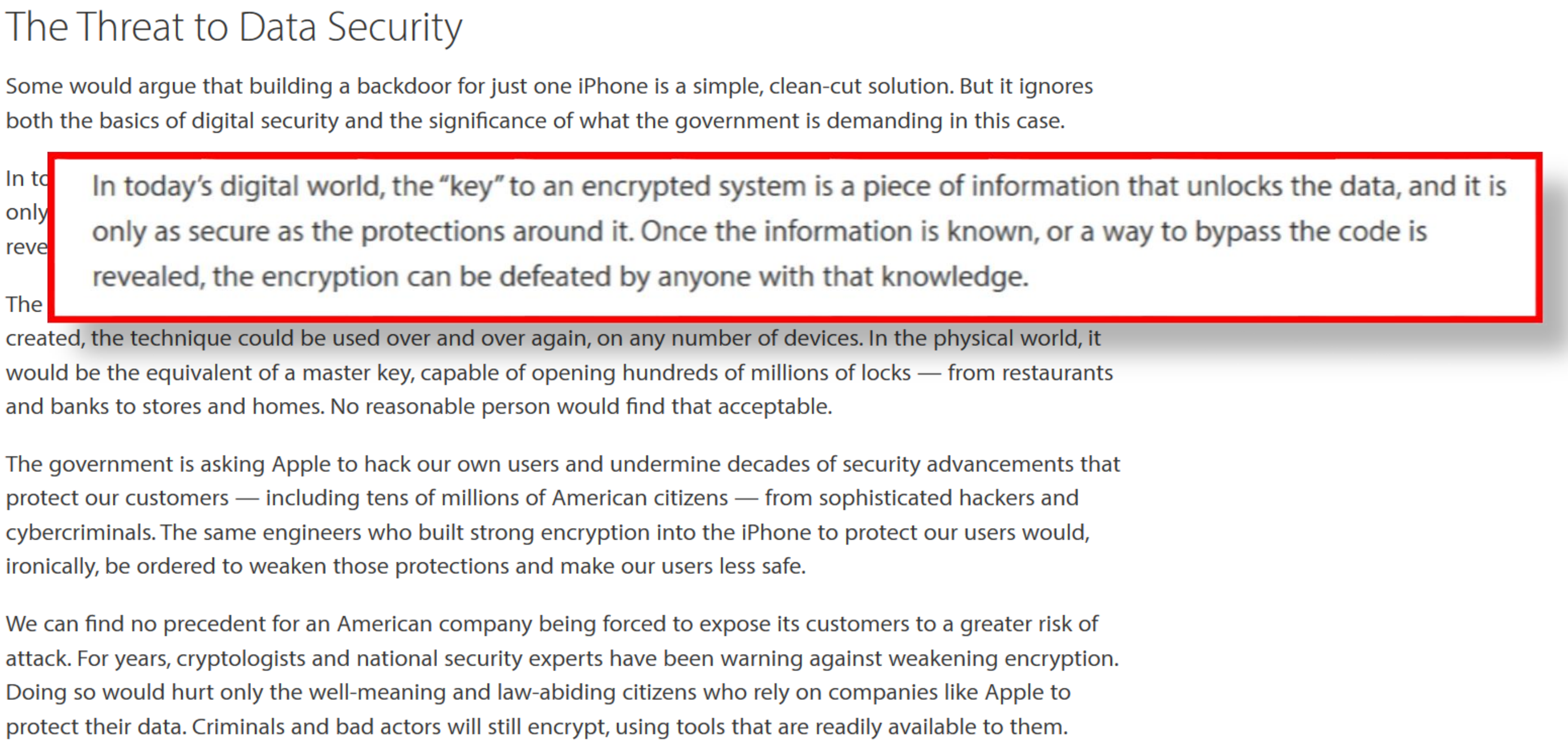
All that information needs to be protected from hackers and criminals who want to access it, steal it, and use it without our knowledge or permission. Customers expect Apple and other technology companies to do
every
safeg

Comp
why

All that information needs to be protected from hackers and criminals who want to access it, steal it, and use it without our knowledge or permission.

Compromising the security of our personal information can ultimately put our personal safety at risk. That is why encryption has become so important to all of us.

Tim Cook Letter (Cont'd)



The Threat to Data Security

Some would argue that building a backdoor for just one iPhone is a simple, clean-cut solution. But it ignores both the basics of digital security and the significance of what the government is demanding in this case.

In to
only
reve

> In today's digital world, the "key" to an encrypted system is a piece of information that unlocks the data, and it is only as secure as the protections around it. Once the information is known, or a way to bypass the code is revealed, the encryption can be defeated by anyone with that knowledge.

The

created, the technique could be used over and over again, on any number of devices. In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks — from restaurants and banks to stores and homes. No reasonable person would find that acceptable.

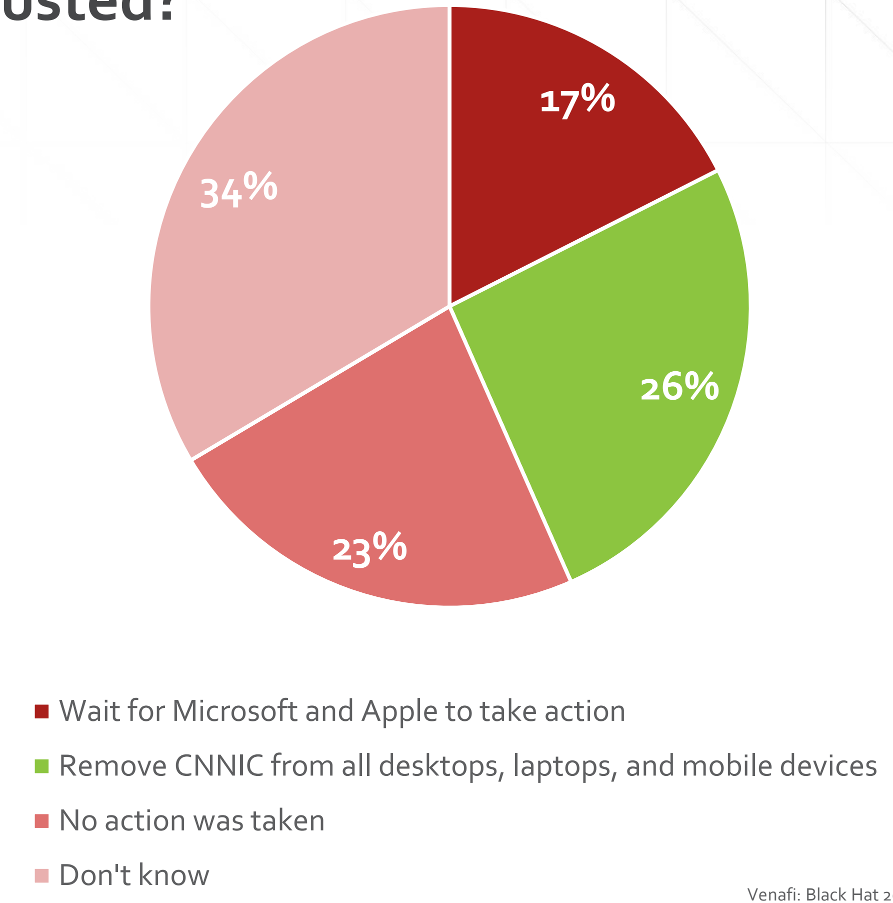
The government is asking Apple to hack our own users and undermine decades of security advancements that protect our customers — including tens of millions of American citizens — from sophisticated hackers and cybercriminals. The same engineers who built strong encryption into the iPhone to protect our users would, ironically, be ordered to weaken those protections and make our users less safe.

We can find no precedent for an American company being forced to expose its customers to a greater risk of attack. For years, cryptologists and national security experts have been warning against weakening encryption. Doing so would hurt only the well-meaning and law-abiding citizens who rely on companies like Apple to protect their data. Criminals and bad actors will still encrypt, using tools that are readily available to them.

What action did your organization take after CNNIC was deemed untrusted?

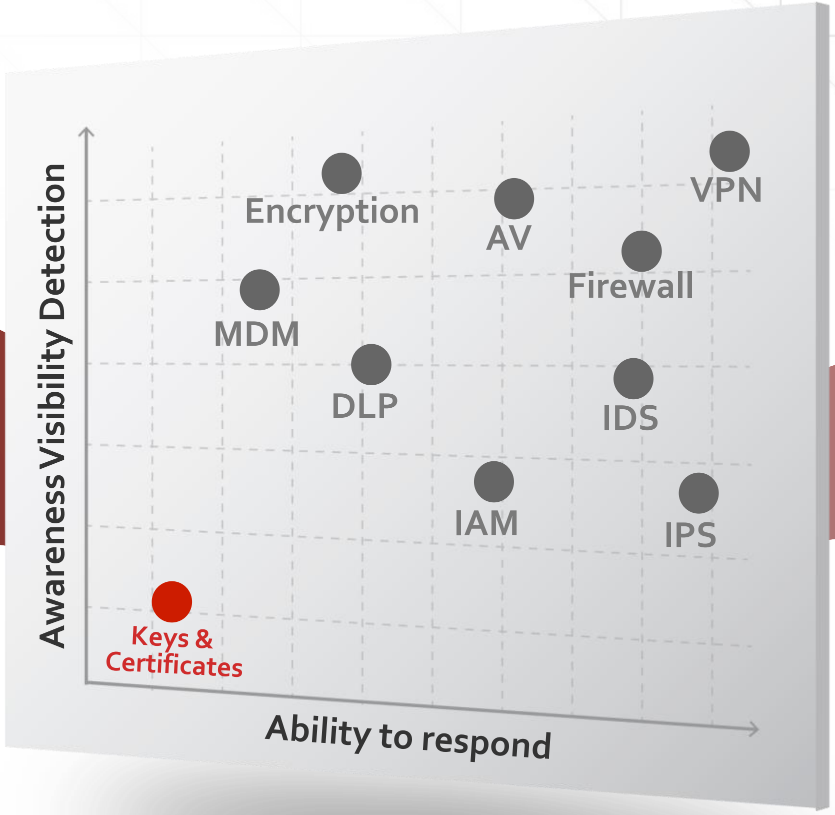
74%

remain exposed

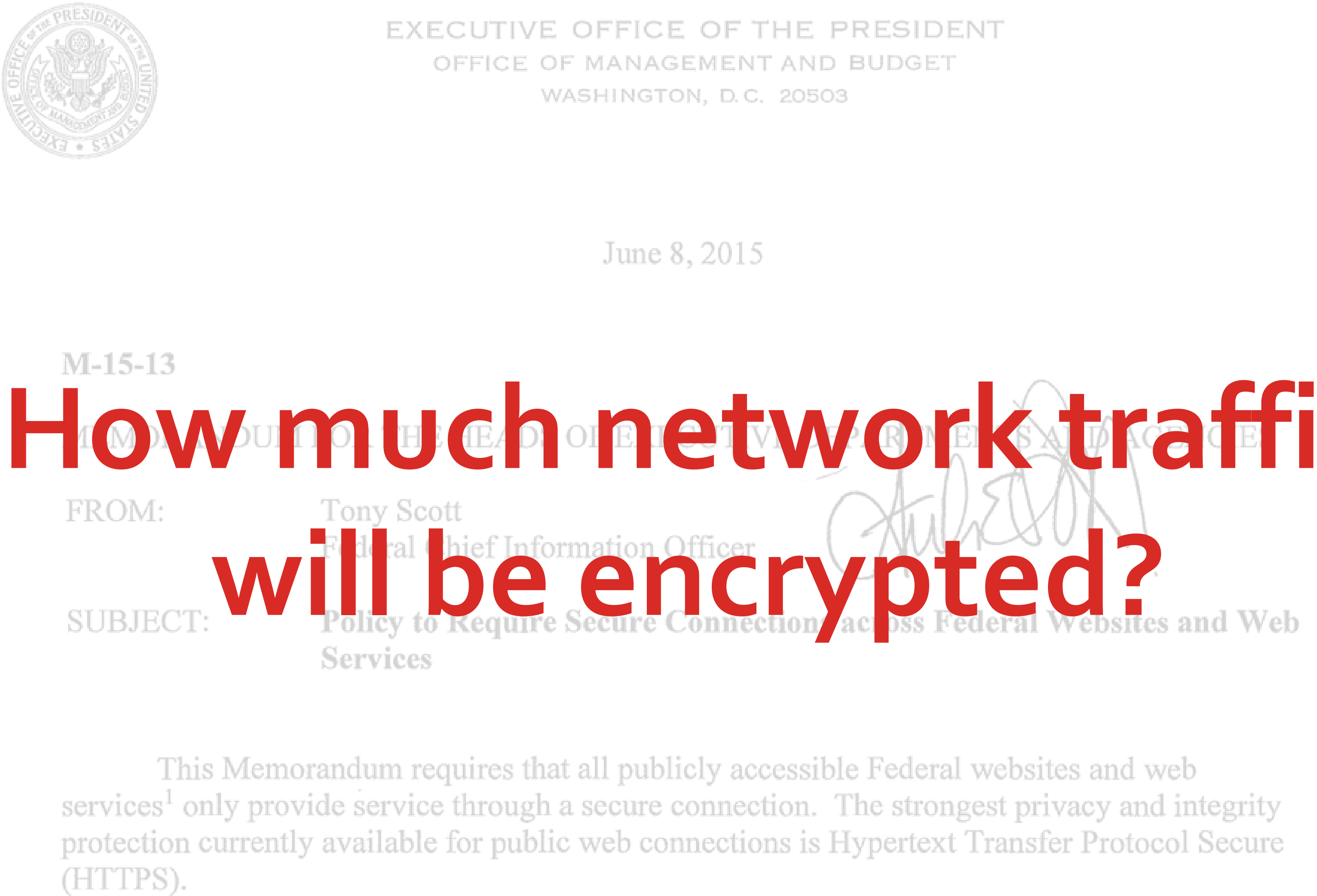


Venafi: Black Hat 2015 survey

Blind Spot in Security



How much network traffic will be encrypted?



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

June 8, 2015

M-15-13

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Tony Scott
Federal Chief Information Officer

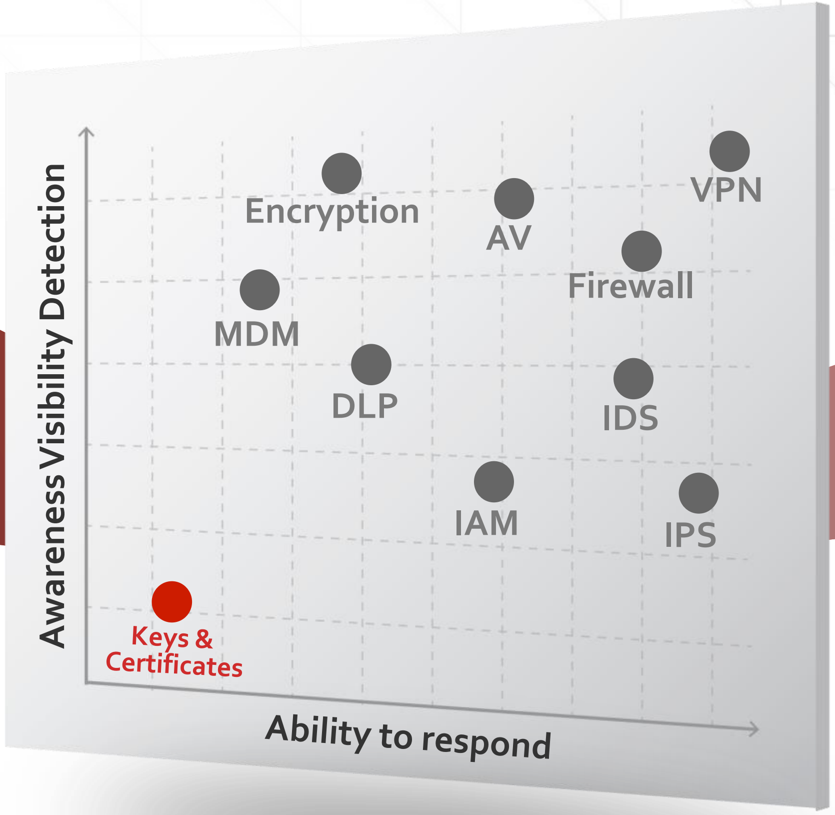
SUBJECT: **Policy to Require Secure Connections across Federal Websites and Web Services**

This Memorandum requires that all publicly accessible Federal websites and web services[1] only provide service through a secure connection. The strongest privacy and integrity protection currently available for public web connections is Hypertext Transfer Protocol Secure (HTTPS).

“50% of network attacks will use SSL by 2017”

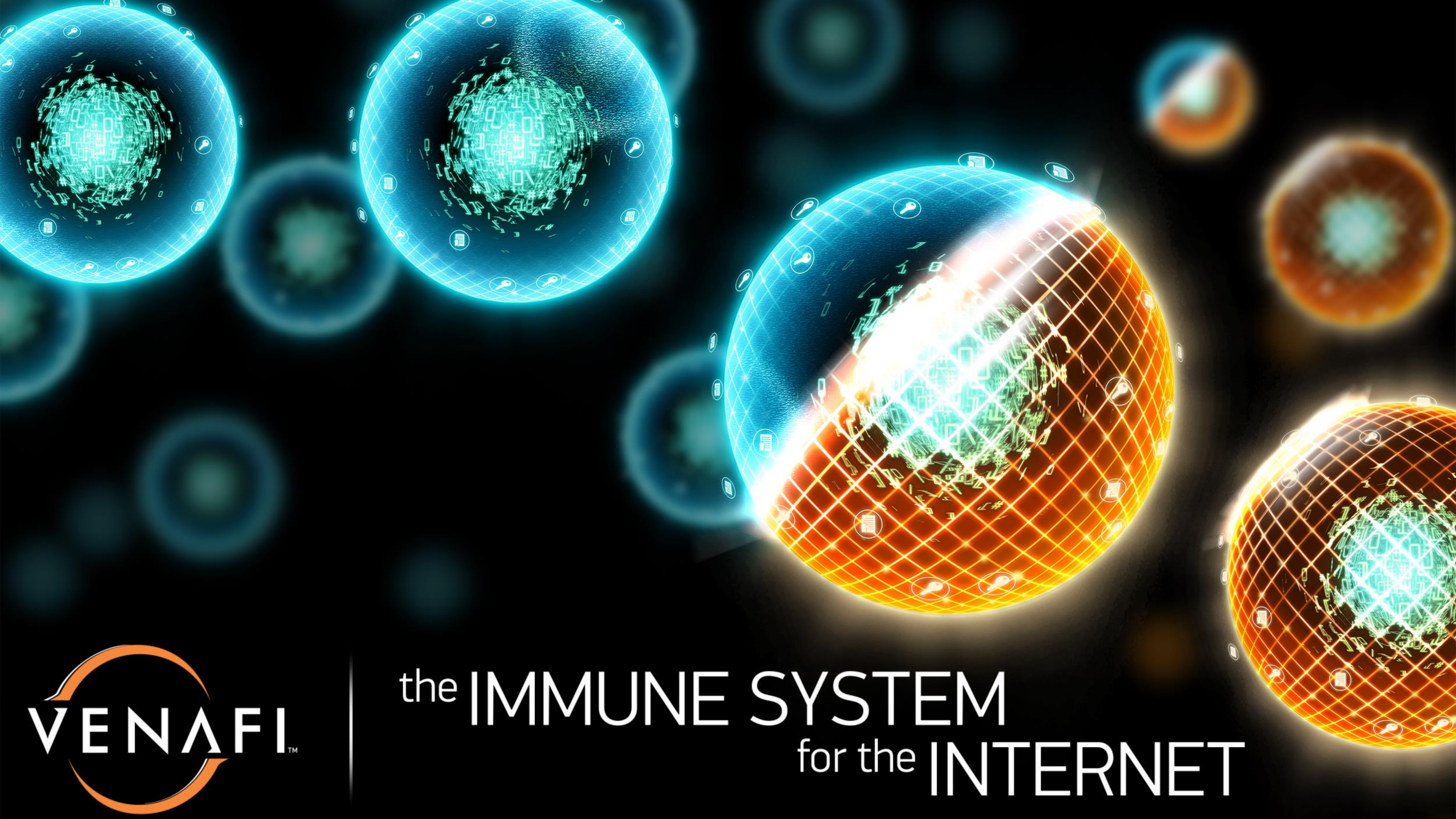
Gartner

Undermines Security



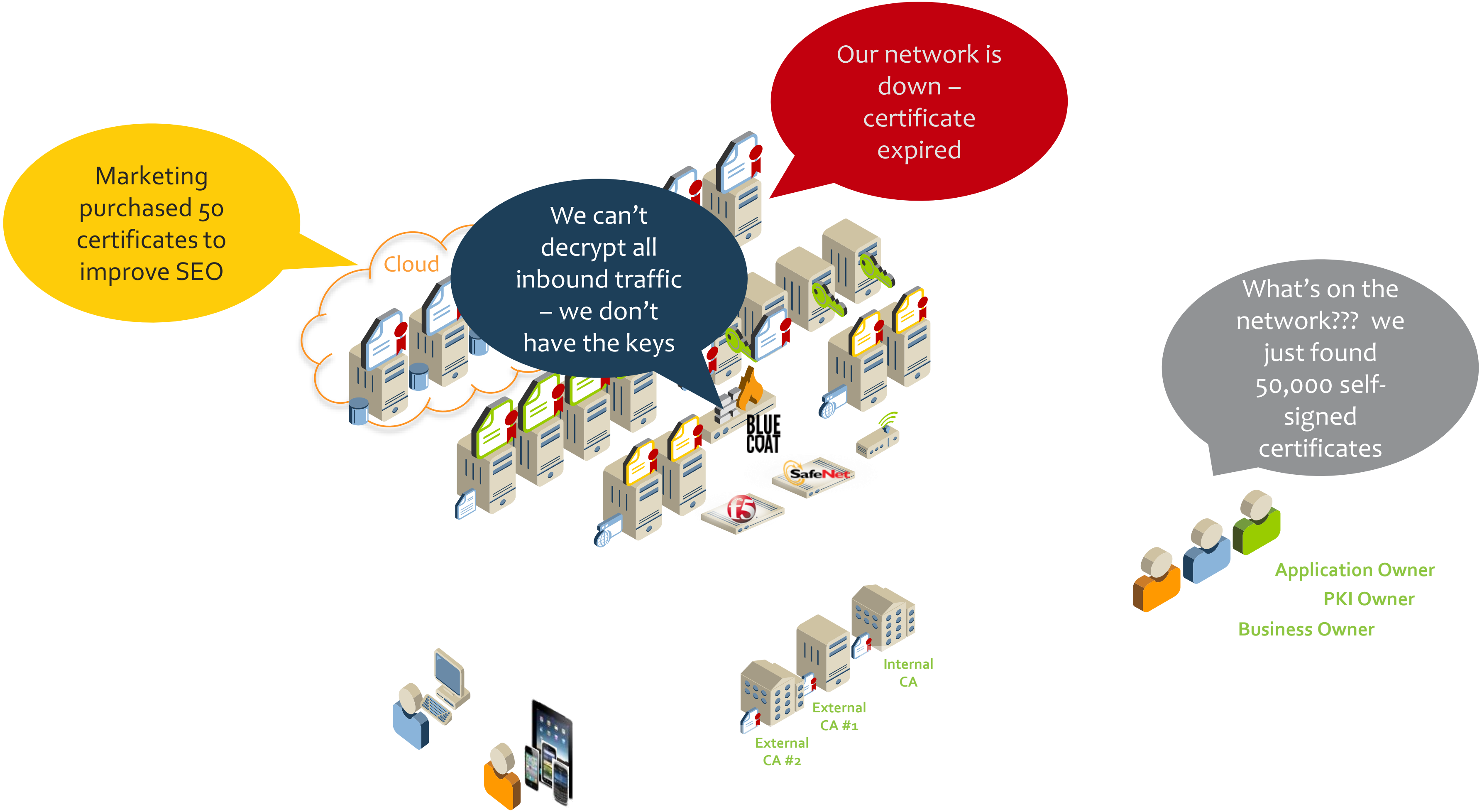
“Basically, the enterprise is a sitting duck.”

FORRESTER®



VENAFI™
the IMMUNE SYSTEM
for the INTERNET

Customer Problems we Find

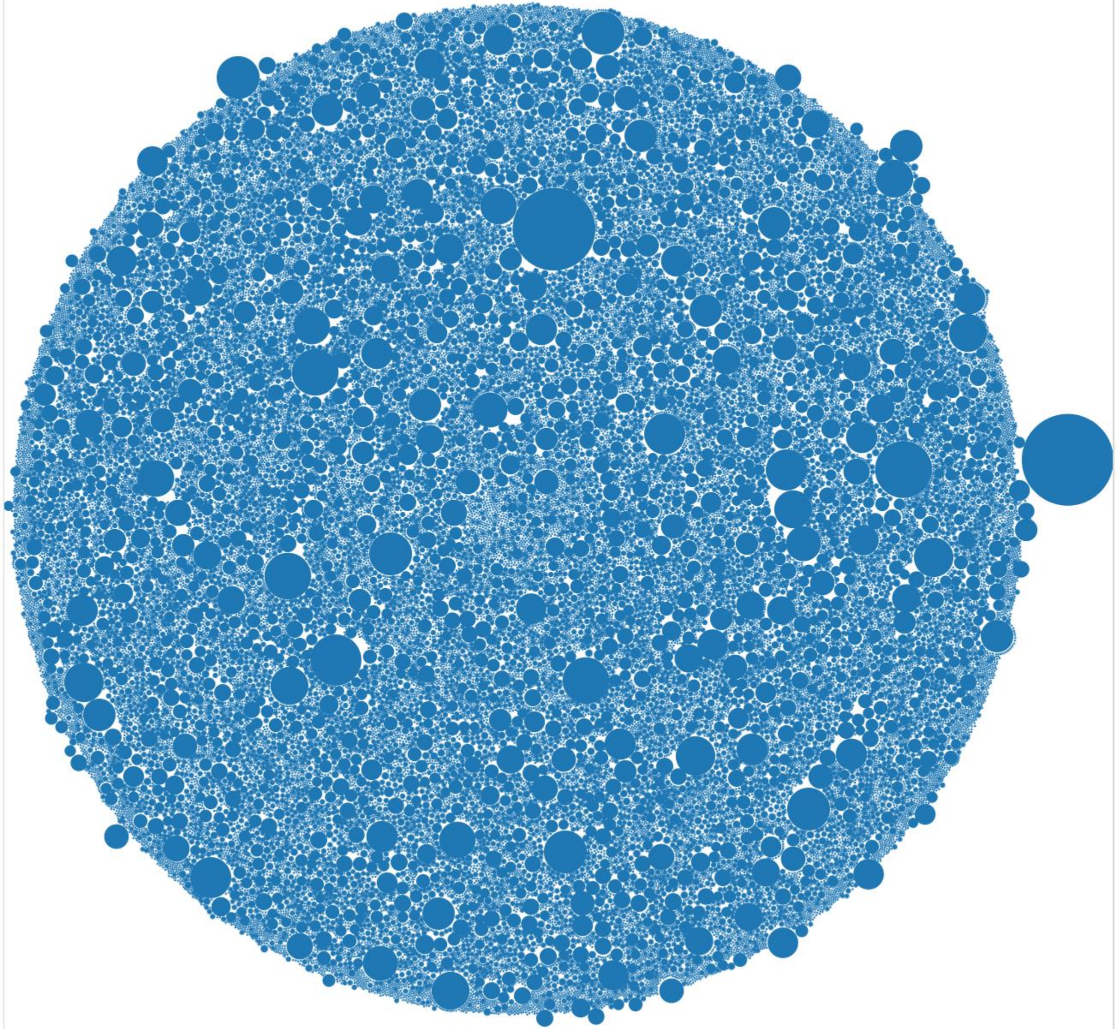


Marketing purchased 50 certificates to improve SEO

We can't decrypt all inbound traffic – we don't have the keys

Our network is down – certificate expired

What's on the network??? we just found 50,000 self-signed certificates



GLOBAL TELCO

millions of certificates

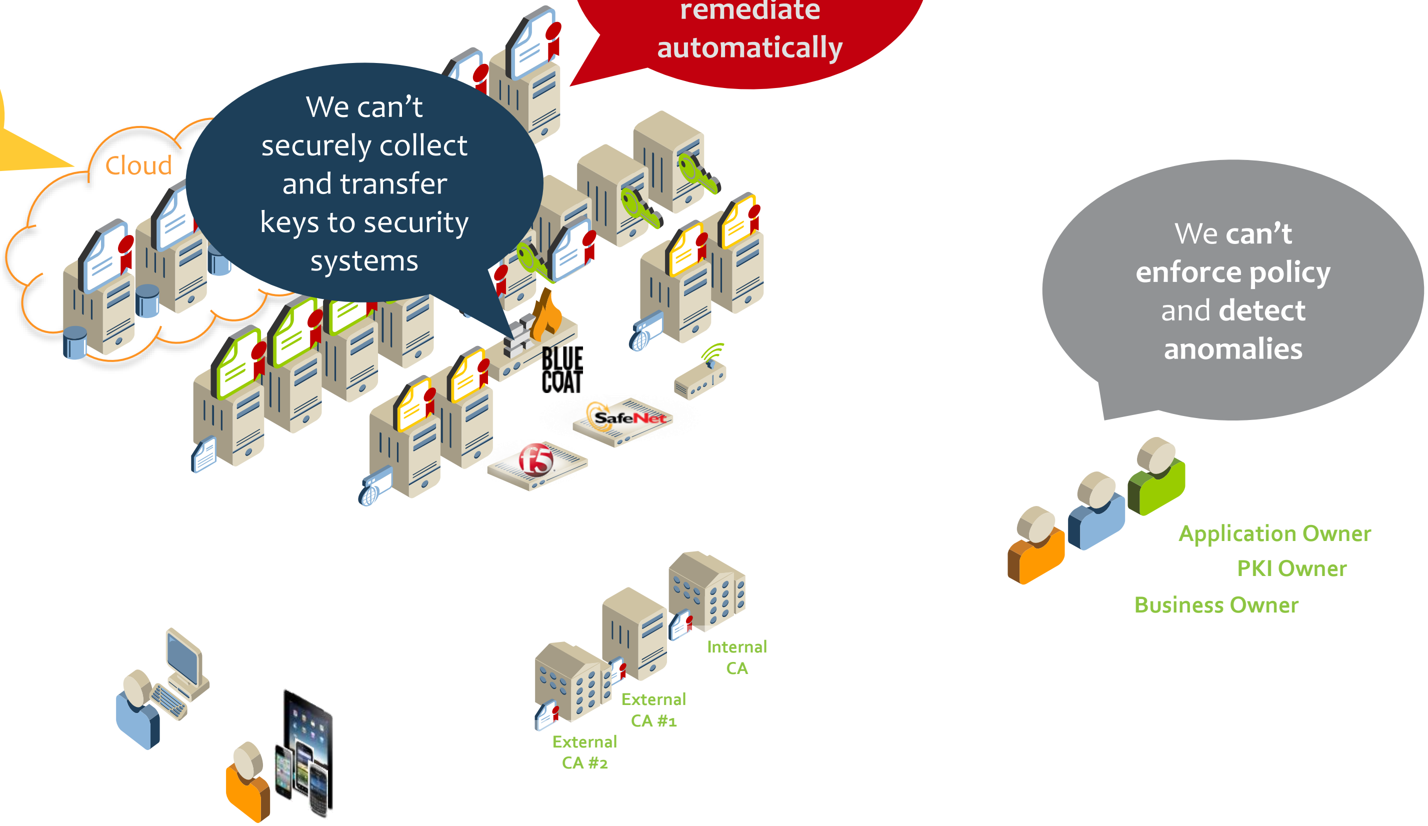
Consequences of the Problems we Find

We have **no visibility** in to certificates outside the firewall

We can't securely collect and transfer keys to security systems

We're **unable to continuously monitor** and **remediate automatically**

We **can't enforce policy** and **detect anomalies**



Where to Start?

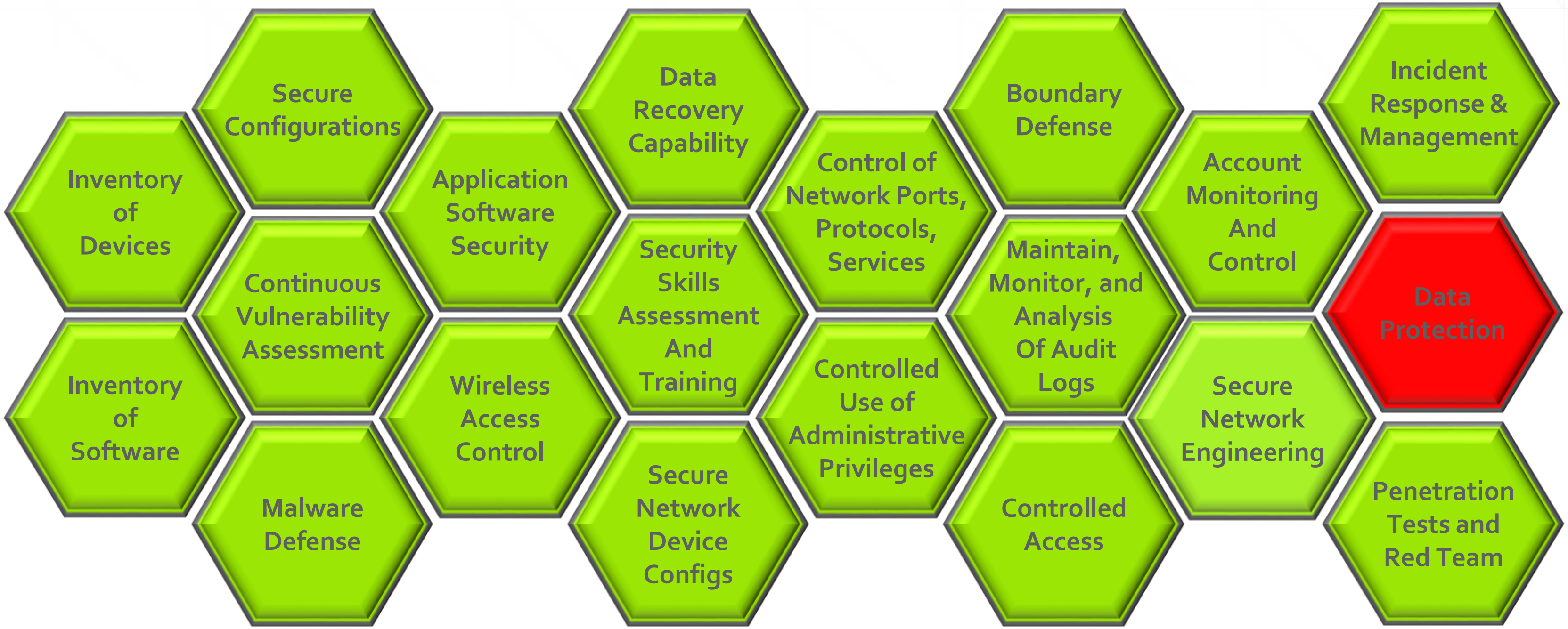
Survey and monitor all certificates

Secure keys as a ‘top priority’

Document and enforce policies, like revocation processes

Monitor security feeds for compromised CAs and certificates

SANS - 20 Critical Security Controls



Inventory of Devices

Inventory of Software

Secure Configurations

Continuous Vulnerability Assessment

Malware Defense

Application Software Security

Wireless Access Control

Data Recovery Capability

Security Skills Assessment And Training

Secure Network Device Configs

Control of Network Ports, Protocols, Services

Controlled Use of Administrative Privileges

Boundary Defense

Maintain, Monitor, and Analysis Of Audit Logs

Controlled Access

Account Monitoring And Control

Secure Network Engineering

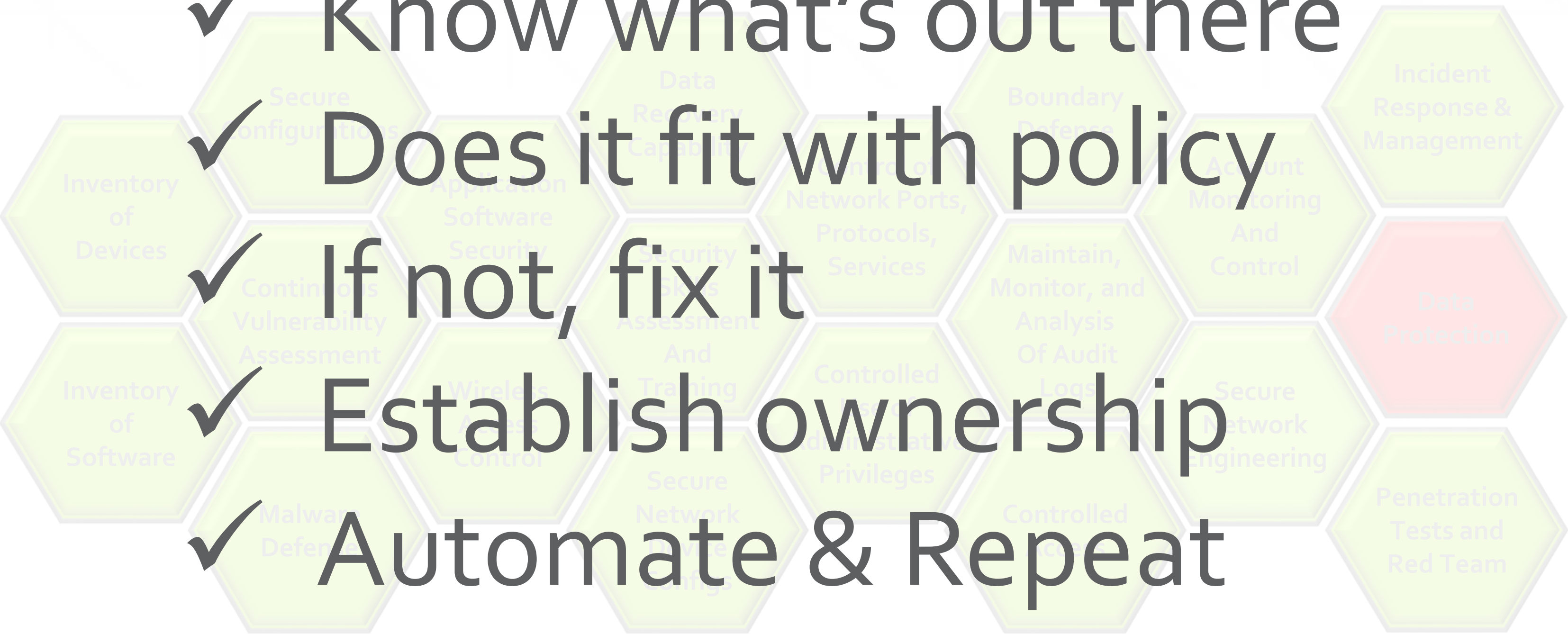
Incident Response & Management

Data Protection

Penetration Tests and Red Team

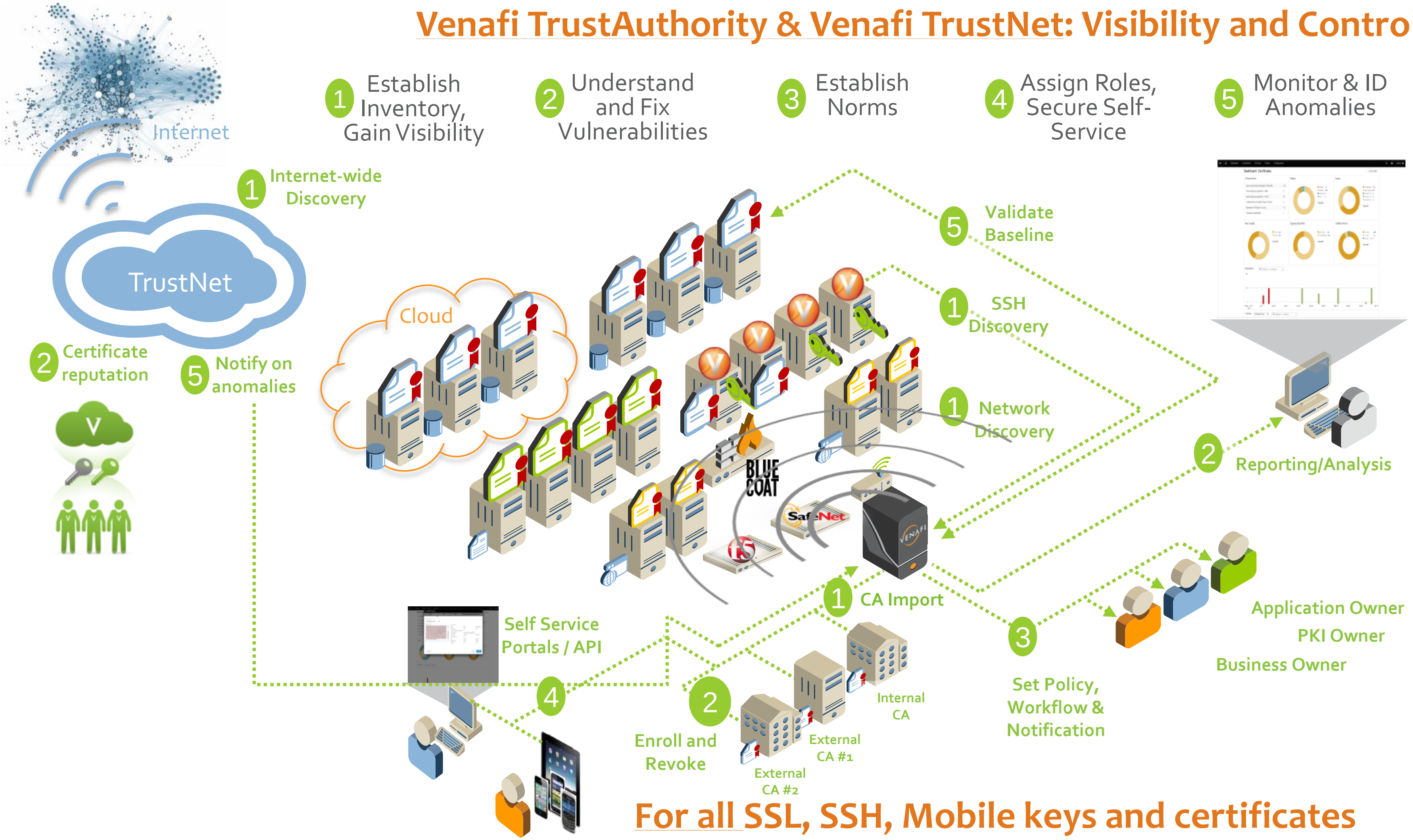
CSC17 Update

- ✓ Know what’s out there
- ✓ Does it fit with policy
- ✓ If not, fix it
- ✓ Establish ownership
- ✓ Automate & Repeat



Secure Configurations
Inventory of Devices
Application Software Security
Data Recovery Capability
Network Ports, Protocols, Services
Boundary Defense
Account Monitoring And Control
Incident Response & Management
Continuous Vulnerability Assessment
Security Skills Assessment And Training
Maintain, Monitor, and Analysis Of Audit Logs
Data Protection
Inventory of Software
Wireless Access Control
Controlled Use of Administrative Privileges
Secure Network Engineering
Malware Defenses
Secure Network Device Configs
Controlled Access
Penetration Tests and Red Team

Venafi TrustAuthority & Venafi TrustNet: Visibility and Control



1 Establish Inventory, Gain Visibility

2 Understand and Fix Vulnerabilities

3 Establish Norms

4 Assign Roles, Secure Self-Service

5 Monitor & ID Anomalies

Internet

TrustNet

1 Internet-wide Discovery

2 Certificate reputation

5 Notify on anomalies

Cloud

5 Validate Baseline

1 SSH Discovery

1 Network Discovery

1 CA Import

2 Reporting/Analysis

Self Service Portals / API

4

2 Enroll and Revoke

Internal CA

External CA #1

External CA #2

3 Set Policy, Workflow & Notification

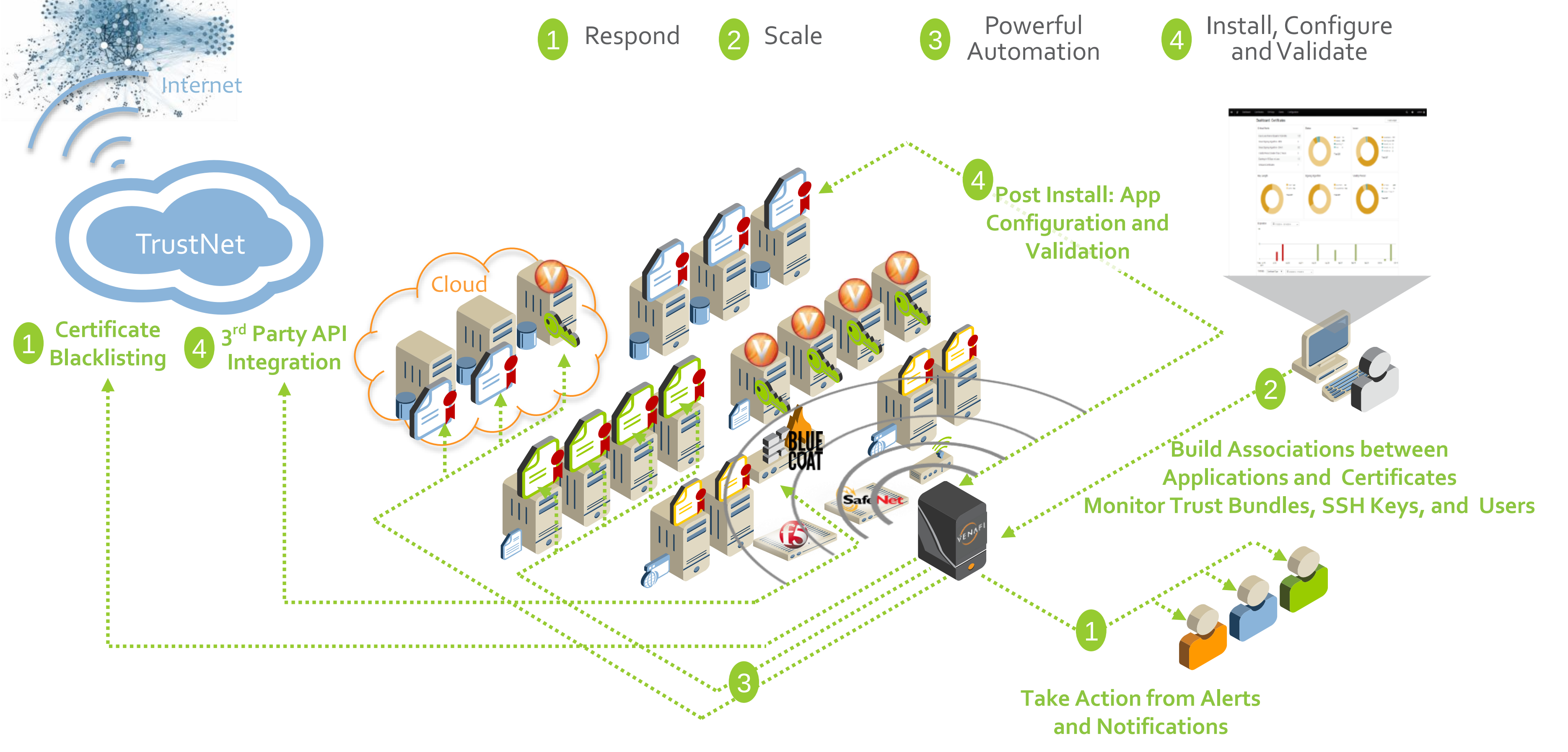
Application Owner

PKI Owner

Business Owner

For all SSL, SSH, Mobile keys and certificates

Venafi TrustForce & Venafi TrustNet: Rapid Response and Remediation



1 Respond

2 Scale

3 Powerful Automation

4 Install, Configure and Validate

1 Certificate Blacklisting

4 3rd Party API Integration

4 Post Install: App Configuration and Validation

2 Build Associations between Applications and Certificates Monitor Trust Bundles, SSH Keys, and Users

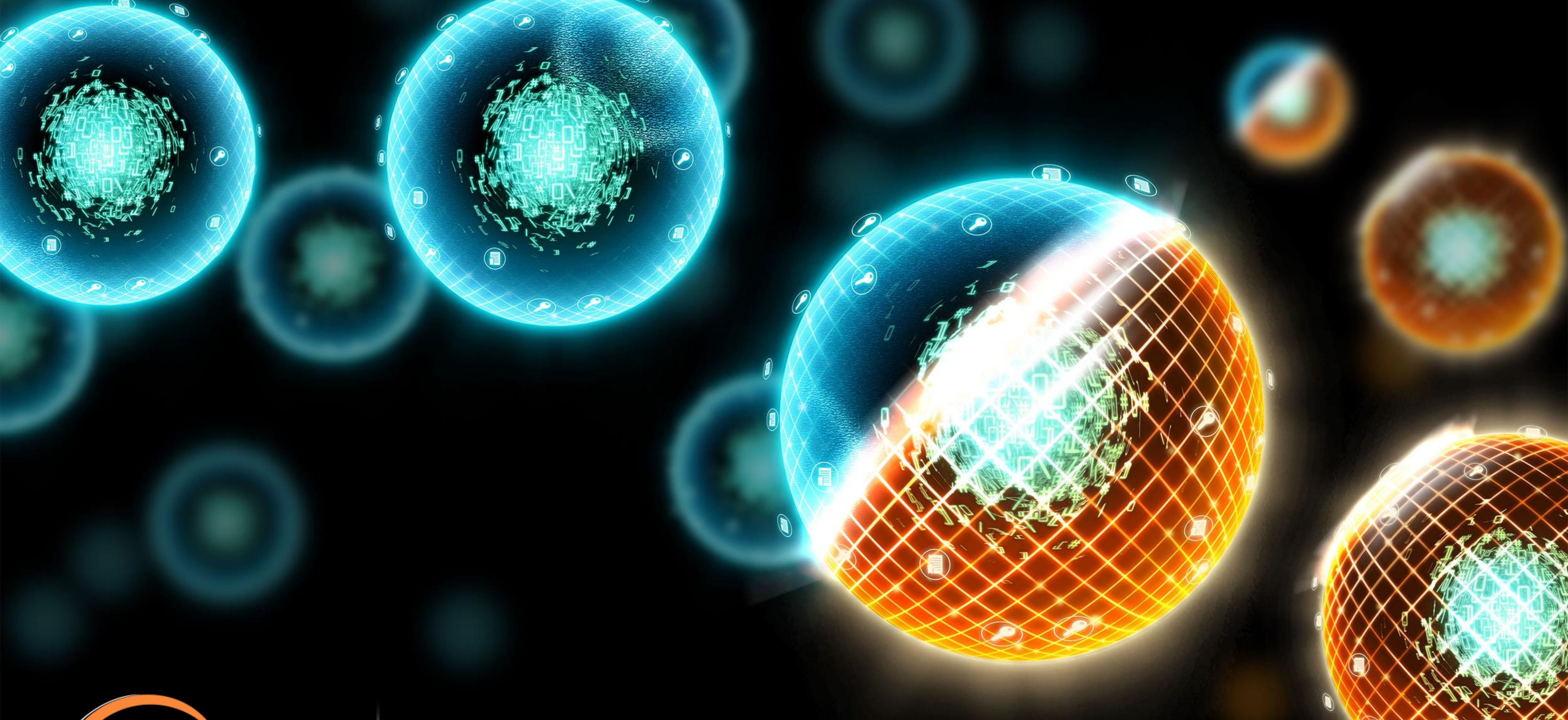
1 Take Action from Alerts and Notifications

3 Install Certs and Rotate Keys on Demand (Physical, Virtual, Cloud)

For all SSL keys/certificates and SSH keys

Lessons from Human Immune System

- Keys and certificates can’t be blindly trusted
- We have to actively inspect, constantly adapt
- Find keys certificates, trusted?, fix, securely distribute and scale



VENAFI™

Find out more at **venafi.com**