ICION 6TH CONFERENCE 2018

Title : Securing the Modern Enterprise with a Modern Approach

Fernando Serto

Head of Security Tech and Strategy, APAC

06th March 2018, Ambarrukmo Yogajakarta, ICION 6TH Conference

Akamai

ICION
Indonesian CIO Network

Cloud infrastructure alone is **not enough**

“slow” is the new “down”

BIGGER ISN’T JUST BETTER — **IT’S A NECESSITY**

ONLY AKAMAI SERVERS ARE EVERYWHERE YOUR USERS ARE, DELIVERING UNMATCHED SPEED AND RELIABILITY

That’s where Akamai comes in.

Akamai is the world’s largest and most trusted cloud delivery platform, making it easier for companies to provide the best and most secure digital experiences today and in the future.

Cloud infrastructure

Optimized for high availability

+

Cloud delivery platform

Optimized for secure, high accessibility

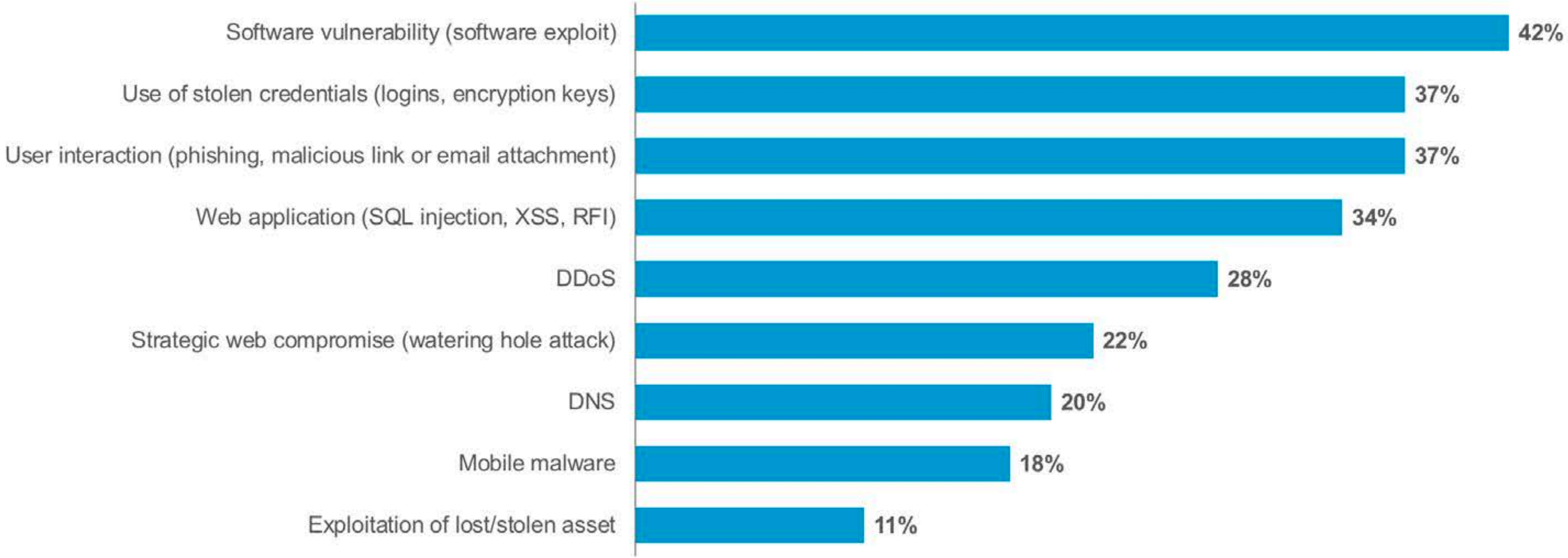
Massive scale is about more than content

Akamai gathers and analyzes huge amounts of ***performance*** and ***security*** data in real time to optimize routing faster than anyone and identify and respond to security threats in real time.

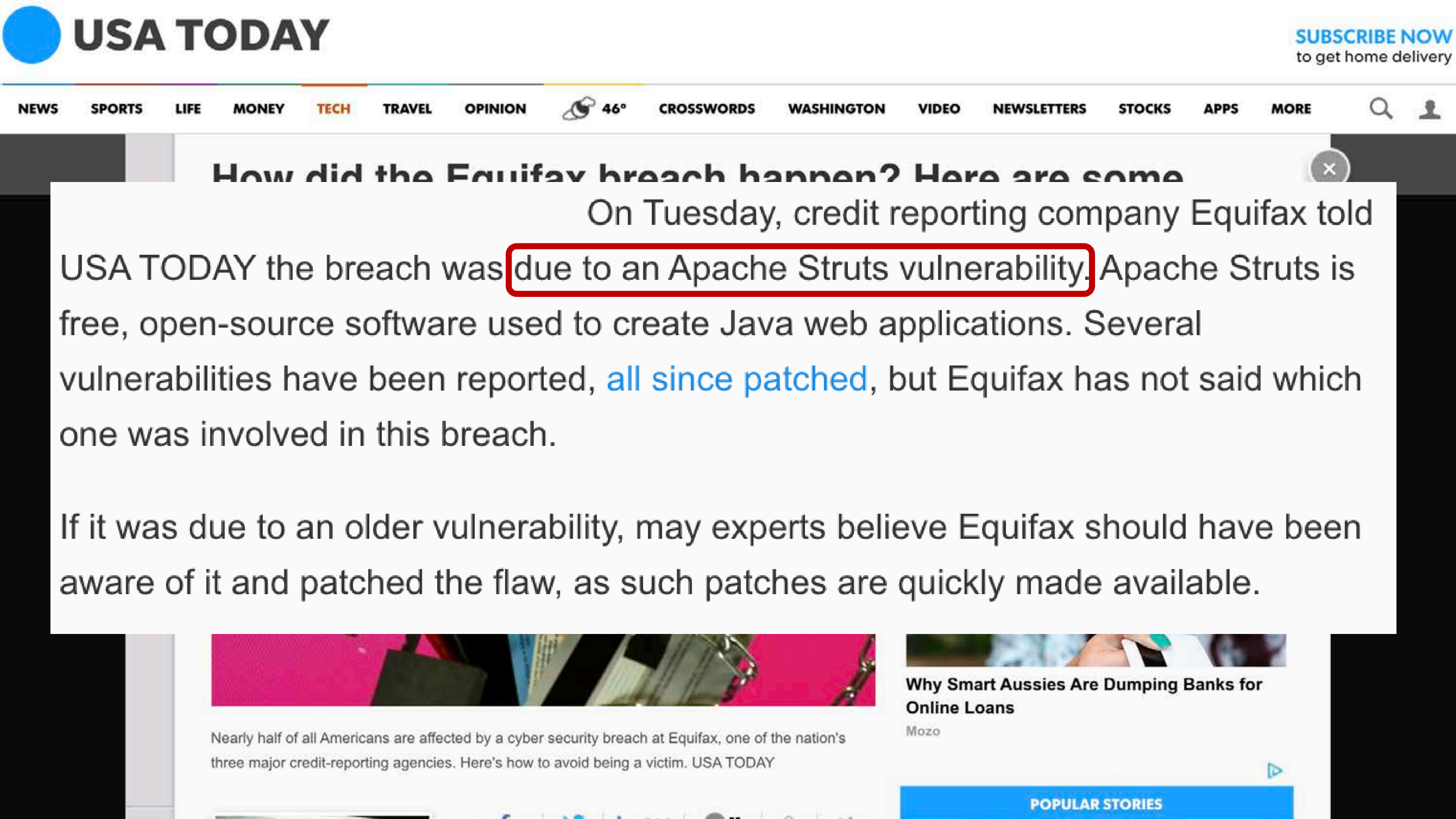
MADE POSSIBLE WITH AKAMAI’S VAST DATA GATHERING AND MACHINE LEARNING

Top external attack vectors

BUSINESS RISK



Source: The State of Network Security: 2016-2017, Forrester, January 2017

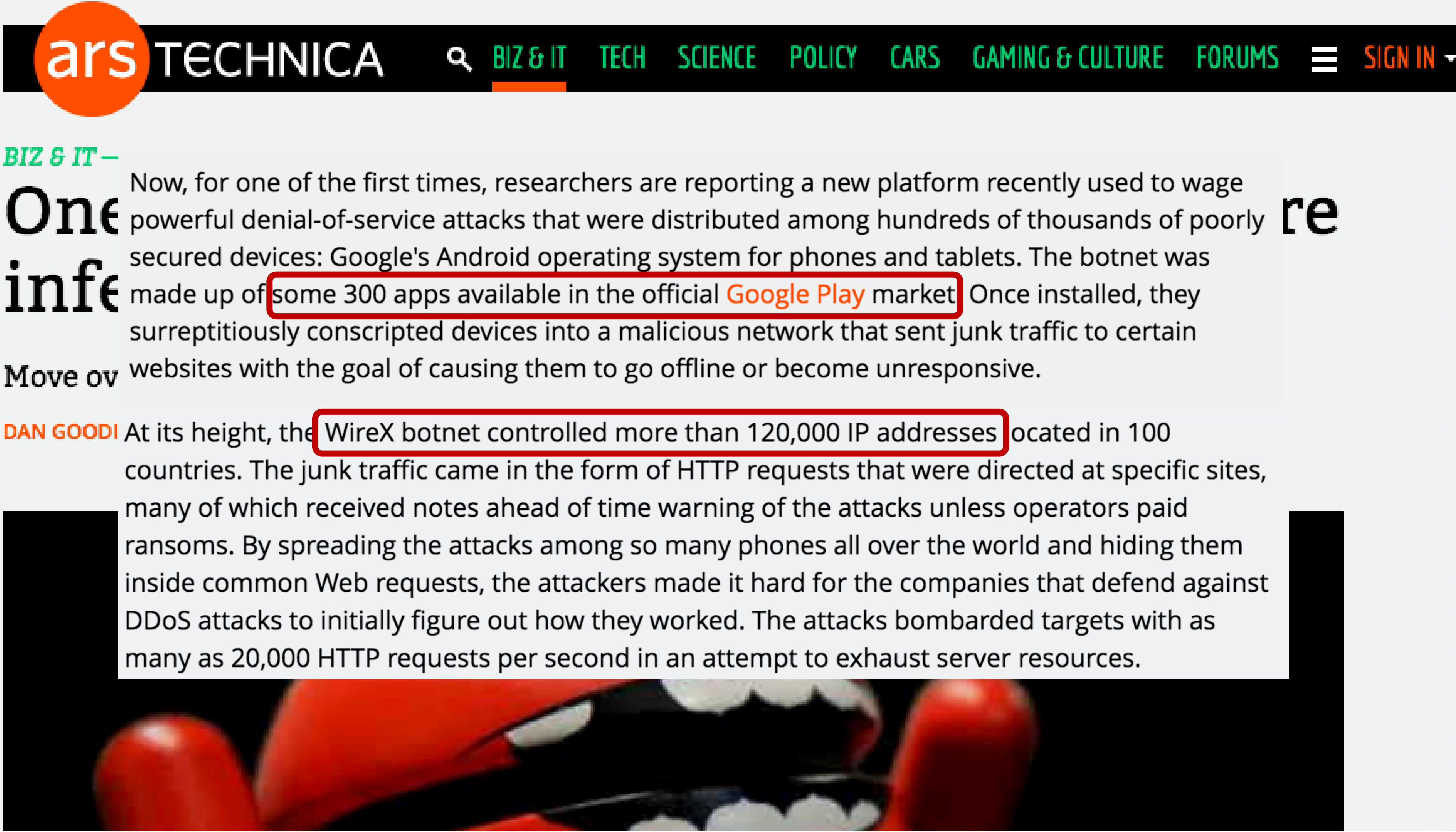


How did the Equifax breach happen? Here are some

On Tuesday, credit reporting company Equifax told USA TODAY the breach was due to an Apache Struts vulnerability. Apache Struts is free, open-source software used to create Java web applications. Several vulnerabilities have been reported, all since patched, but Equifax has not said which one was involved in this breach.

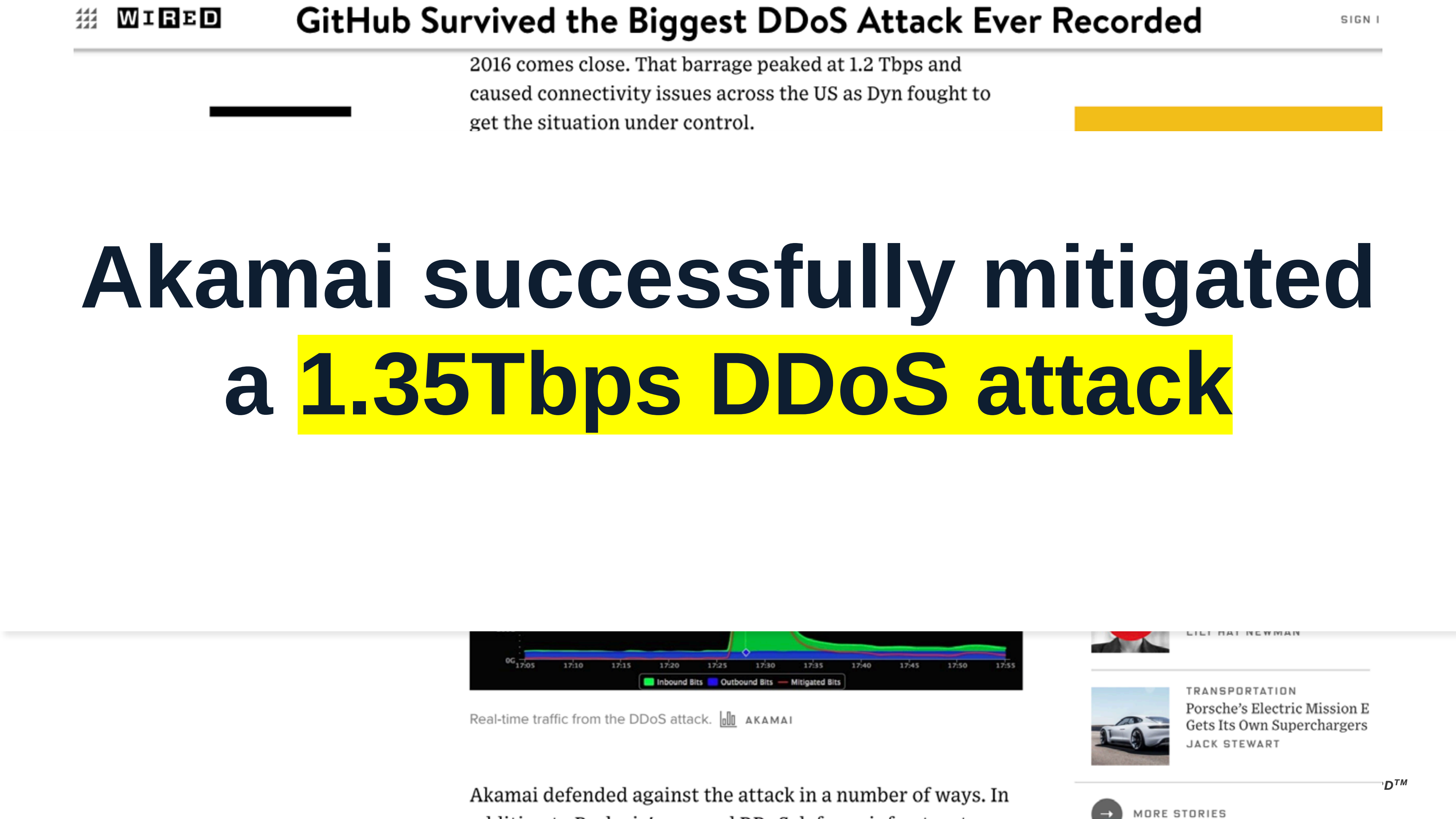
If it was due to an older vulnerability, may experts believe Equifax should have been aware of it and patched the flaw, as such patches are quickly made available.

Nearly half of all Americans are affected by a cyber security breach at Equifax, one of the nation's three major credit-reporting agencies. Here's how to avoid being a victim. USA TODAY



Now, for one of the first times, researchers are reporting a new platform recently used to wage powerful denial-of-service attacks that were distributed among hundreds of thousands of poorly secured devices: Google's Android operating system for phones and tablets. The botnet was made up of some 300 apps available in the official Google Play market. Once installed, they surreptitiously conscripted devices into a malicious network that sent junk traffic to certain websites with the goal of causing them to go offline or become unresponsive.

At its height, the WireX botnet controlled more than 120,000 IP addresses located in 100 countries. The junk traffic came in the form of HTTP requests that were directed at specific sites, many of which received notes ahead of time warning of the attacks unless operators paid ransoms. By spreading the attacks among so many phones all over the world and hiding them inside common Web requests, the attackers made it hard for the companies that defend against DDoS attacks to initially figure out how they worked. The attacks bombarded targets with as many as 20,000 HTTP requests per second in an attempt to exhaust server resources.



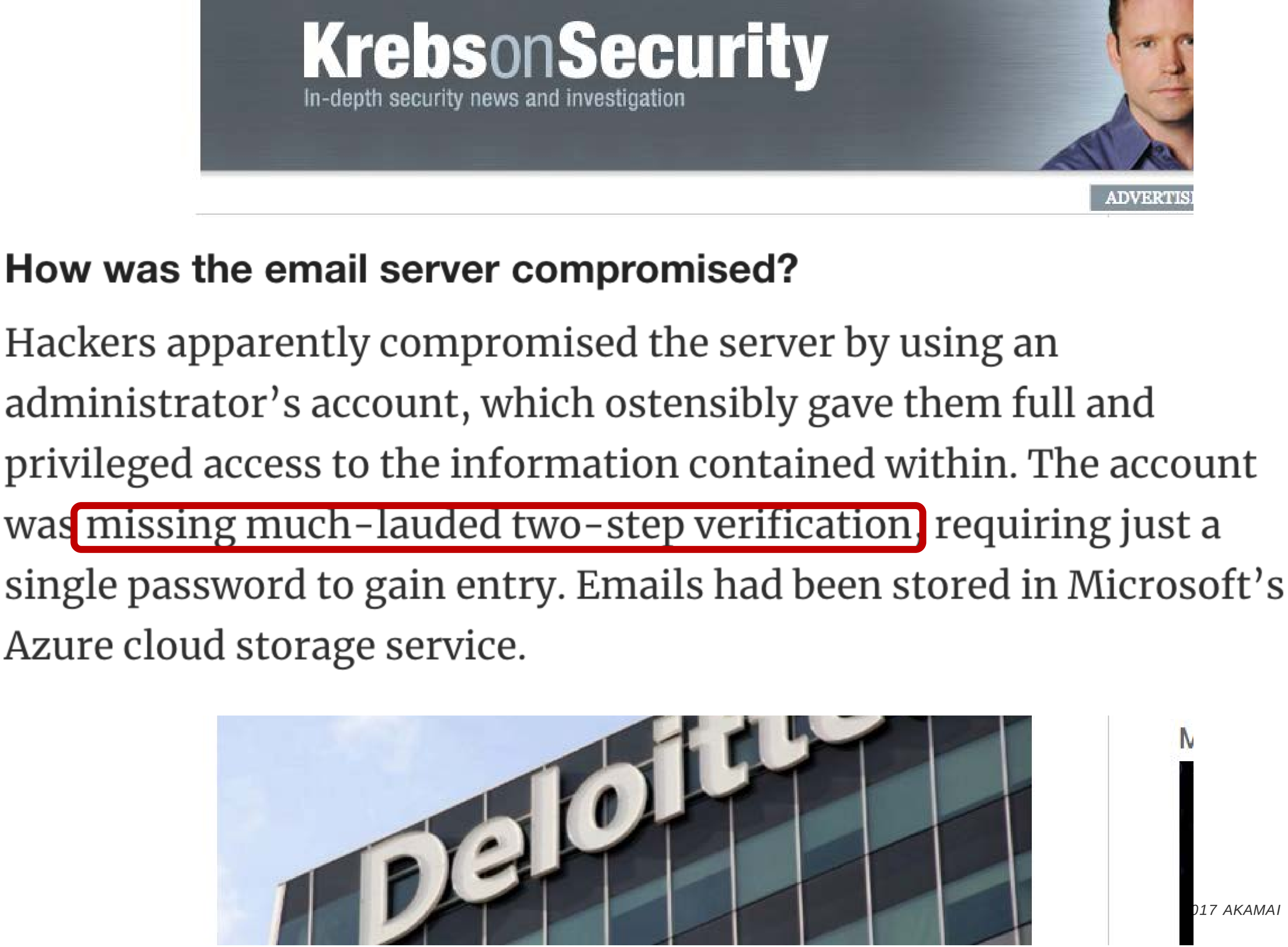
GitHub Survived the Biggest DDoS Attack Ever Recorded

2016 comes close. That barrage peaked at 1.2 Tbps and caused connectivity issues across the US as Dyn fought to get the situation under control.

Akamai successfully mitigated a 1.35Tbps DDoS attack

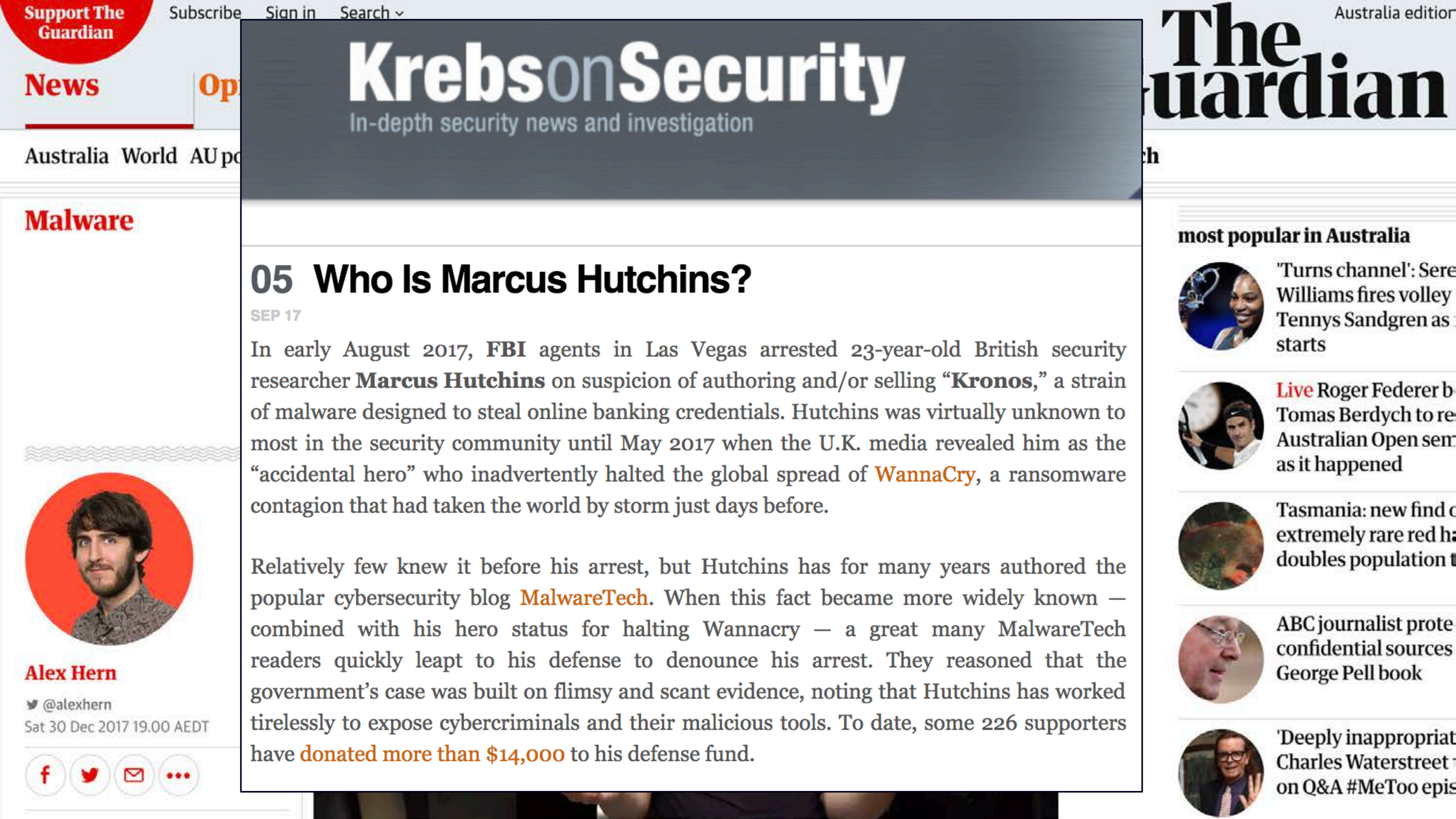
Real-time traffic from the DDoS attack. AKAMAI

Akamai defended against the attack in a number of ways. In



How was the email server compromised?

Hackers apparently compromised the server by using an administrator’s account, which ostensibly gave them full and privileged access to the information contained within. The account was missing much-lauded two-step verification, requiring just a single password to gain entry. Emails had been stored in Microsoft’s Azure cloud storage service.



Support The Guardian

Subscribe Sign in Search

Australia edition

The Guardian

News Opi

Australia World AU po

h

Malware

Alex Hern

@alexhern

Sat 30 Dec 2017 19.00 AEDT

KrebsonSecurity

In-depth security news and investigation

05 Who Is Marcus Hutchins?

SEP 17

In early August 2017, **FBI** agents in Las Vegas arrested 23-year-old British security researcher **Marcus Hutchins** on suspicion of authoring and/or selling "**Kronos**," a strain of malware designed to steal online banking credentials. Hutchins was virtually unknown to most in the security community until May 2017 when the U.K. media revealed him as the "accidental hero" who inadvertently halted the global spread of WannaCry, a ransomware contagion that had taken the world by storm just days before.

Relatively few knew it before his arrest, but Hutchins has for many years authored the popular cybersecurity blog MalwareTech. When this fact became more widely known — combined with his hero status for halting Wannacry — a great many MalwareTech readers quickly leapt to his defense to denounce his arrest. They reasoned that the government's case was built on flimsy and scant evidence, noting that Hutchins has worked tirelessly to expose cybercriminals and their malicious tools. To date, some 226 supporters have donated more than $14,000 to his defense fund.

most popular in Australia

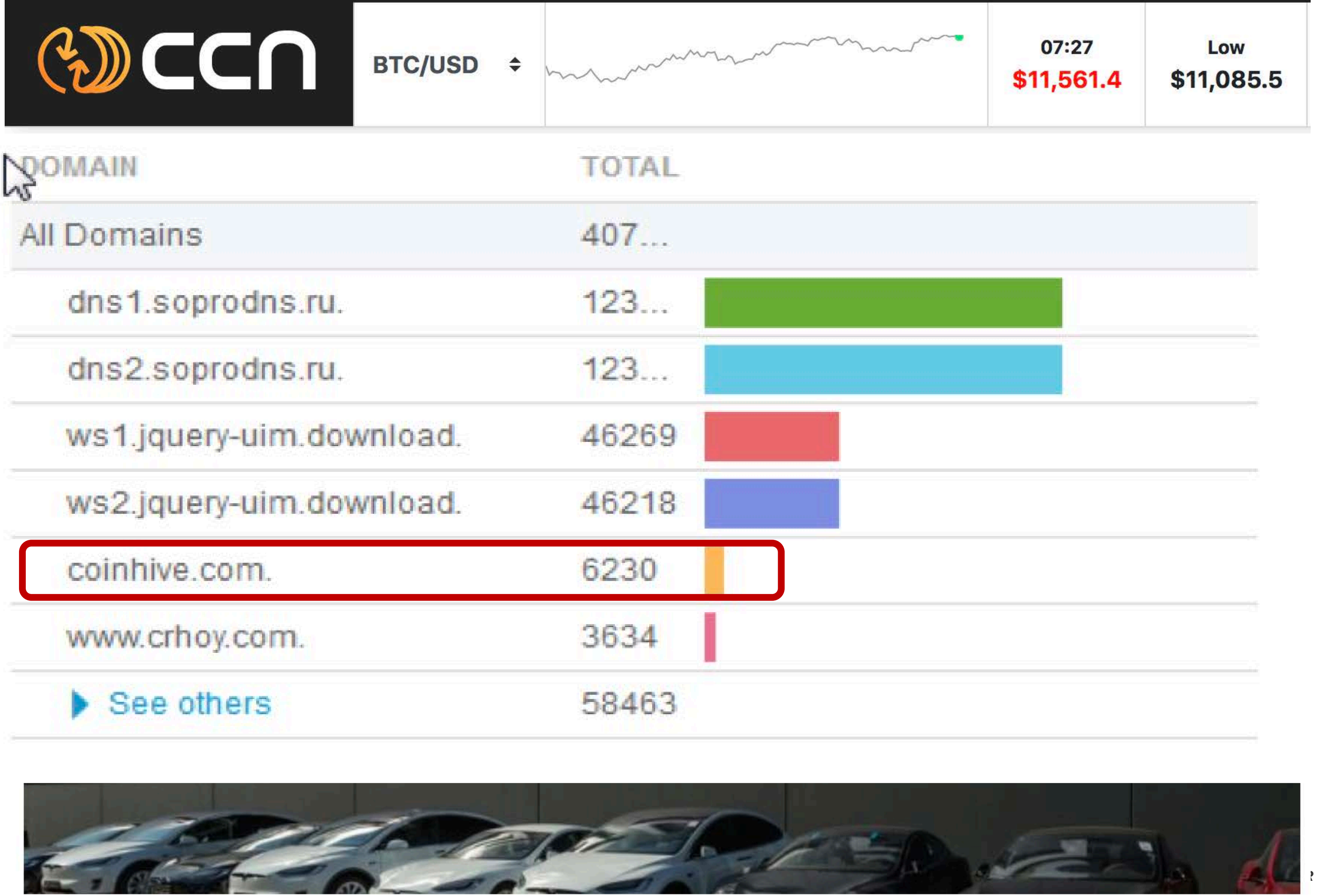
'Turns channel': Sere Williams fires volley Tennys Sandgren as starts

Live Roger Federer b Tomas Berdych to re Australian Open sem as it happened

Tasmania: new find o extremely rare red ha doubles population t

ABC journalist prote confidential sources George Pell book

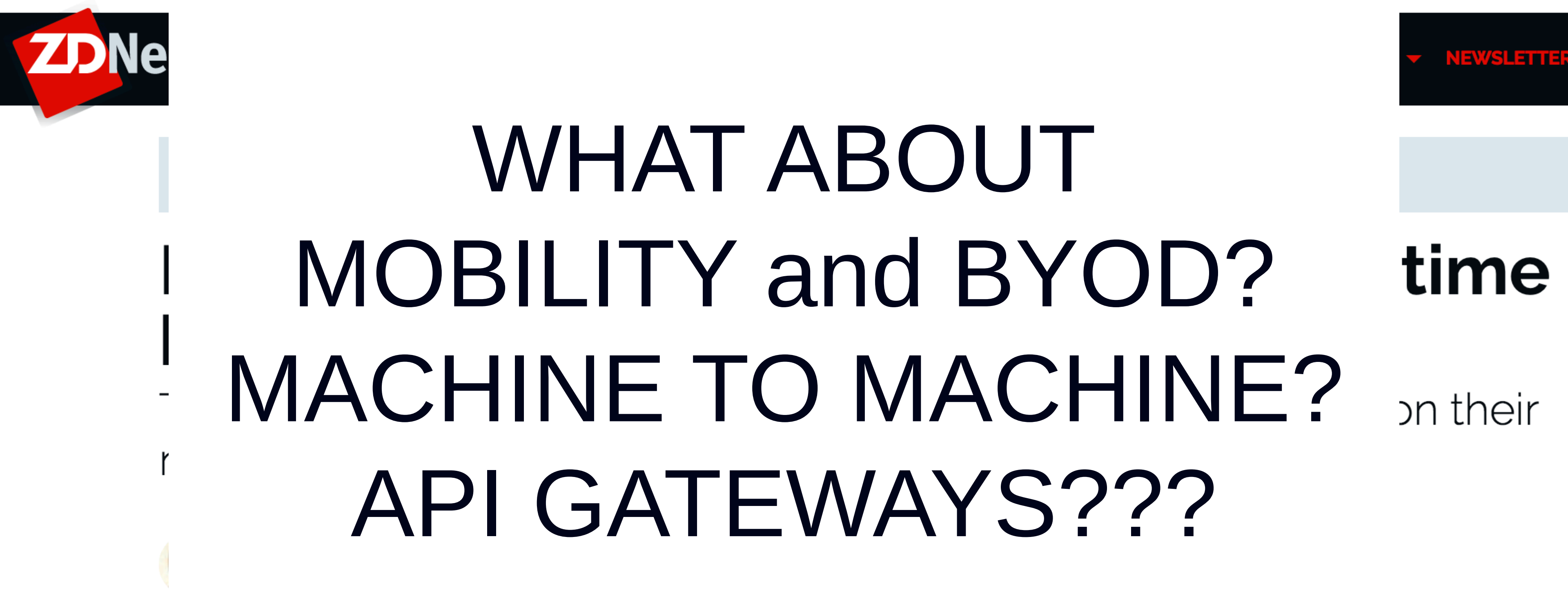
'Deeply inappropriat Charles Waterstreet on Q&A #MeToo epis



07:27
$11,561.4

Low
$11,085.5

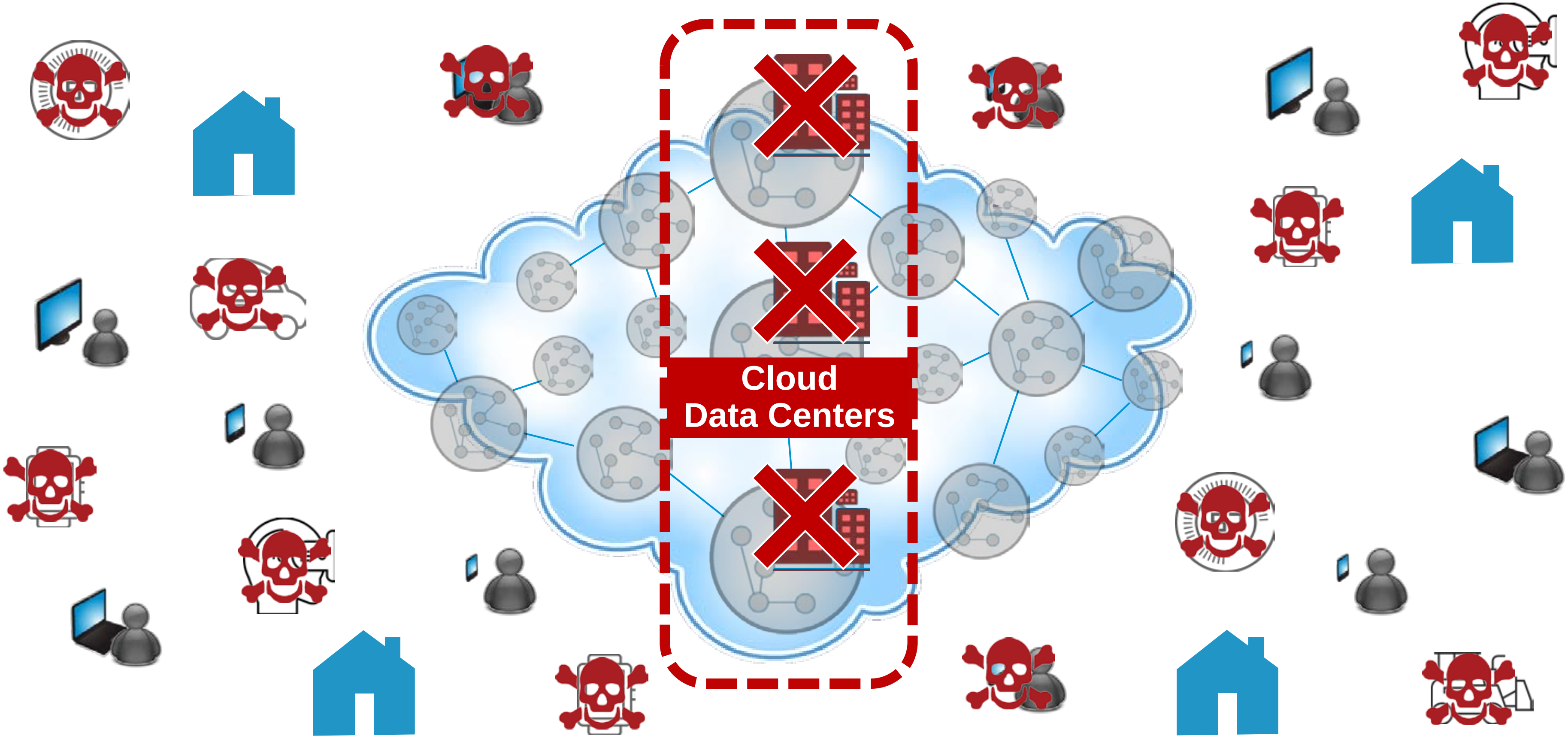
DOMAIN	TOTAL
All Domains	407...
dns1.soprodns.ru.	123...
dns2.soprodns.ru.	123...
ws1.jquery-uim.download.	46269
ws2.jquery-uim.download.	46218
coinhive.com.	6230
www.crhoy.com.	3634
▶ See others	58463



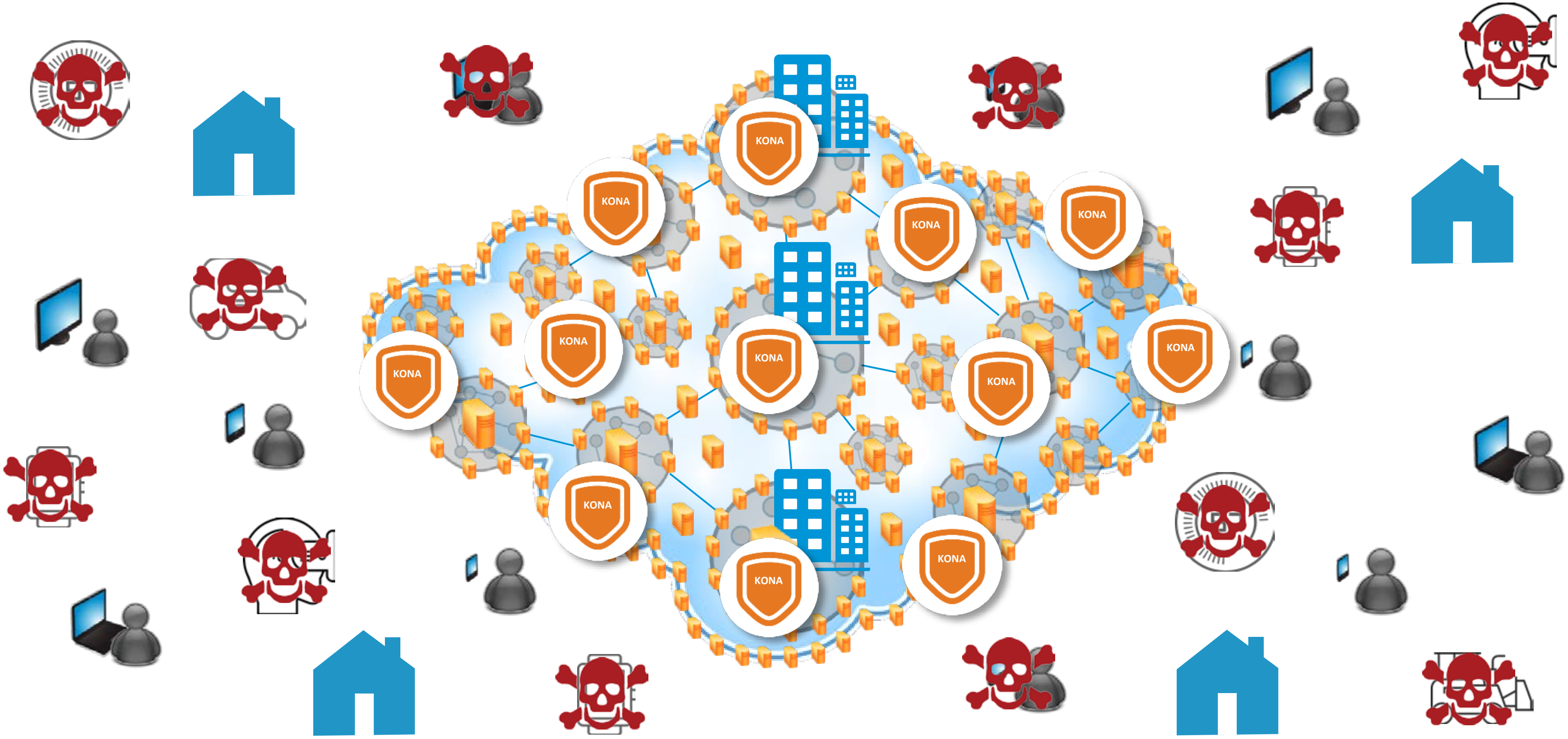
WHAT ABOUT MOBILITY and BYOD? MACHINE TO MACHINE? API GATEWAYS???

Akamai focuses on these areas of Cyber Security,
DNS, **DDoS**, **WAF**, **Bot Mitigation**, **Credential Stuffing/ATO**,
Remote Access and **Malware/Phishing/AUP**

Attackers are exploiting the **72X** imbalance in core capacity (and billions of insecure IoT devices)

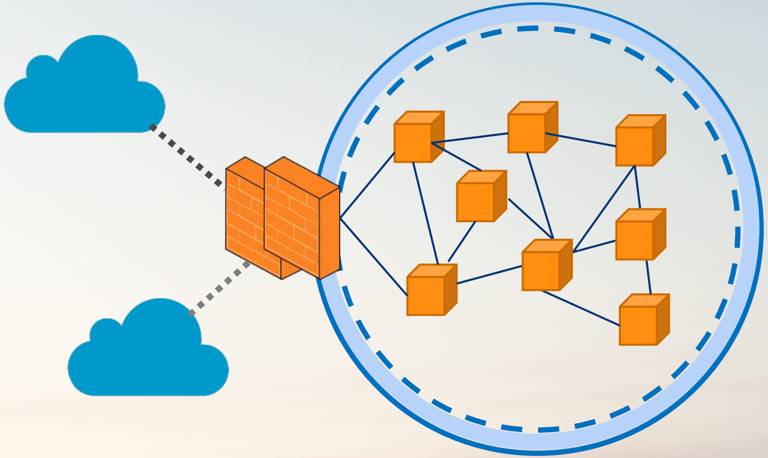


Akamai provides a **defensive shield** to absorb attack traffic… and to block application-layer attacks



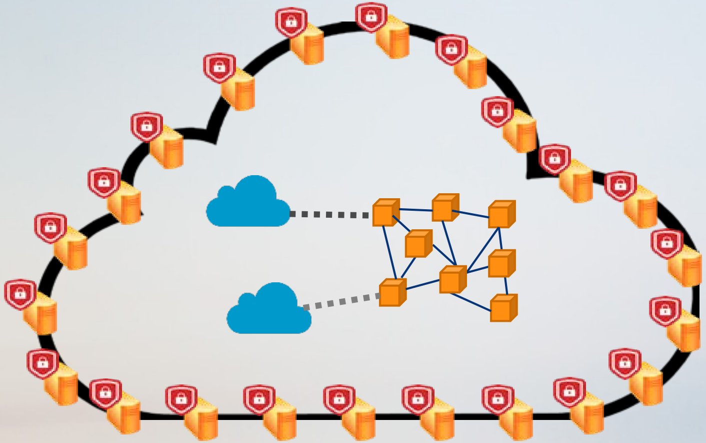
Cloud-native security for a cloud-based world

Traditional “moats and castles” no longer apply; your apps and data and users have moved outside the firewall!



Traditional Perimeter Security

Akamai moves security and policy to the edge of the Internet; providing effortless security for the cloud age

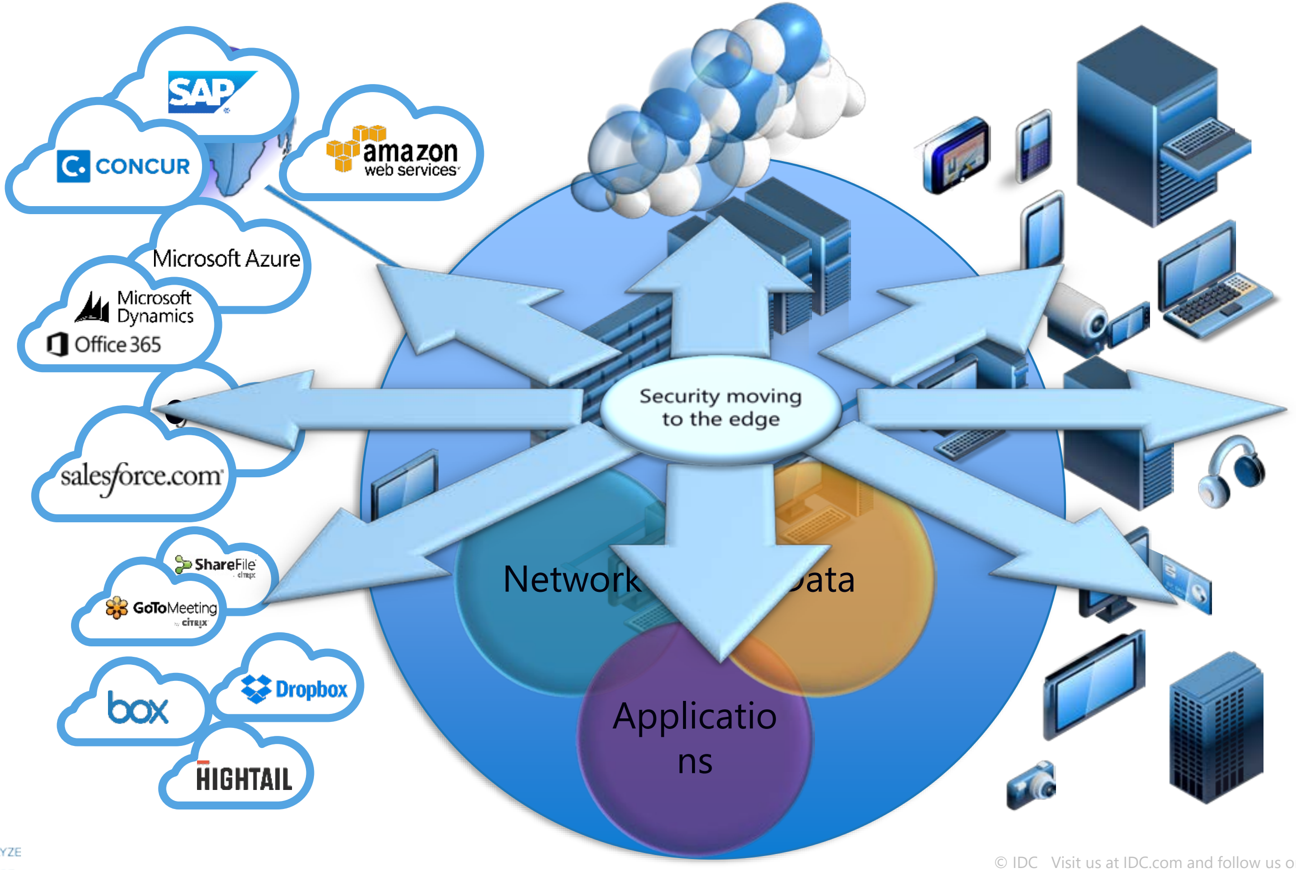


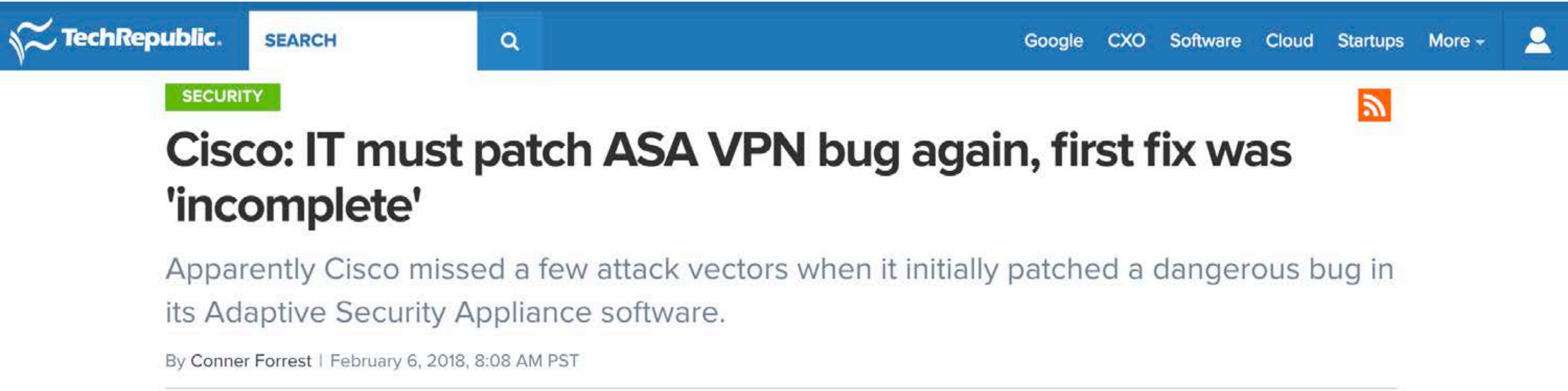
Akamai Cloud Security

DATA CENTER DEFENSES **AREN'T ENOUGH** ANYMORE

ATTACKS ARE BIGGER, MORE SOPHISTICATED,
AND MORE UNPREDICTABLE THAN EVER BEFORE

Old Security Platform in a Modern World?



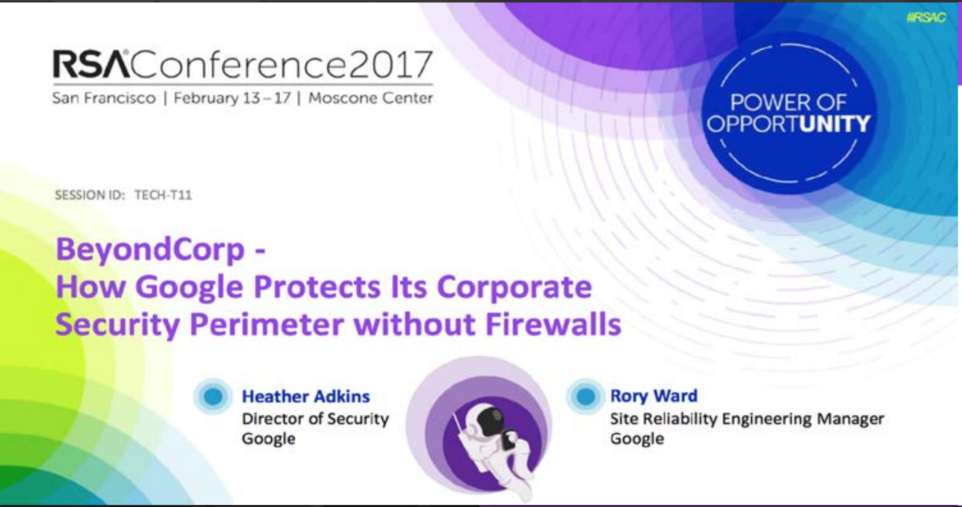


Cisco: IT must patch ASA VPN bug again, first fix was 'incomplete'

Apparently Cisco missed a few attack vectors when it initially patched a dangerous bug in its Adaptive Security Appliance software.

By Conner Forrest | February 6, 2018, 8:08 AM PST

Google BeyondCorp



#RSAC

RSAConference2017

San Francisco | February 13 – 17 | Moscone Center

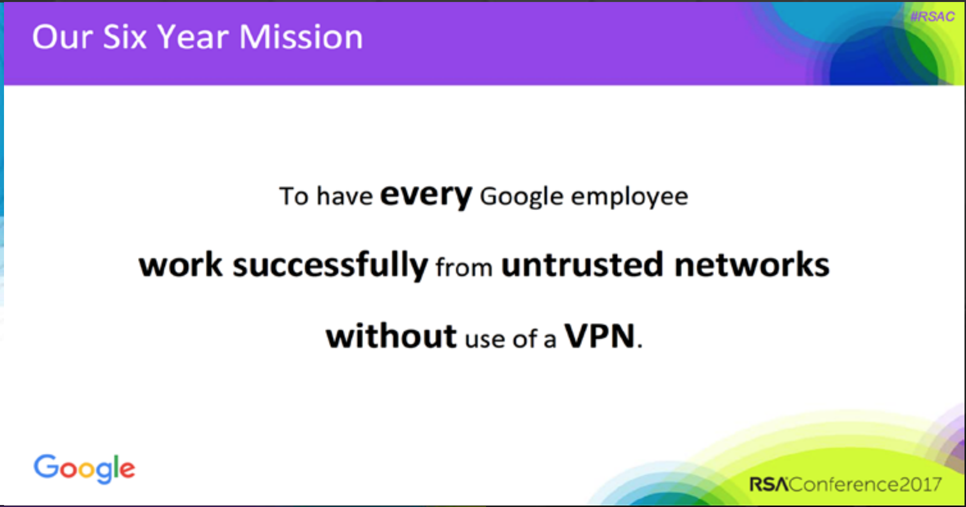
POWER OF OPPORTUNITY

SESSION ID: TECH-T11

BeyondCorp - How Google Protects Its Corporate Security Perimeter without Firewalls

Heather Adkins
Director of Security
Google

Rory Ward
Site Reliability Engineering Manager
Google



#RSAC

Our Six Year Mission

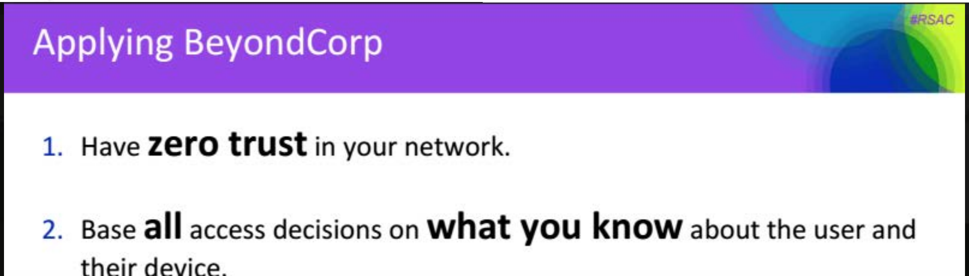
To have **every** Google employee

work successfully from **untrusted networks**

without use of a **VPN**.

Google

RSAConference2017



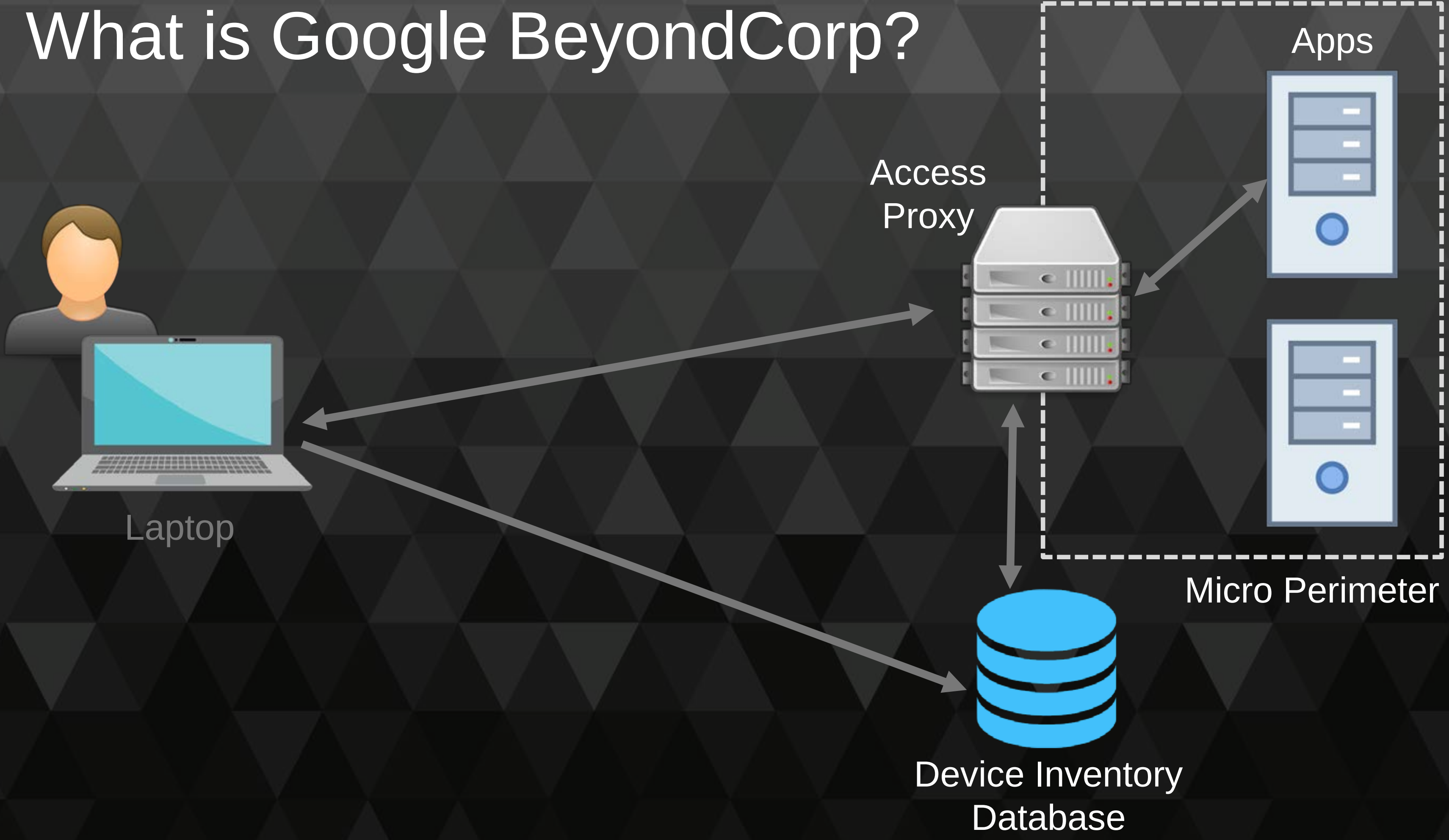
#RSAC

Applying BeyondCorp

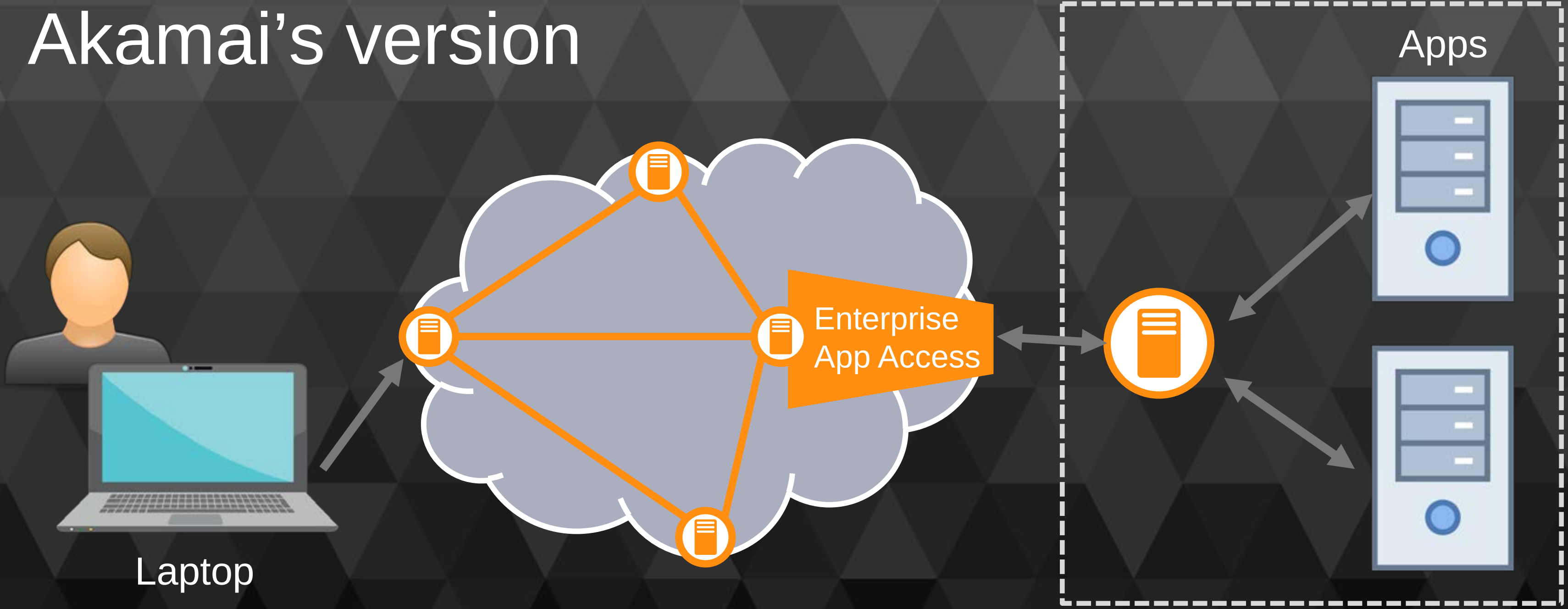
1. Have **zero trust** in your network.
2. Base **all** access decisions on **what you know** about the user and their device.

#ZeroTrust

What is Google BeyondCorp?



Akamai’s version



Micro Perimeter

Simpler, **Secure Access** to Enterprise Apps

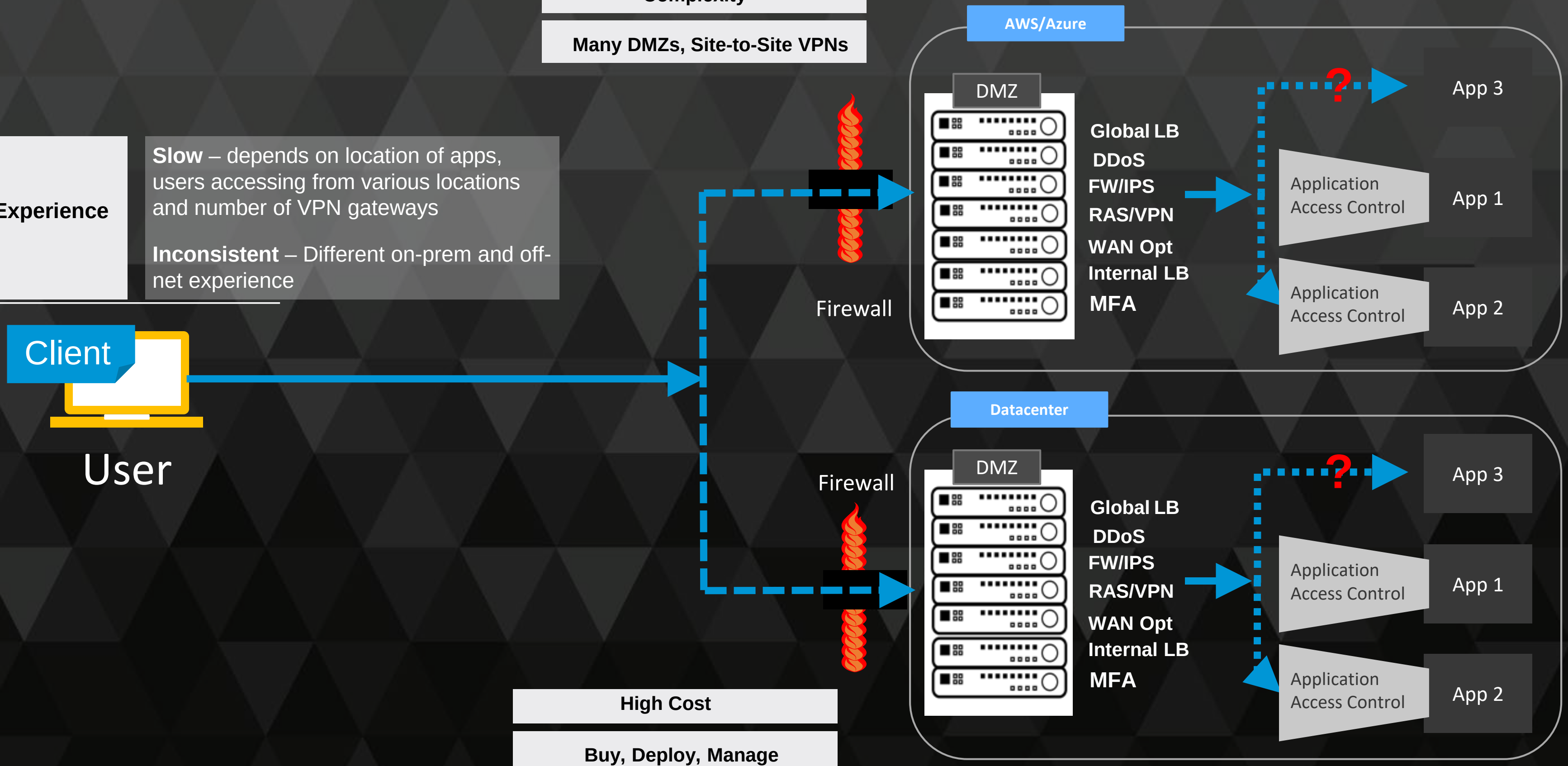
Complexity

Many DMZs, Site-to-Site VPNs

User Experience

Slow – depends on location of apps, users accessing from various locations and number of VPN gateways

Inconsistent – Different on-prem and off-net experience



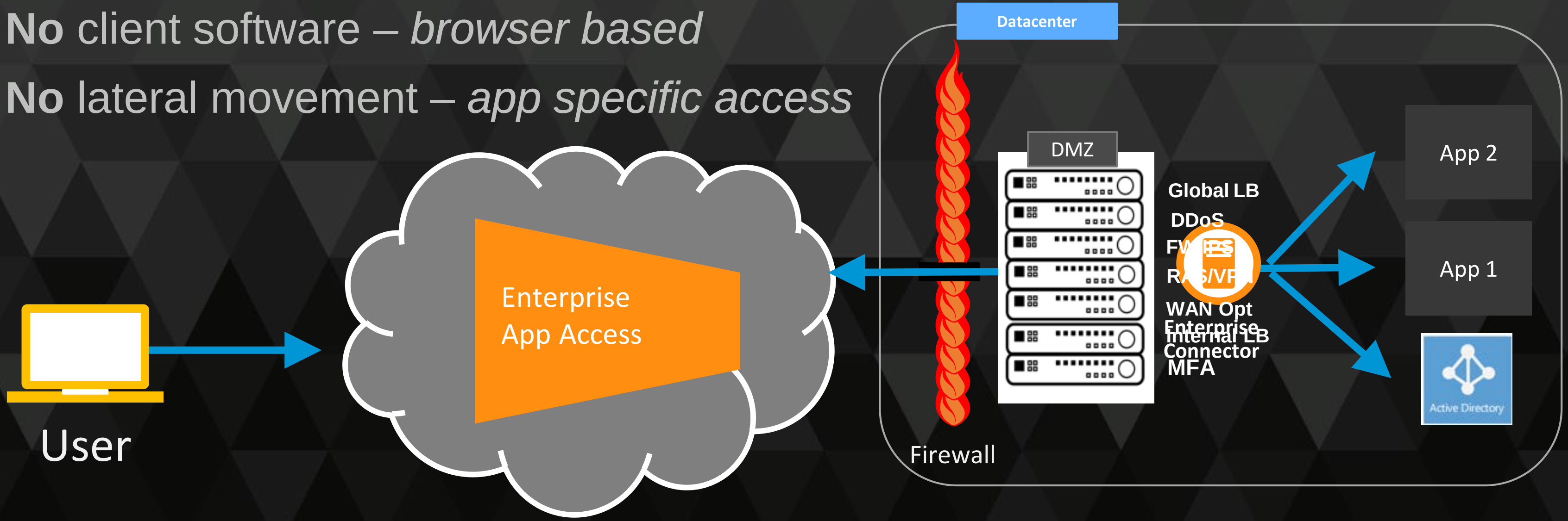
High Cost

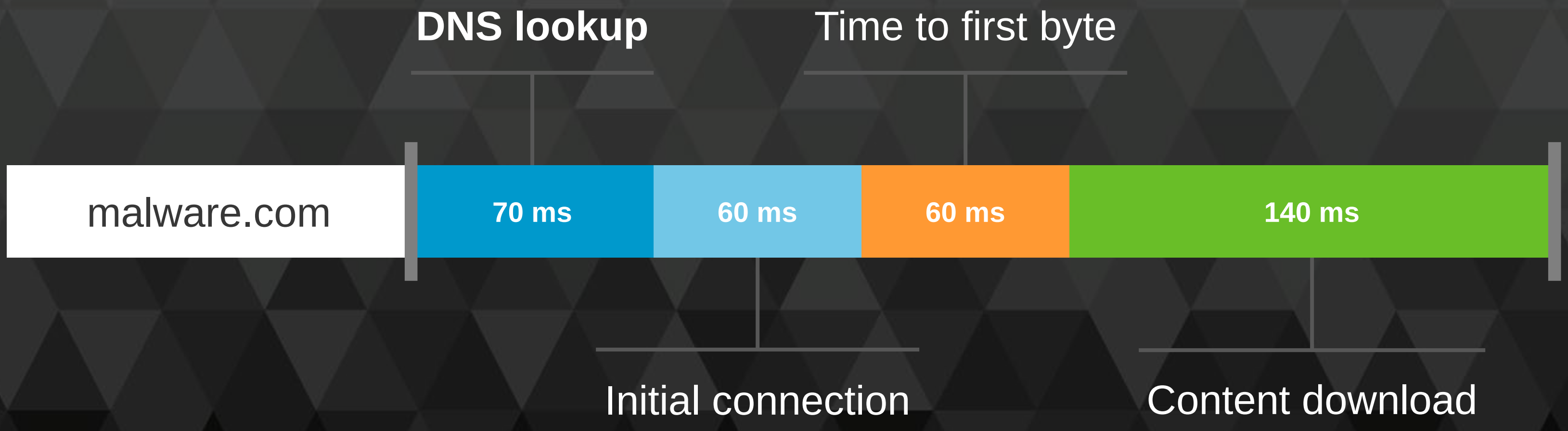
Buy, Deploy, Manage

Simpler, **Secure Access** to Enterprise Apps

Access and security controls move from static on-premise to the cloud

- > **No** hole in the firewall – *outbound only*
- > **No** complex configuration – *cloud managed*
- > **No** client software – *browser based*
- > **No** lateral movement – *app specific access*





DNS lookup

Time to first byte

malware.com

70 ms

60 ms

60 ms

140 ms

Initial connection

Content download

91.3% of known bad malware uses DNS

DNS – The New Signal

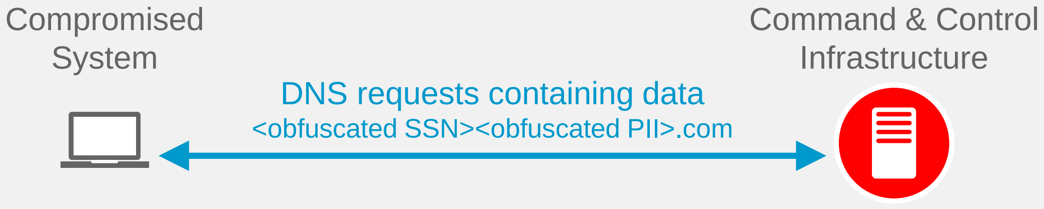
Limited Visibility

Enterprise **A**

Enterprise **B**

VS

DNS Exfiltration



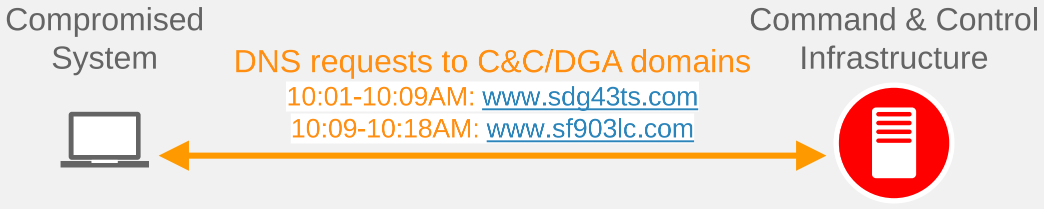
Compromised System

Command & Control Infrastructure

DNS requests containing data

<obfuscated SSN><obfuscated PII>.com

Blacklist Evasion



Compromised System

Command & Control Infrastructure

DNS requests to C&C/DGA domains

10:01-10:09AM: www.sdg43ts.com

10:09-10:18AM: www.sf903lc.com

TRENDS

Apps Moving Outside

User Diversity

Malware Evolving

CHALLENGES

Network Trust & Malware

Complexity & IT Resources

Poor User Experience

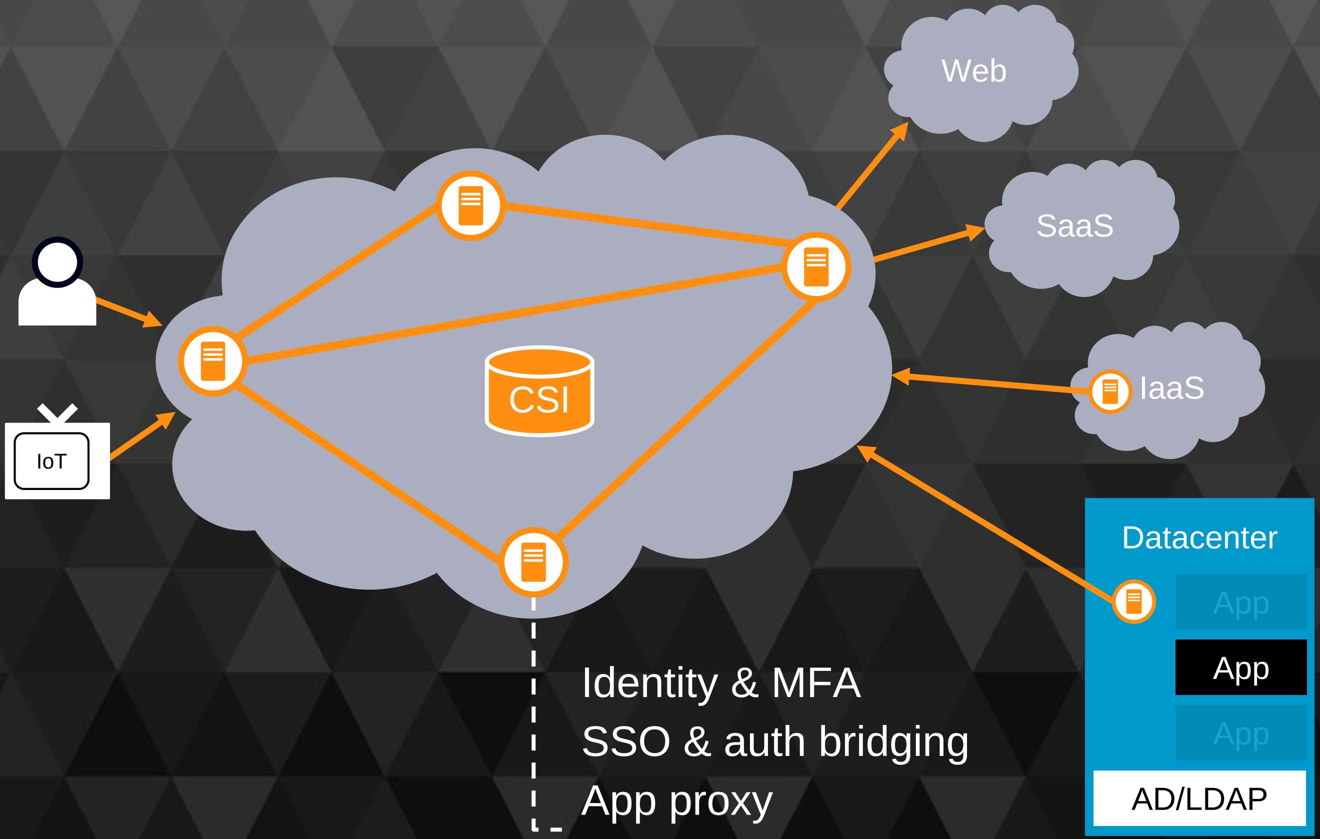
BENEFITS

Zero Trust Architecture

Simple & Flexible

Improved User Experience

Visibility & Auditing



Identity & MFA

SSO & auth bridging

App proxy

Performance acceleration

App security (WAF)

Malware & threat protection

Zero Trust - Where To Get Started

3rd Parties

Simplify and lock down 3rd party access

Employees

Remote developers, field employees, BYOD, M&A, etc.

Applications

Performance sensitive apps, public cloud apps, etc.

Malware Protection

Simple, proactive malware protection on & off net

Zero Trust Assessment & Phasing Guide

Fernando Serto
Head of Security Technology and Strategy, Asia Pacific

With the challenges associated with a modern enterprise environment, companies are now facing multiple challenges, from performance problems with users spread around large geographies to the threat of modern security threats, such as targeted phishing and malware campaigns.

Akamai has been working with our customers on how to adapt to such challenges and provide a secure approach to protect users and infrastructure from modern threats. From Web Security services to a complete ZeroTrust approach.

- Increasing importance of API security
- Protecting your business from malicious bots and credential stuffing
- Adopting a cloud perimeter and taking a ‘verify and never trust’ approach”

ICION
Indonesian CIO Network

Thank You, see you in ICION 2019

- Support our effort to build a Safer Cyber Security World in Indonesia. Our official CISSP classes scheduled for April 23th to 27th 2018

(ISC)² OFFICIAL TRAINING PROVIDER

- Contact to Vannie via +62 877 7567 8589
- Join us in our Linkedin Group ICION as below
- https://www.linkedin.com/groups/3942786

ICION
Indonesian CIO Network

Call to Vannie at +62 877 7567 8589

SHAPING AND SECURING
THE DIGITAL ECONOMY IN INDONESIA
INDONESIAN CIO NETWORK 6TH CONFERENCE

ICION
Indonesian CIO Network

SOC and SIEM – THREE DAYS IN may

- Cyber Security Class on the 2rd,3rd and 4th of May three days with last day on SIEM best practices and lab

- Ping to us via +62 818 102085 , a ICION PRODUCTION
- Trainer Kirby Chong