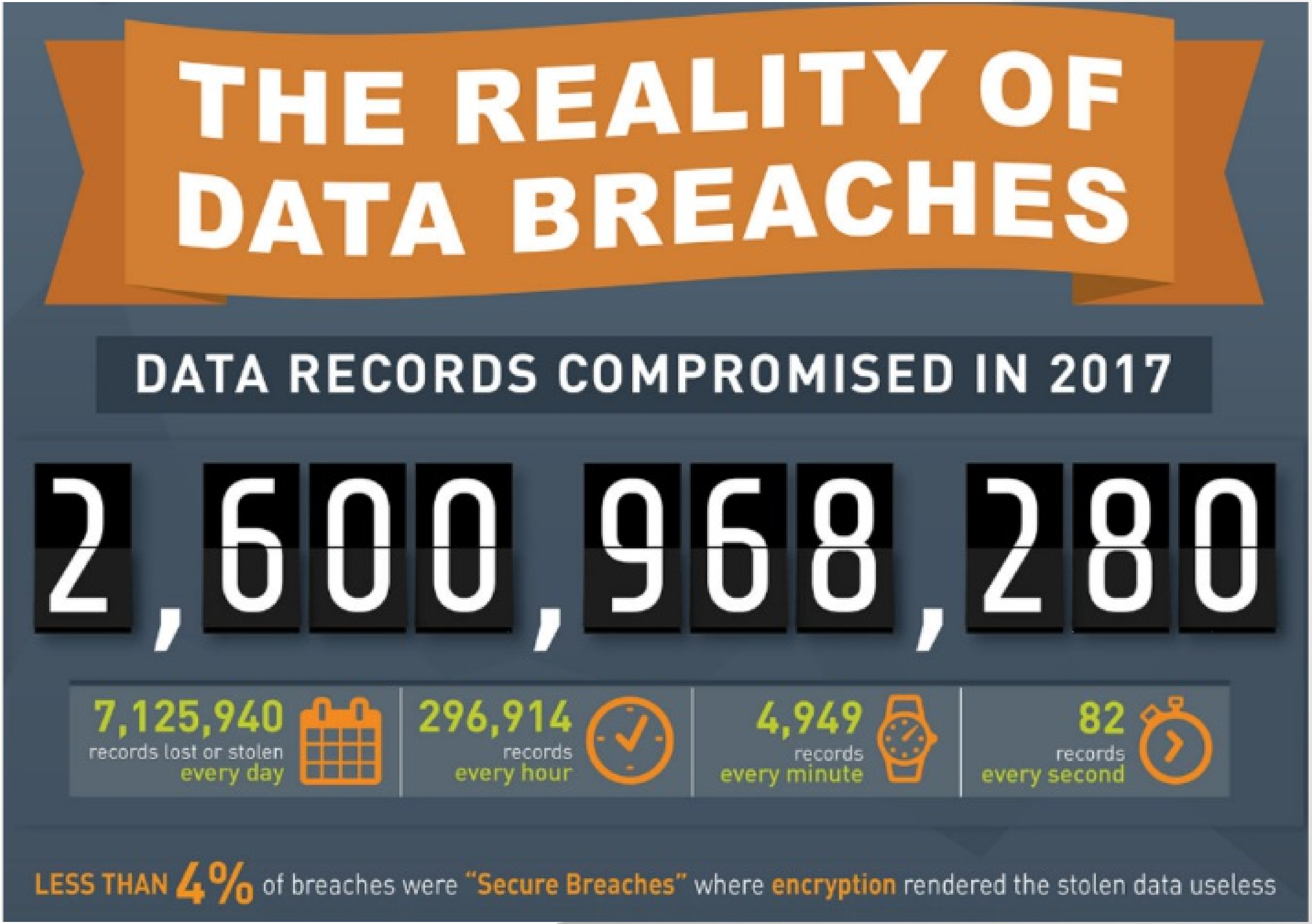
Cyber-Angriffe durch Vermeidung von Netzwerk-Schwachstellen eindämmen

Romanus Raymond Prabhu
Head - Global Technical Support

Automating
Patch Management



THE REALITY OF DATA BREACHES

DATA RECORDS COMPROMISED IN 2017

2,600,968,280

7,125,940 records lost or stolen every day

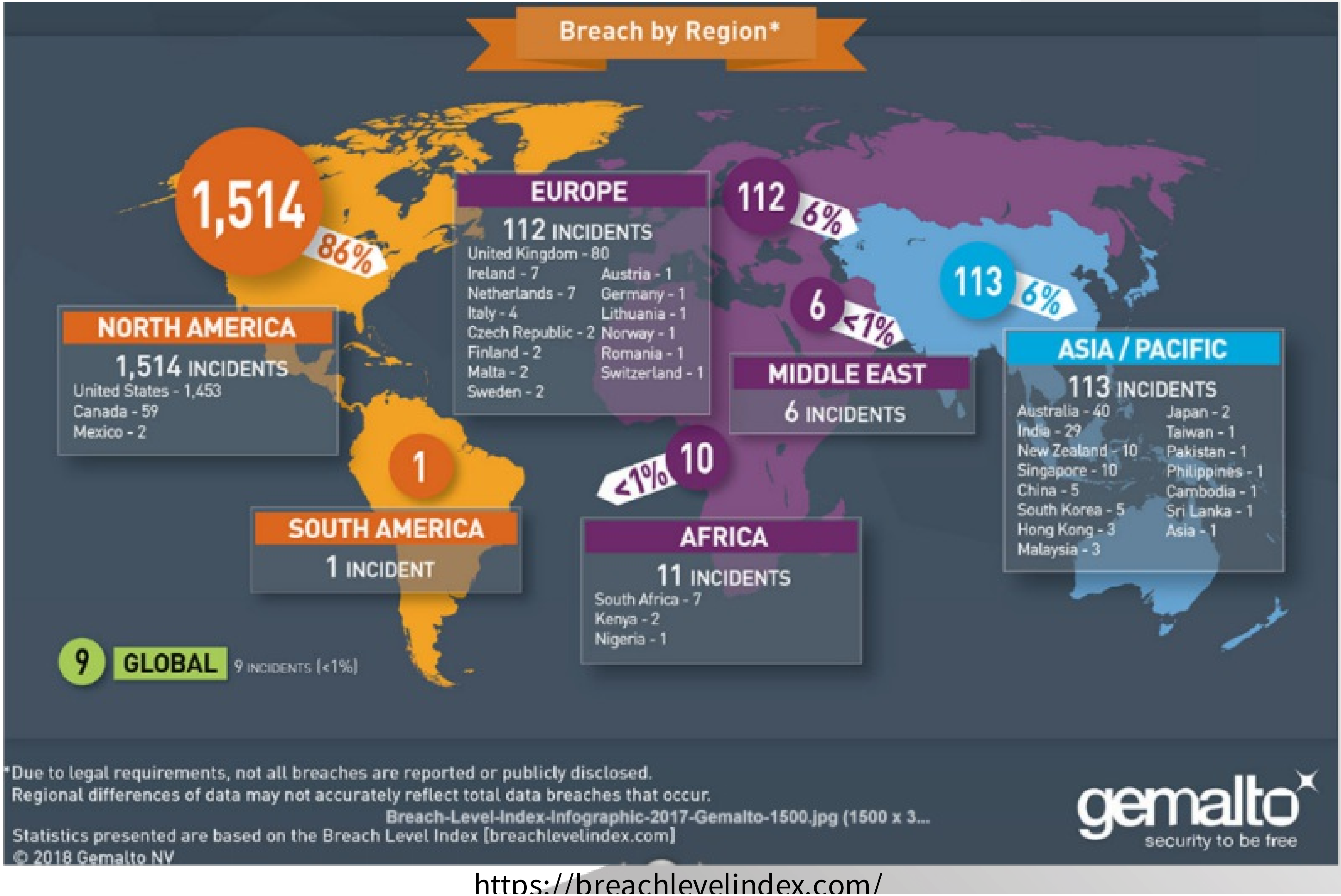
296,914 records every hour

4,949 records every minute

82 records every second

LESS THAN 4% of breaches were "Secure Breaches" where encryption rendered the stolen data useless

https://breachlevelindex.com/



Breach by Region*

NORTH AMERICA

1,514 INCIDENTS

United States	1,453
Canada	59
Mexico	2

EUROPE

112 INCIDENTS

United Kingdom	80
Ireland	7
Netherlands	7
Italy	4
Czech Republic	2
Finland	2
Malta	2
Sweden	2
Austria	1
Germany	1
Lithuania	1
Norway	1
Romania	1
Switzerland	1

MIDDLE EAST

6 INCIDENTS

ASIA / PACIFIC

113 INCIDENTS

Australia	40
India	29
New Zealand	10
Singapore	10
China	5
South Korea	5
Hong Kong	3
Malaysia	3
Japan	2
Taiwan	1
Pakistan	1
Philippines	1
Cambodia	1
Sri Lanka	1
Asia	1

SOUTH AMERICA

1 INCIDENT

AFRICA

11 INCIDENTS

South Africa	7
Kenya	2
Nigeria	1

9 GLOBAL 9 INCIDENTS (<1%)

*Due to legal requirements, not all breaches are reported or publicly disclosed.
Regional differences of data may not accurately reflect total data breaches that occur.

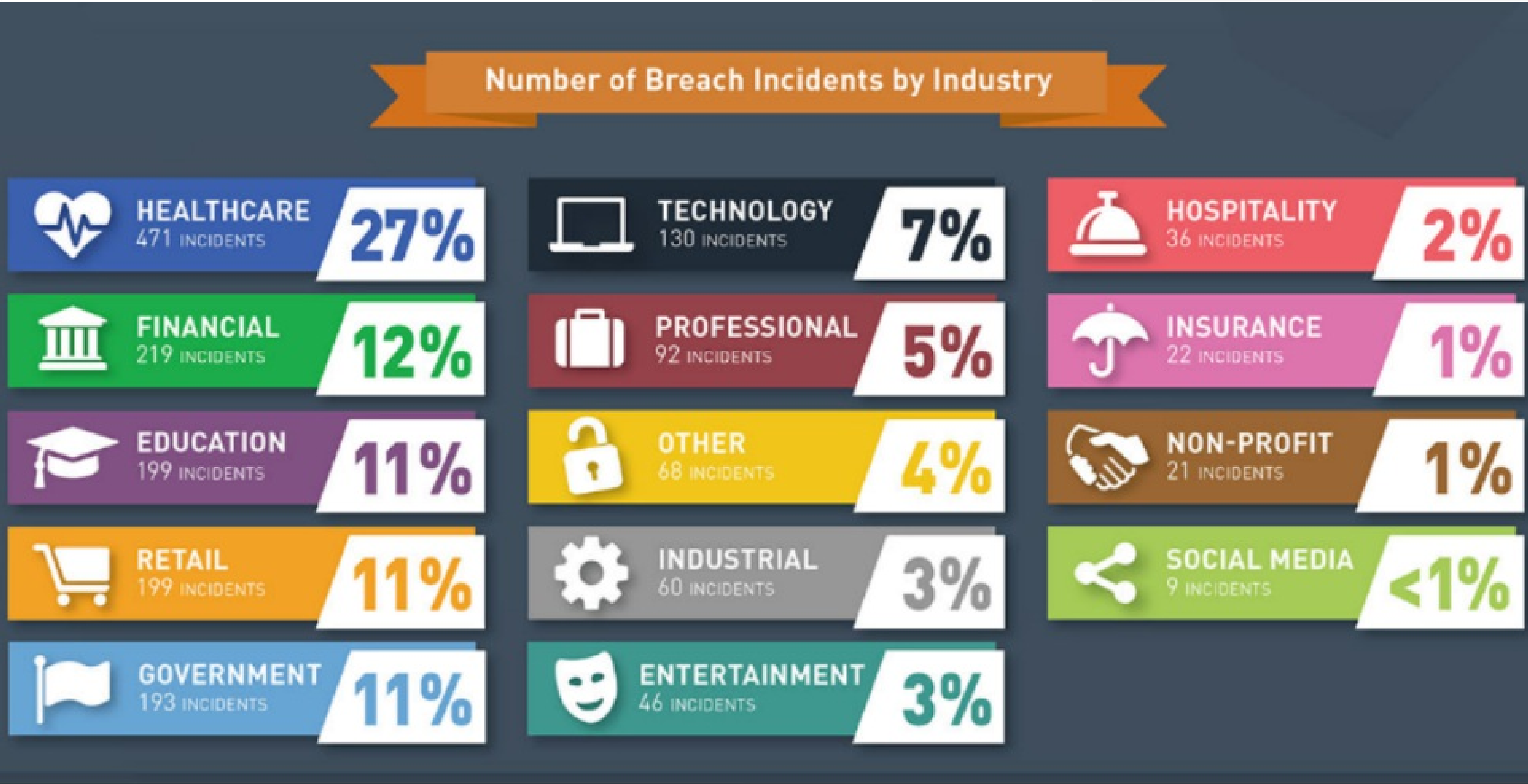
Breach-Level-Index-Infographic-2017-Gemalto-1500.jpg (1500 x 3...

Statistics presented are based on the Breach Level Index [breachlevelindex.com]

© 2018 Gemalto NV

gemalto security to be free

https://breachlevelindex.com/



Number of Breach Incidents by Industry

HEALTHCARE	471 INCIDENTS	27%
FINANCIAL	219 INCIDENTS	12%
EDUCATION	199 INCIDENTS	11%
RETAIL	199 INCIDENTS	11%
GOVERNMENT	193 INCIDENTS	11%
TECHNOLOGY	130 INCIDENTS	7%
PROFESSIONAL	92 INCIDENTS	5%
OTHER	68 INCIDENTS	4%
INDUSTRIAL	60 INCIDENTS	3%
ENTERTAINMENT	46 INCIDENTS	3%
HOSPITALITY	36 INCIDENTS	2%
INSURANCE	22 INCIDENTS	1%
NON-PROFIT	21 INCIDENTS	1%
SOCIAL MEDIA	9 INCIDENTS	<1%

https://breachlevelindex.com/

“Over 4,000 ransomware attacks occur every day”

Source: Computer Crime and Intellectual Property Section (CCIPS)

Meltdown

Spectre

Fireball

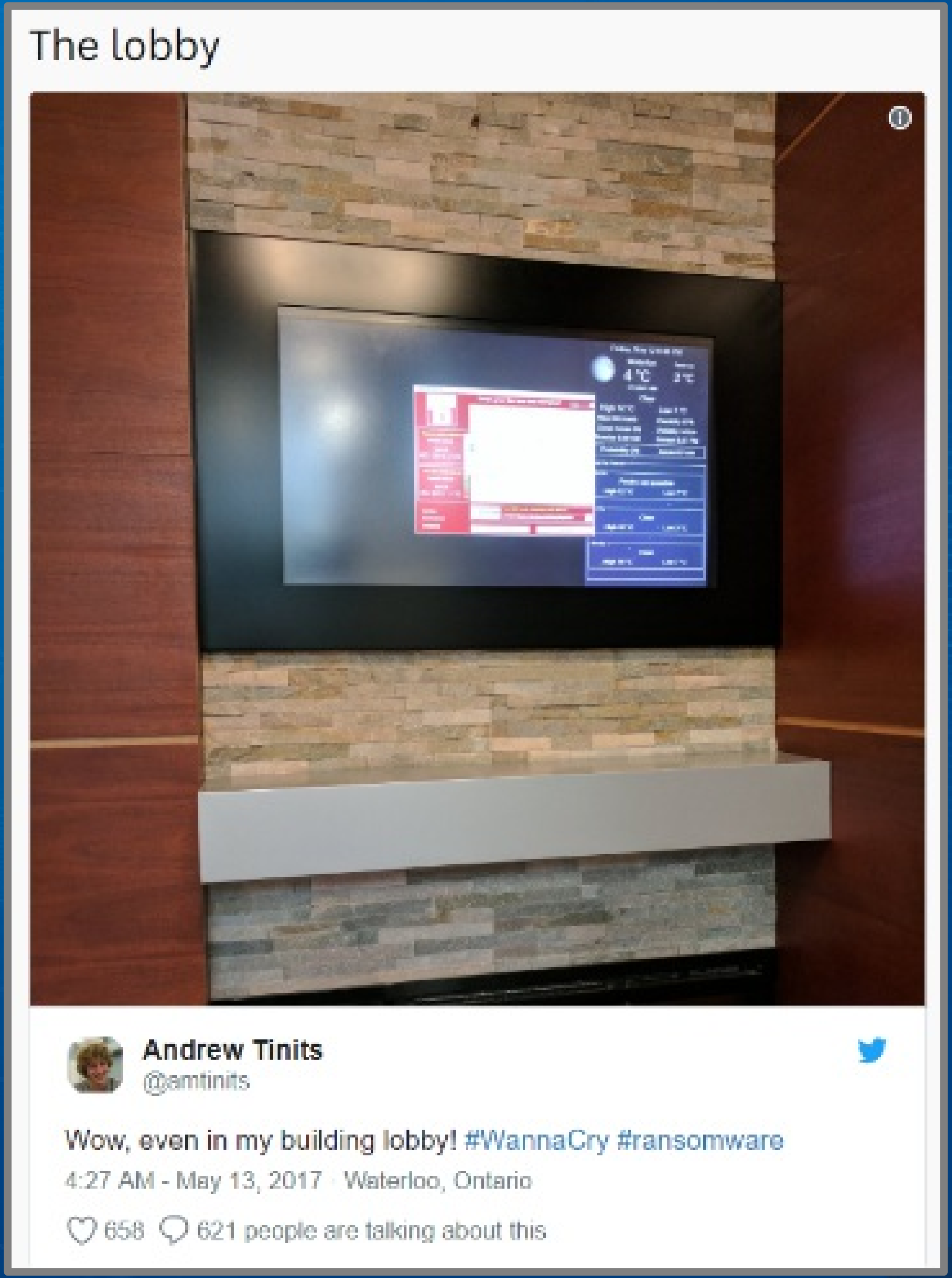
Adylkuzz

Petya

Sambacry

Wannacry

Delta Charlie



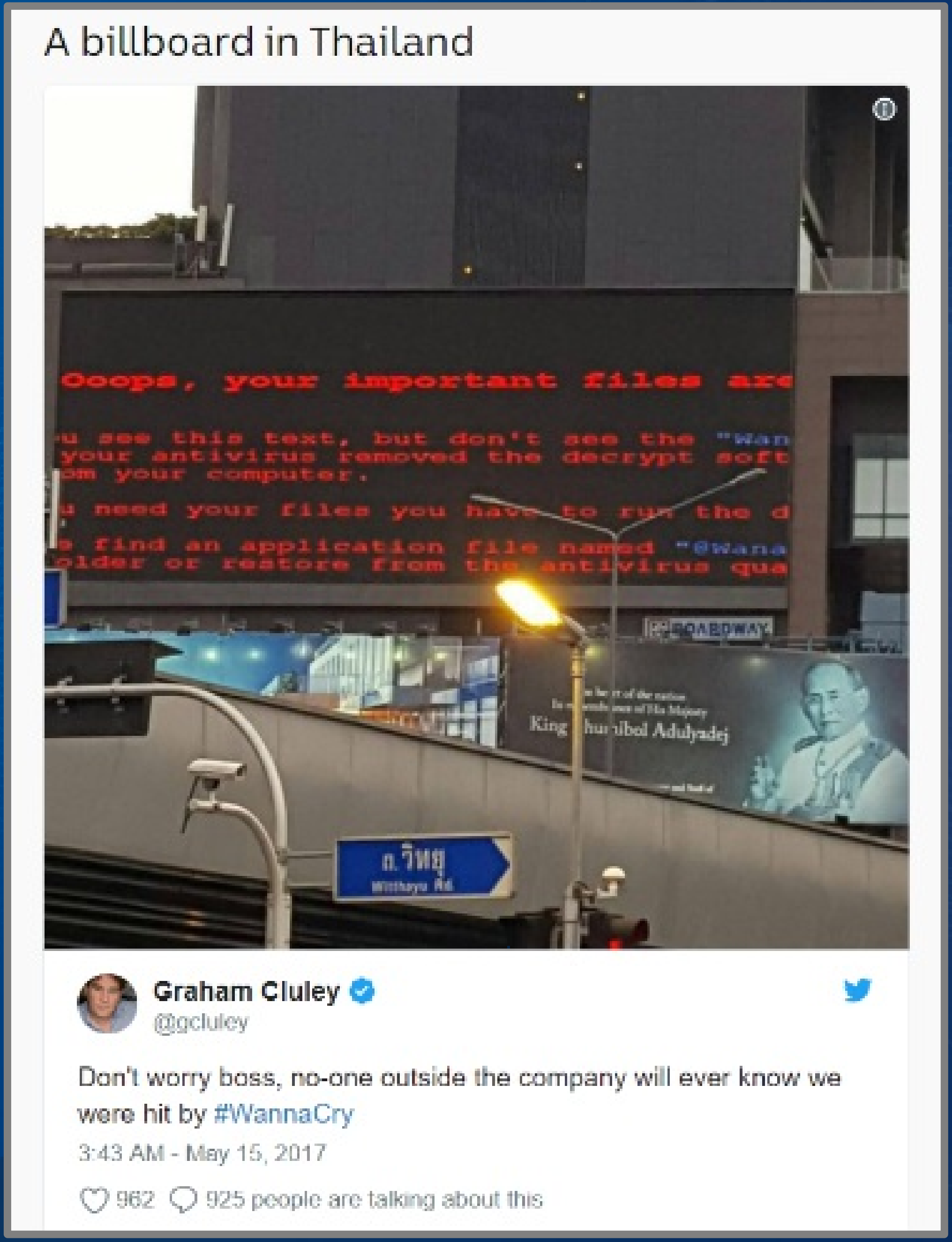
The lobby

Andrew Tinits
@amtinits

Wow, even in my building lobby! #WannaCry #ransomware

4:27 AM - May 13, 2017 · Waterloo, Ontario

♡ 658 💬 621 people are talking about this



A billboard in Thailand

Ooops, your important files are
u see this text, but don't see the "Wan
your antivirus removed the decrypt soft
om your computer.
u need your files you have to run the d
e find an application file named "@Wana
older or restore from the antivirus qua
King Bhumibol Adulyadej
ถ.วิทยุ
Witthayu Rd.

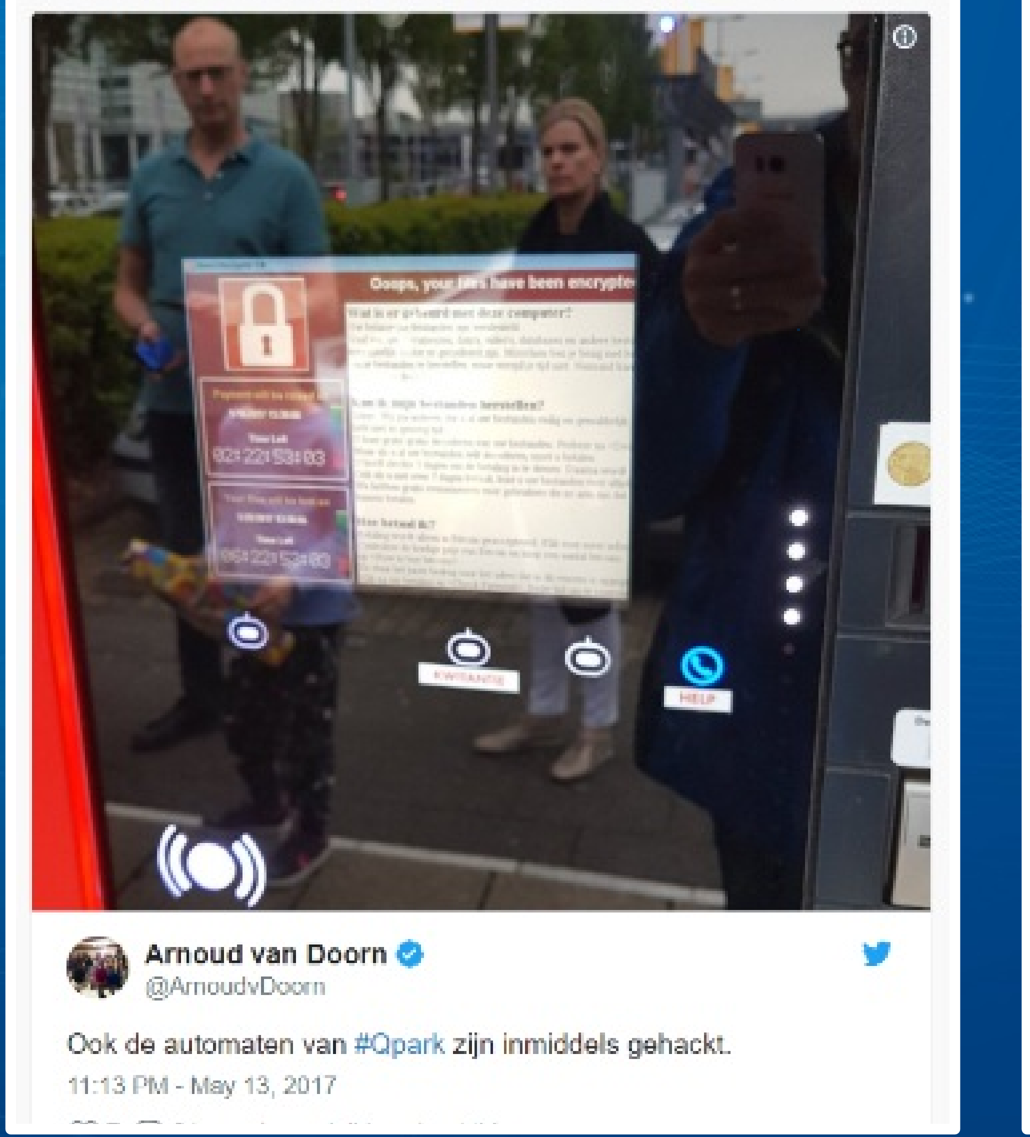
Graham Cluley
@gcluley

Don't worry boss, no-one outside the company will ever know we were hit by #WannaCry

3:43 AM - May 15, 2017

♡ 962 💬 925 people are talking about this

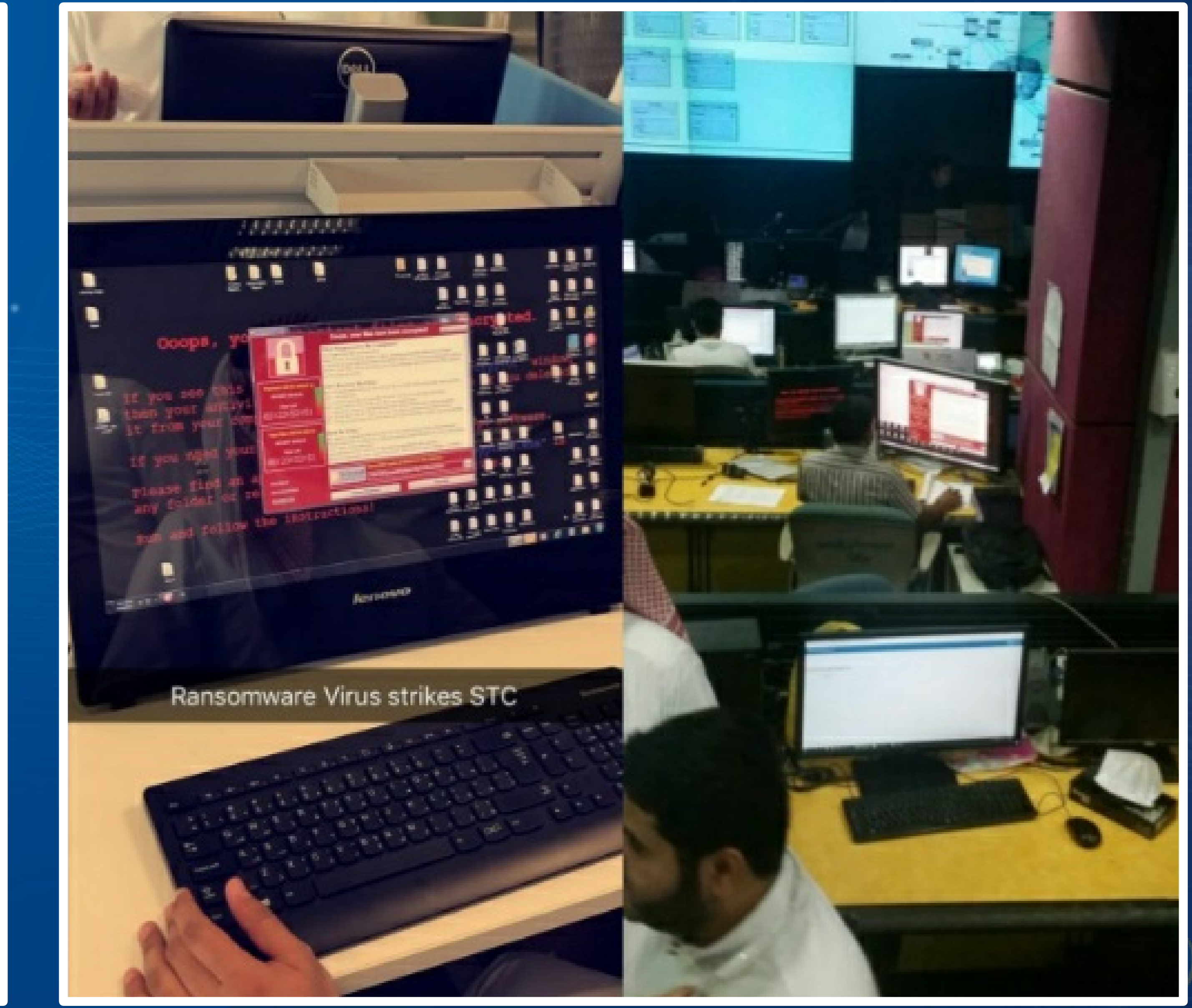
Parking machines in UK and Netherlands



Arnoud van Doorn
@ArnoudvDoorn

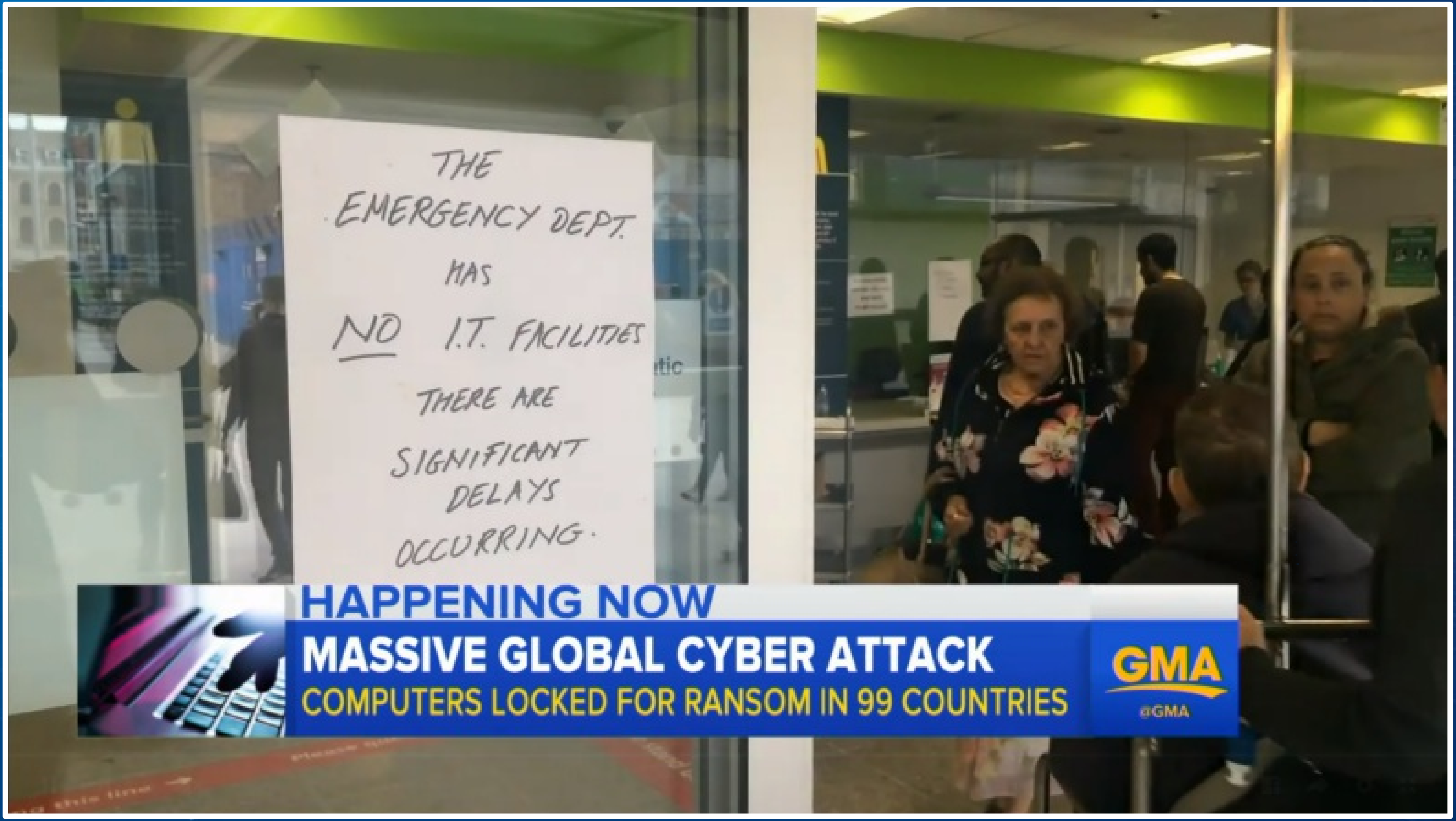
Ook de automaten van #Qpark zijn inmiddels gehackt.

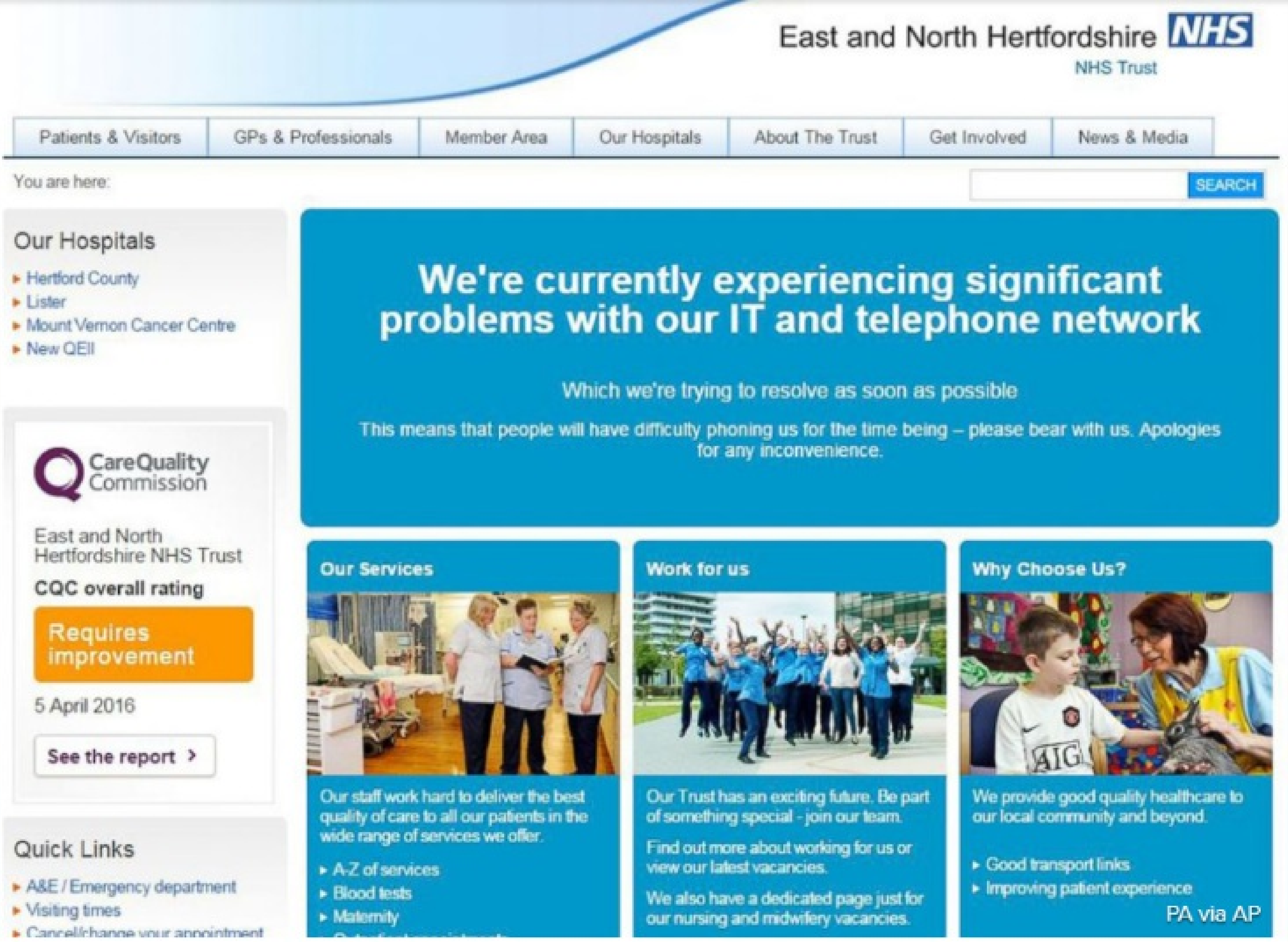
11:13 PM - May 13, 2017



Ransomware Virus strikes STC

自动取款机
ATM
自动取款机
ATM
存取款一体机
CDS
存取款一体机
CDS


THE
EMERGENCY DEPT.
HAS
NO I.T. FACILITIES
THERE ARE
SIGNIFICANT
DELAYS
OCCURRING.
HAPPENING NOW
MASSIVE GLOBAL CYBER ATTACK
COMPUTERS LOCKED FOR RANSOM IN 99 COUNTRIES
GMA
@GMA



East and North Hertfordshire NHS
NHS Trust

Patients & Visitors | GPs & Professionals | Member Area | Our Hospitals | About The Trust | Get Involved | News & Media

You are here:

SEARCH

Our Hospitals

- Hertford County
- Lister
- Mount Vernon Cancer Centre
- New QEII

Care Quality Commission

East and North Hertfordshire NHS Trust

CQC overall rating

Requires improvement

5 April 2016

See the report ›

Quick Links

- A&E / Emergency department
- Visiting times
- Cancel/change your appointment

We're currently experiencing significant problems with our IT and telephone network

Which we're trying to resolve as soon as possible

This means that people will have difficulty phoning us for the time being – please bear with us. Apologies for any inconvenience.

Our Services

Our staff work hard to deliver the best quality of care to all our patients in the wide range of services we offer.

- A-Z of services
- Blood tests
- Maternity

Work for us

Our Trust has an exciting future. Be part of something special - join our team.

Find out more about working for us or view our latest vacancies.

We also have a dedicated page just for our nursing and midwifery vacancies.

Why Choose Us?

We provide good quality healthcare to our local community and beyond.

- Good transport links
- Improving patient experience

PA via AP

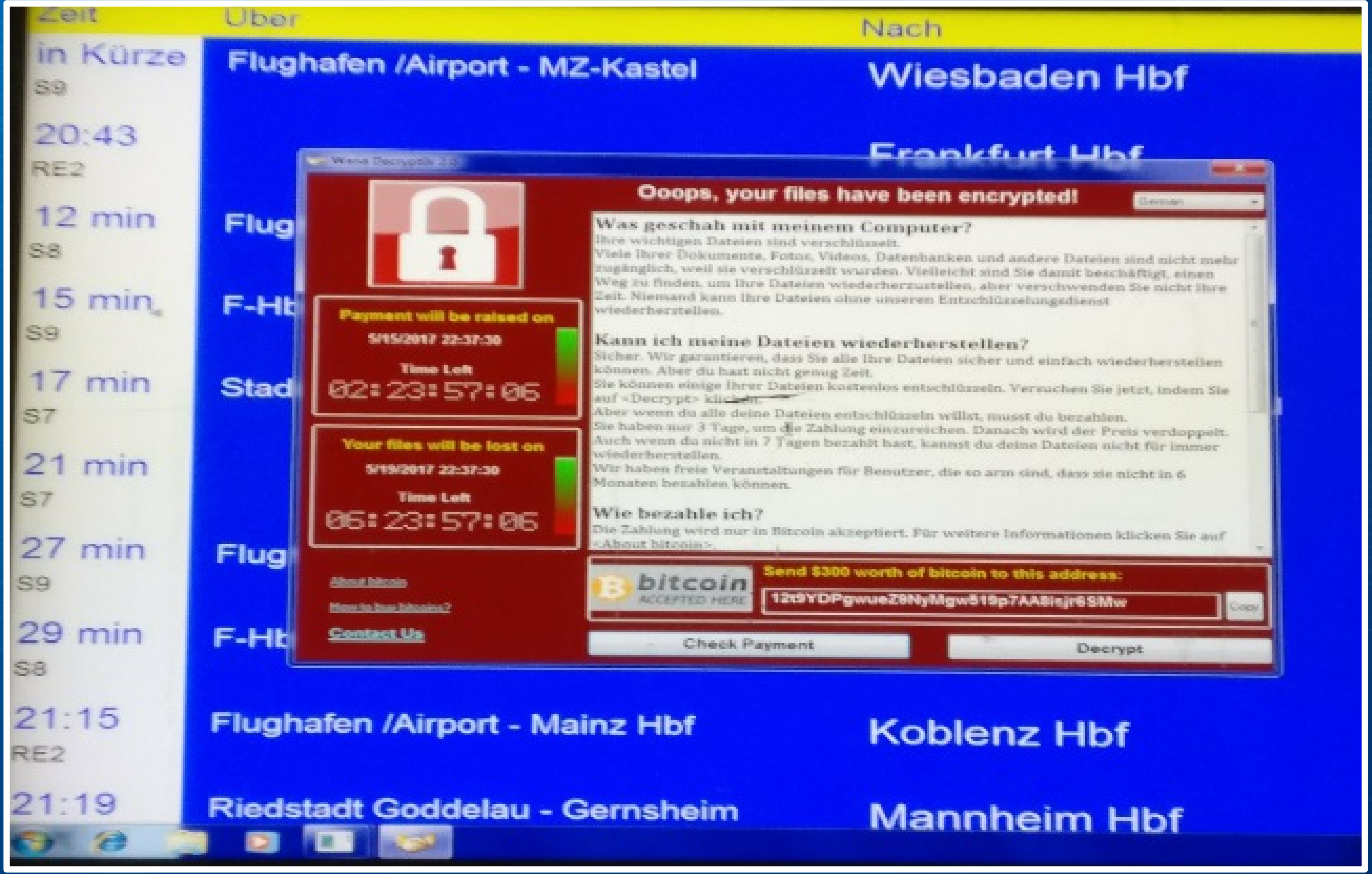
WannaCry

- WannaCry was discovered **91 days prior to the outbreak**
- The patch for the SMB vulnerability was available **59 days prior to the attack**
- Over **200,000 victims** & **300,000 computers** across **150 countries**
- Financial loss : **$4 Billion**

Prime victim

- May. 12th Friday at 4 PM - **NHS declared "Wannacry Attack"**
- 81 out of 236 trusts, 603 primary health care & NHS organizations were affected
- 19494 Appointments were cancelled (5 areas)
- 1220 Medical Equipments were affected

Hackers target Deutsche Bahn



Ooops, your files have been encrypted!

Was geschah mit meinem Computer?

Ihre wichtigen Dateien sind verschlüsselt.
Viele Ihrer Dokumente, Fotos, Videos, Datenbanken und andere Dateien sind nicht mehr zugänglich, weil sie verschlüsselt wurden. Vielleicht sind Sie damit beschäftigt, einen Weg zu finden, um Ihre Dateien wiederherzustellen, aber verschwenden Sie nicht Ihre Zeit. Niemand kann Ihre Dateien ohne unseren Entschlüsselungsdienst wiederherstellen.

Kann ich meine Dateien wiederherstellen?

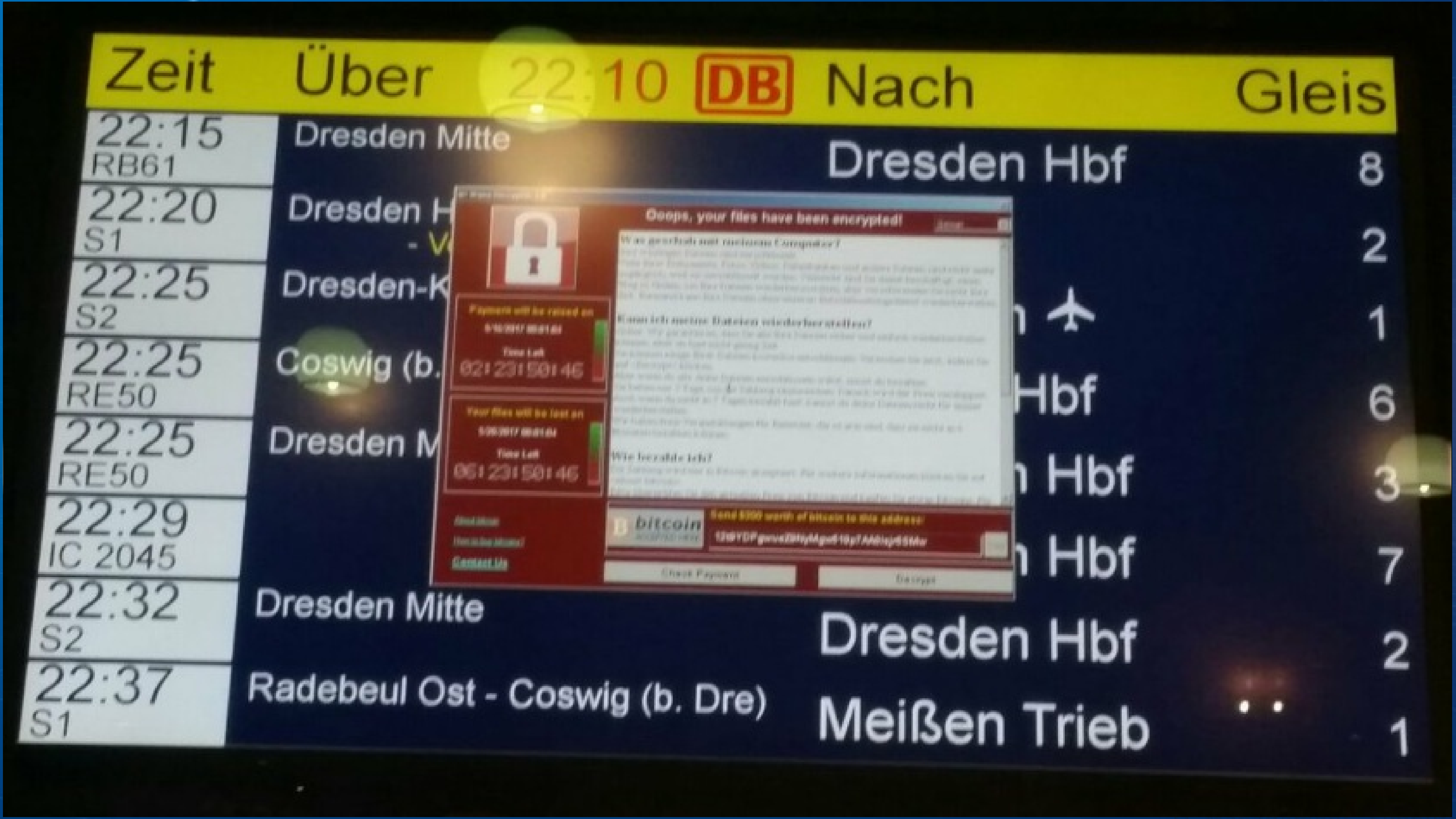
Sicher. Wir garantieren, dass Sie alle Ihre Dateien sicher und einfach wiederherstellen können. Aber du hast nicht genug Zeit.
Sie können einige Ihrer Dateien kostenlos entschlüsseln. Versuchen Sie jetzt, indem Sie auf <Decrypt> klicken.
Aber wenn du alle deine Dateien entschlüsseln willst, musst du bezahlen.
Sie haben nur 3 Tage, um die Zahlung einzureichen. Danach wird der Preis verdoppelt.
Auch wenn du nicht in 7 Tagen bezahlt hast, kannst du deine Dateien nicht für immer wiederherstellen.
Wir haben freie Veranstaltungen für Benutzer, die so arm sind, dass sie nicht in 6 Monaten bezahlen können.

Wie bezahle ich?

Die Zahlung wird nur in Bitcoin akzeptiert. Für weitere Informationen klicken Sie auf <About bitcoin>.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw


Zeit
Über
22:10
DB
Nach
Gleis
22:15 RB61
Dresden Mitte
Dresden Hbf
8
22:20 S1
Dresden H
- V
2
22:25 S2
Dresden-K
1
22:25 RE50
Coswig (b.
Hbf
6
22:25 RE50
Dresden M
Hbf
3
22:29 IC 2045
Hbf
7
22:32 S2
Dresden Mitte
Dresden Hbf
2
22:37 S1
Radebeul Ost - Coswig (b. Dre)
Meißen Trieb
1
Ooops, your files have been encrypted!
Payment will be raised on
Time Left
02:23:59:46
Your files will be lost on
Time Left
06:23:59:46
Was geschah mit meinem Computer?
Kann ich meine Dateien wiederherstellen?
Wie bezahle ich?
bitcoin
Send $300 worth of bitcoin to this address:
Contact Us
Check Payment
Decrypt

Responding to Ransomware

If victimized by ransomware in the past 12 months, did your organization pay a ransom (using Bitcoins or other anonymous currency) to recover data? (n=1,176)

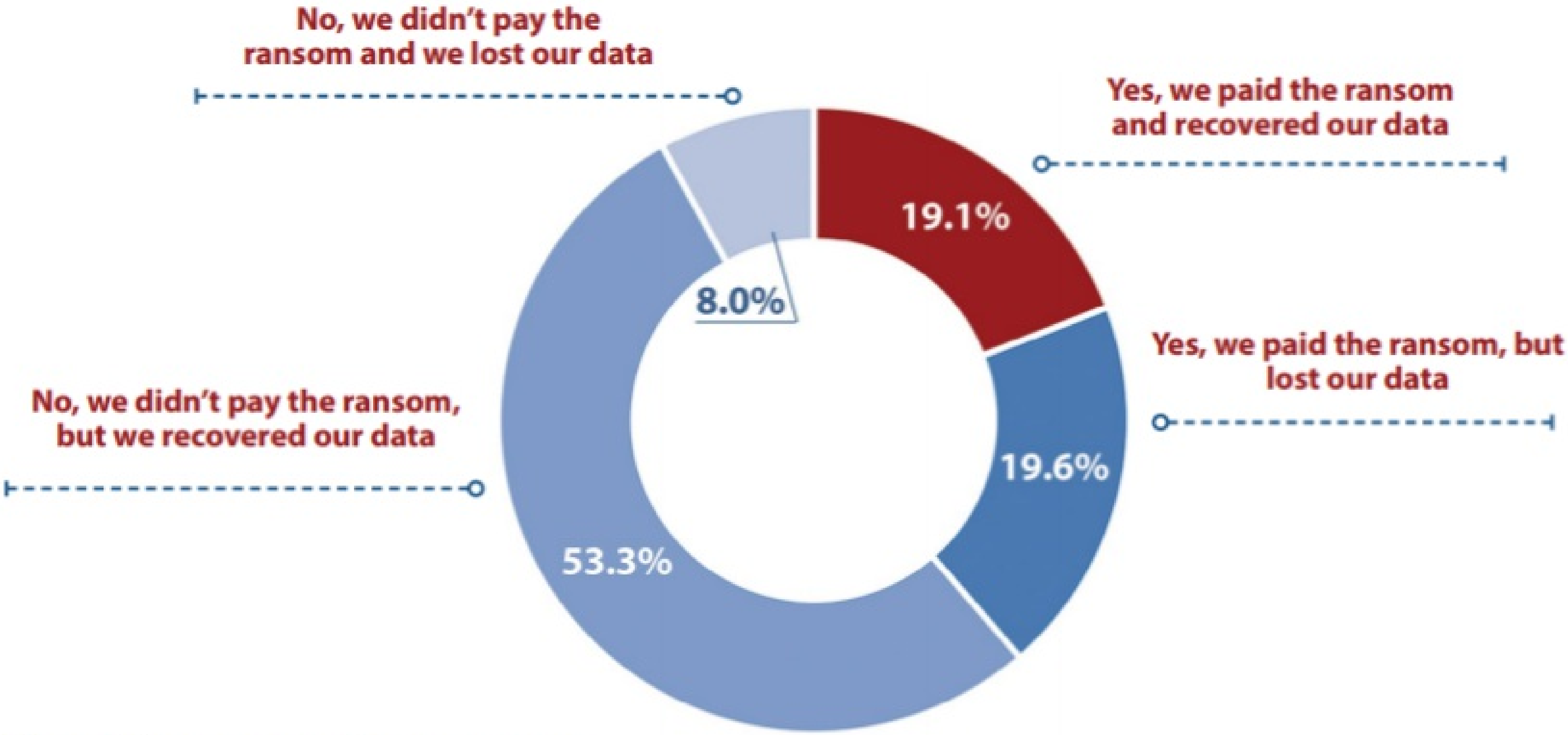


Figure 12: How victims responded to ransomware.

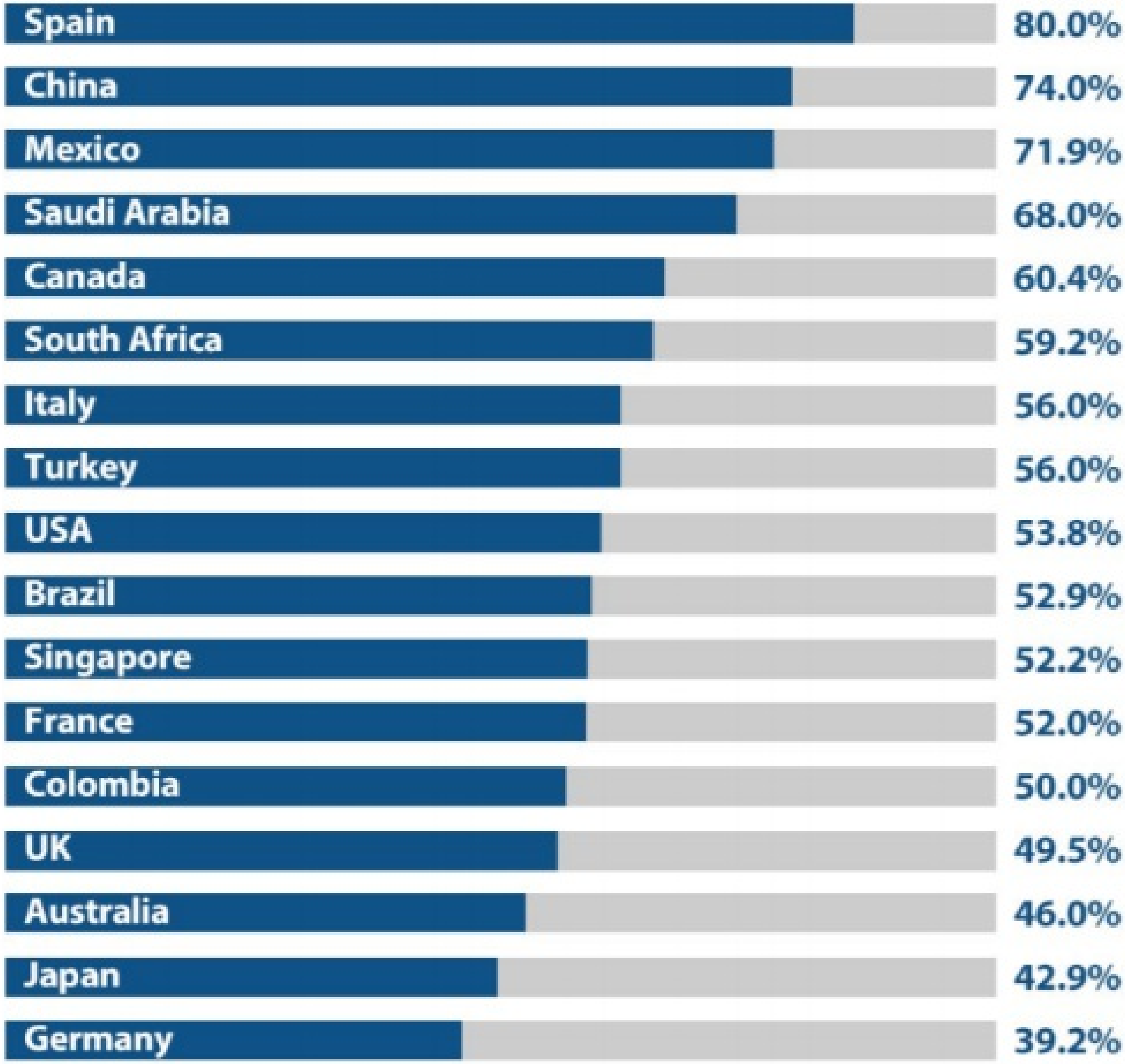


Figure 13: Percentage affected by ransomware in the past 12 months.

Past Frequency of Successful Cyberattacks

How many times do you estimate that your organization's global network has been compromised by a successful cyberattack within the past 12 months? (n=1,136)

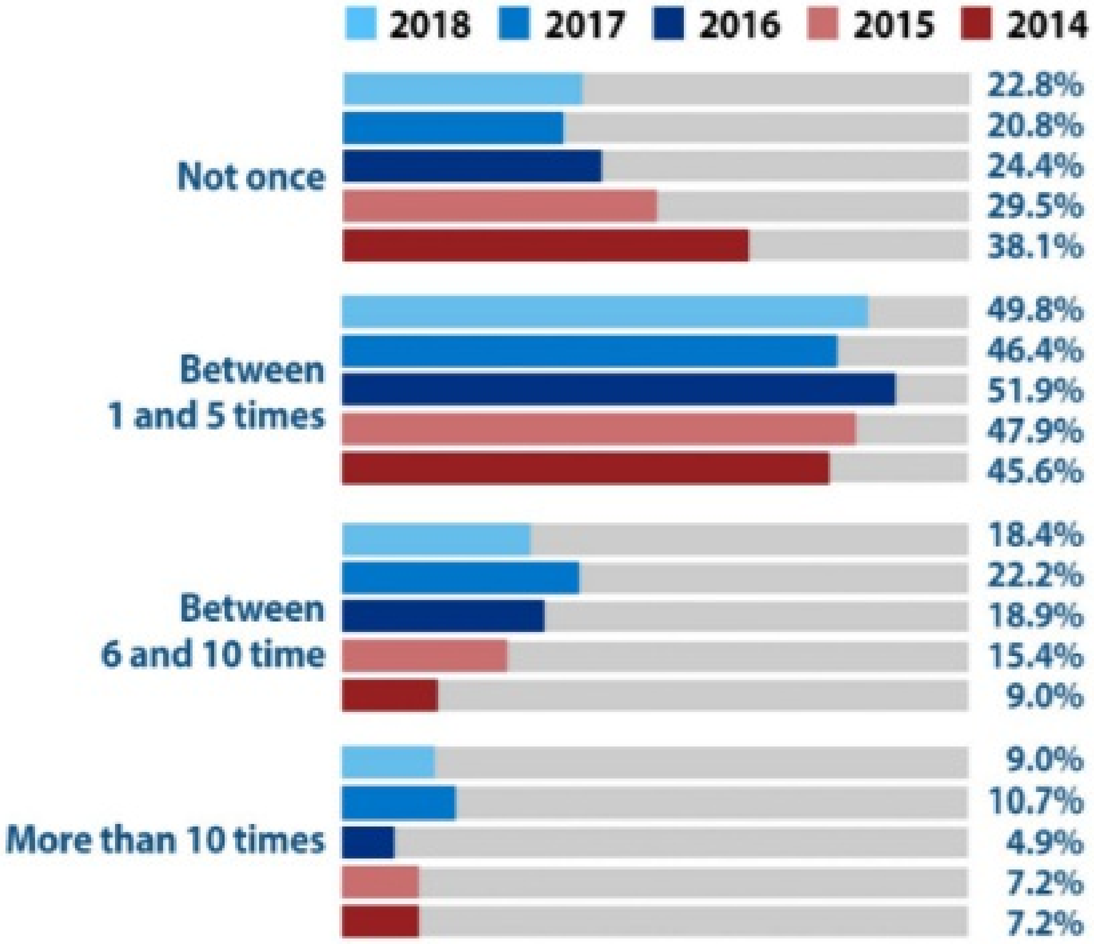


Figure 1: Frequency of successful attacks in the past 12 months.

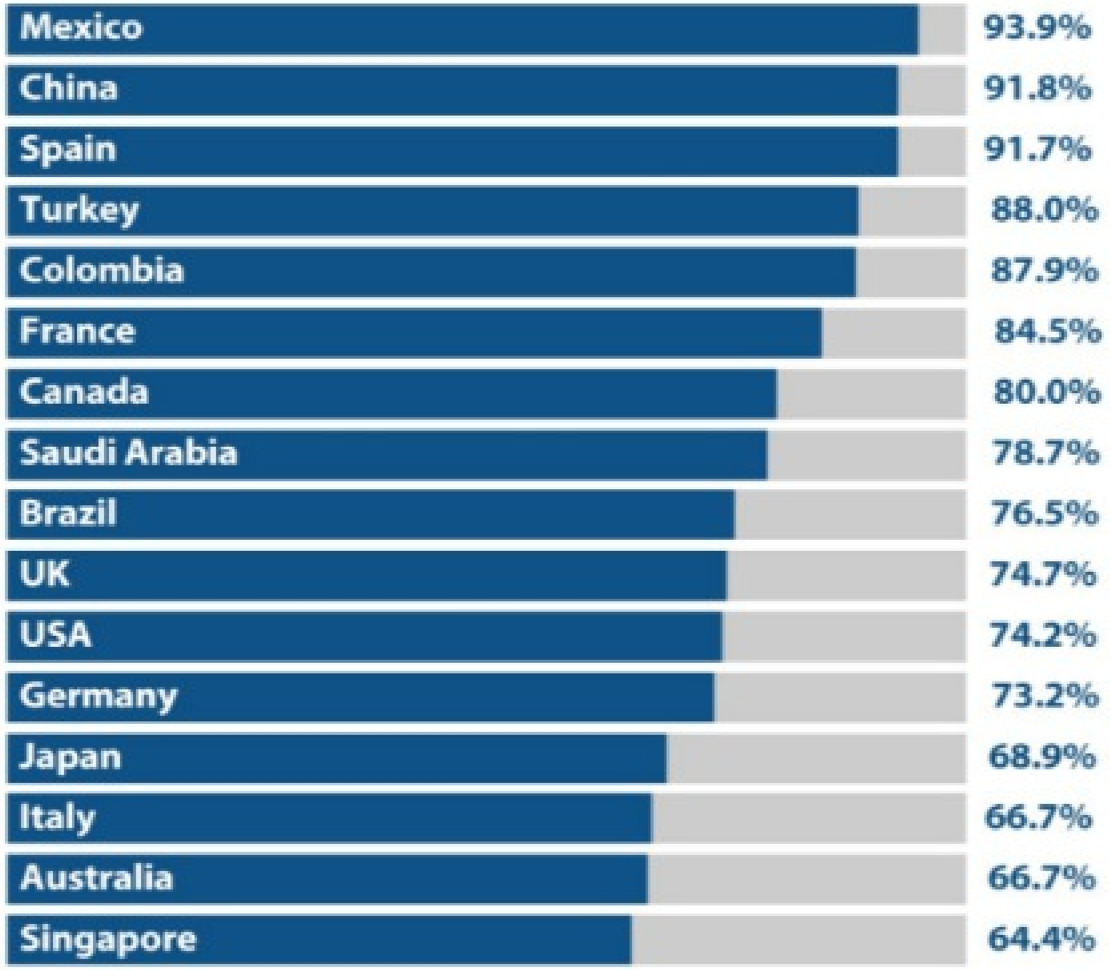


Figure 2: Percentage compromised by at least one successful attack in the past 12 months.

Future Likelihood of Successful Cyberattacks

What is the likelihood that your organization's network will become compromised by a successful cyberattack in 2018? (n=1,175)

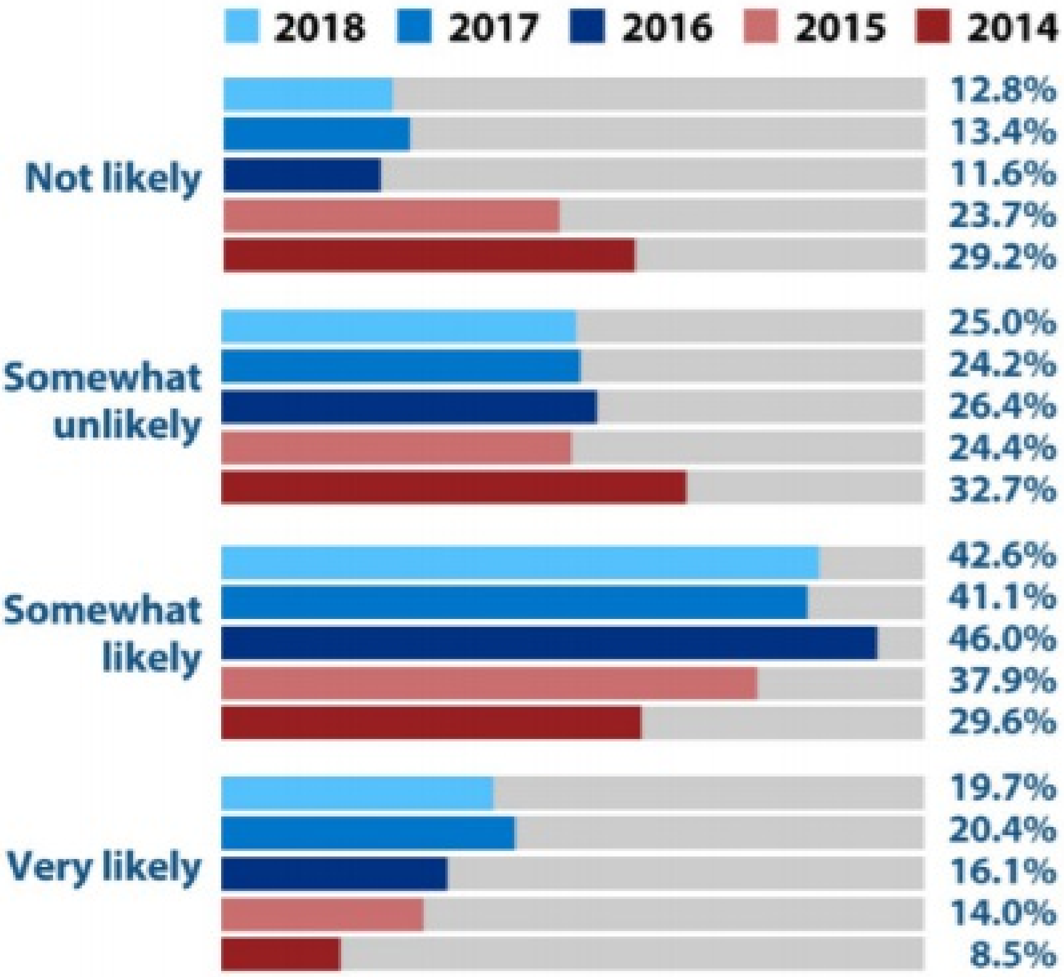


Figure 3: Likelihood of being successfully attacked in the next 12 months.

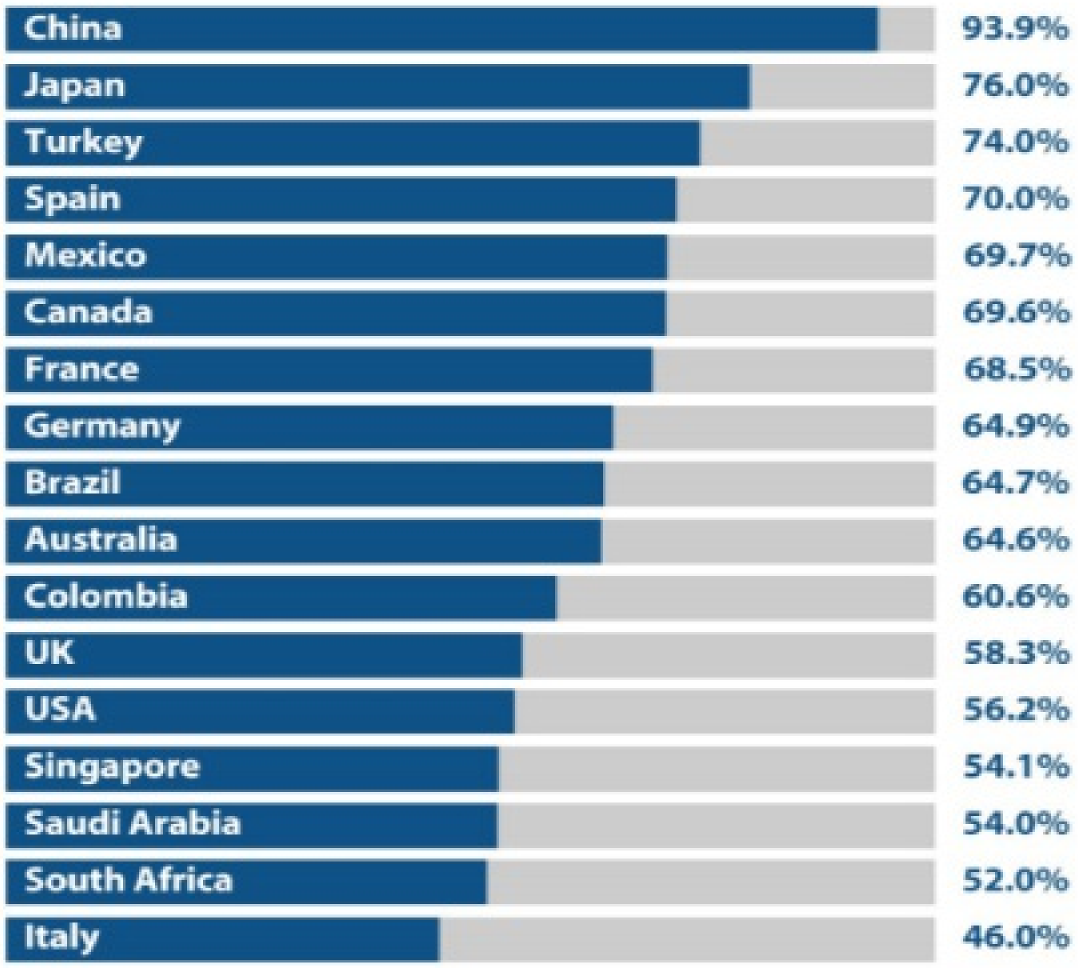
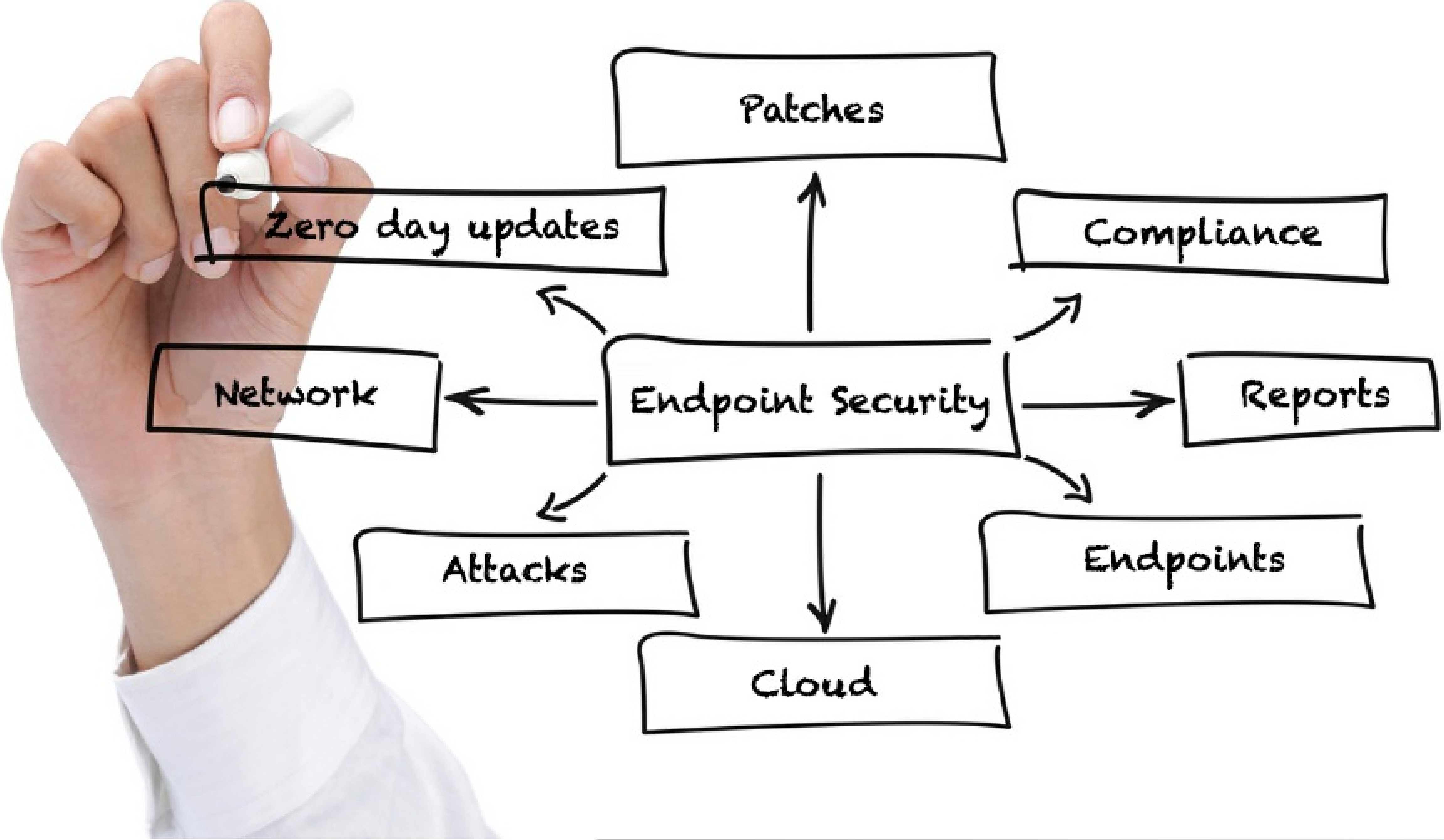


Figure 4: Percentage indicating compromise is "more likely to occur than not" in the next 12 months.

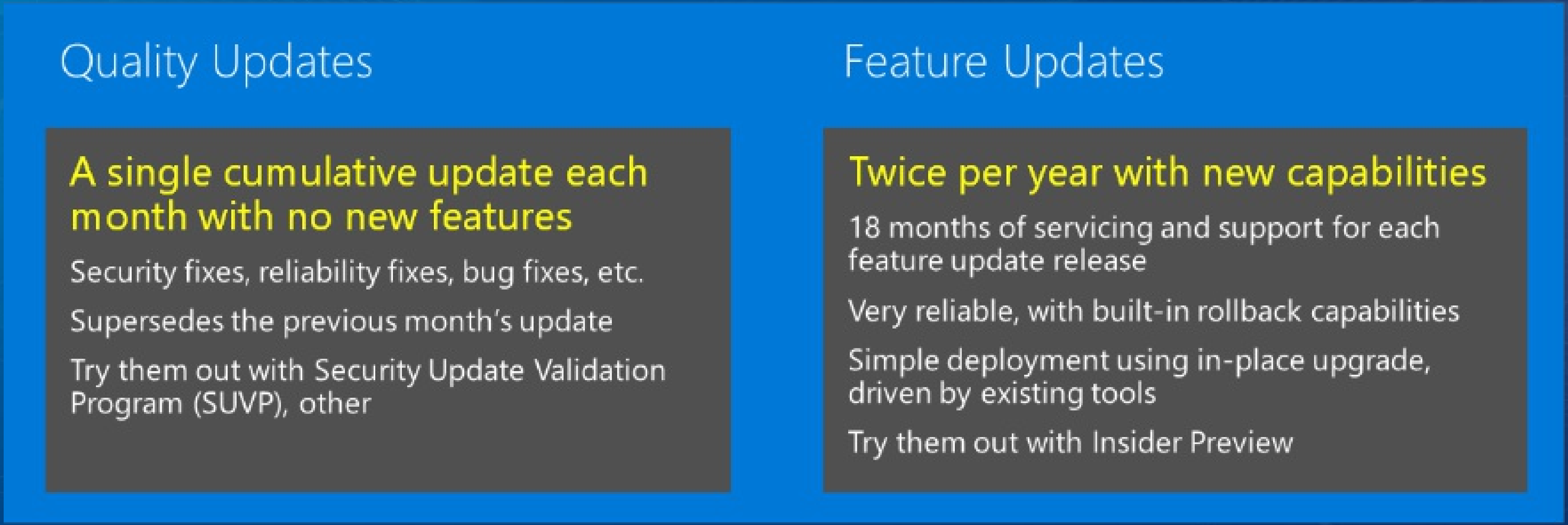
Lessons Learnt

- ❖ OSs and Software/Applications not patched
- ❖ AV updates were missing
- ❖ Firewall security compromised
- ❖ Security Policies were not enforced


Patches
Zero day updates
Compliance
Network
Endpoint Security
Reports
Attacks
Endpoints
Cloud

Insights of patching

Microsoft update approach



Quality Updates

A single cumulative update each month with no new features

Security fixes, reliability fixes, bug fixes, etc.

Supersedes the previous month's update

Try them out with Security Update Validation Program (SUVP), other

Feature Updates

Twice per year with new capabilities

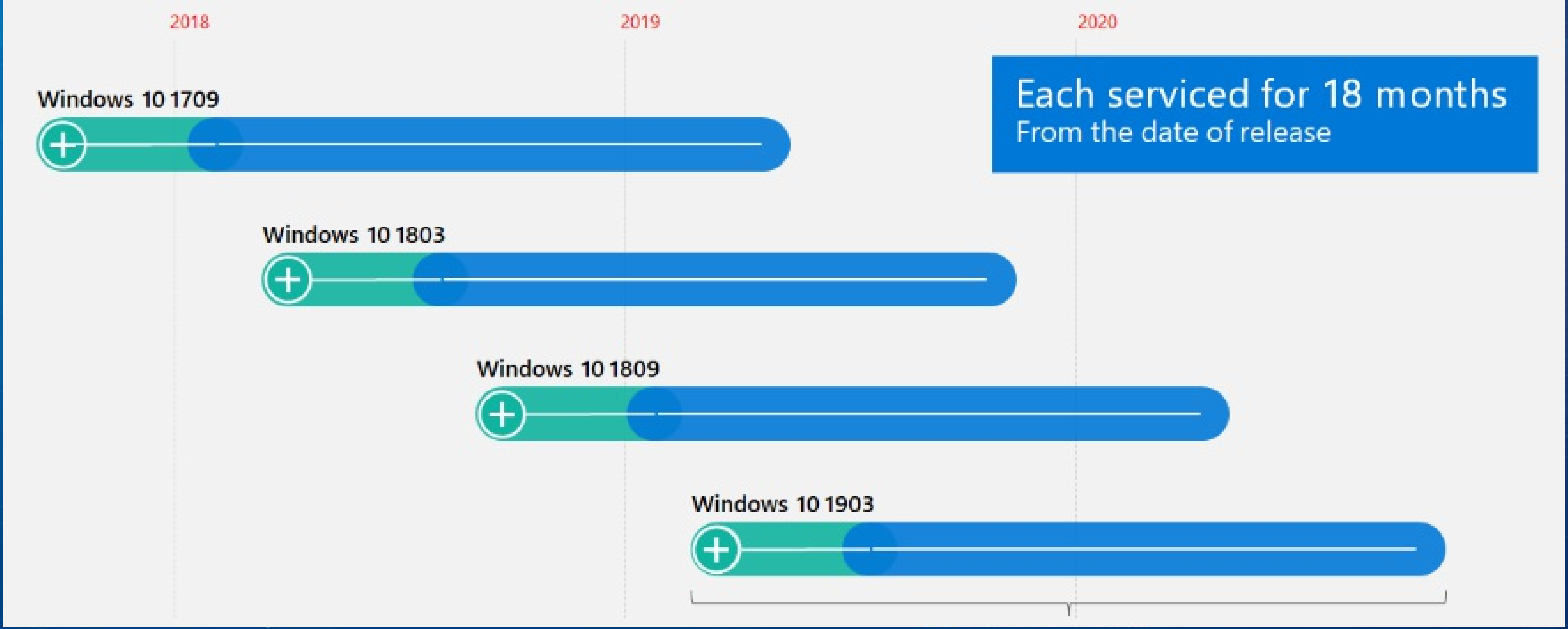
18 months of servicing and support for each feature update release

Very reliable, with built-in rollback capabilities

Simple deployment using in-place upgrade, driven by existing tools

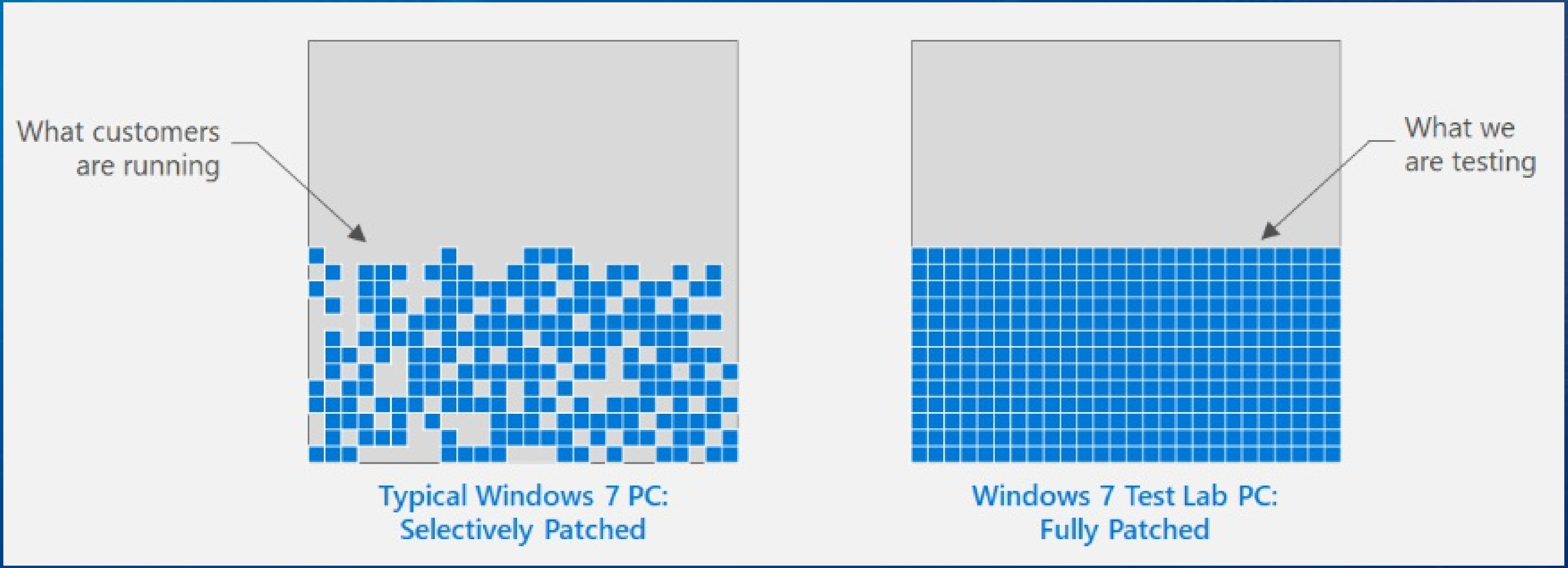
Try them out with Insider Preview

Microsoft update approach

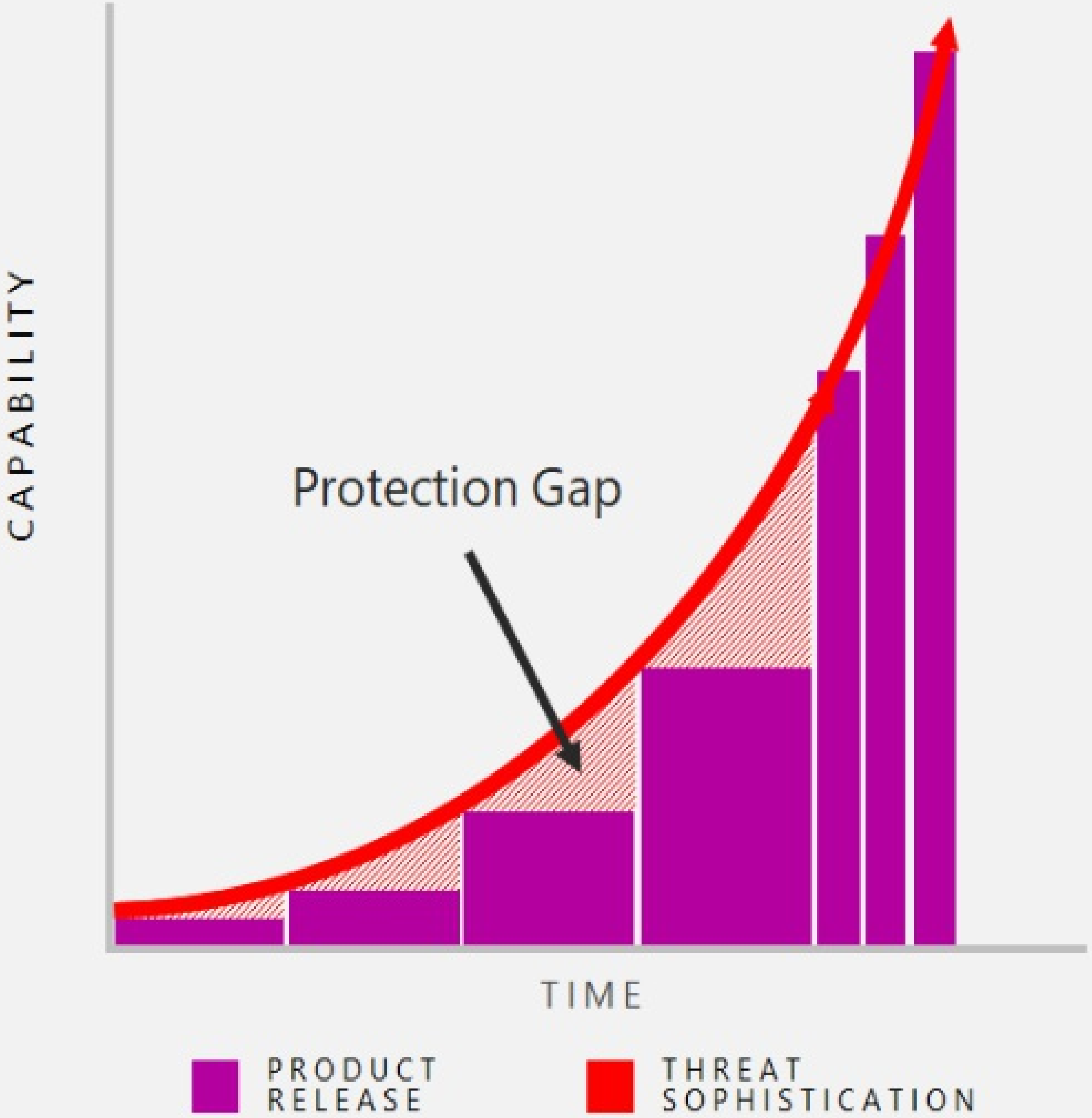


Each serviced for 18 months
From the date of release

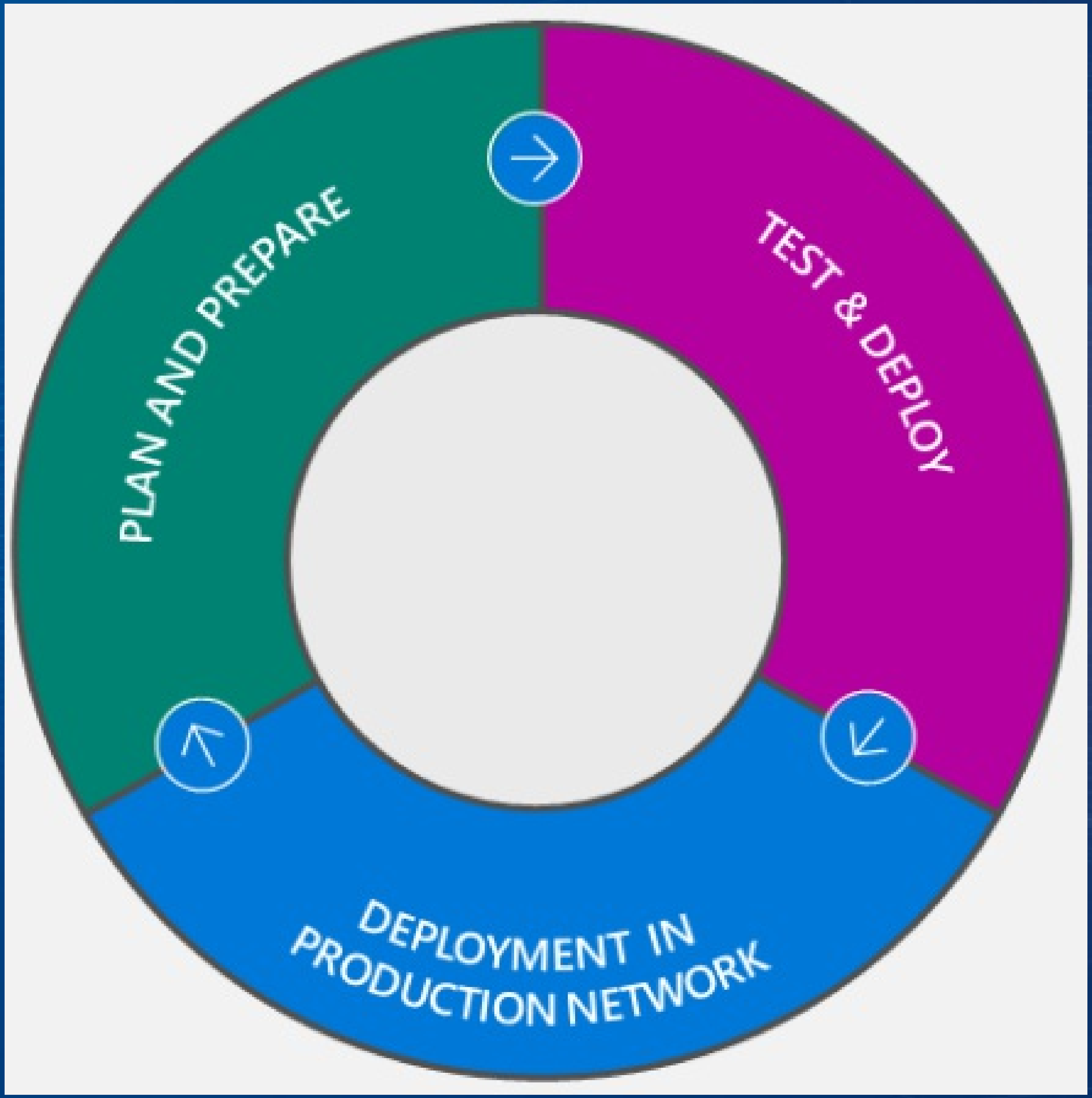
Full patch approach


What customers are running
What we are testing
Typical Windows 7 PC: Selectively Patched
Windows 7 Test Lab PC: Fully Patched

- Predictable update
- Increased protection
- Reduced attack surface

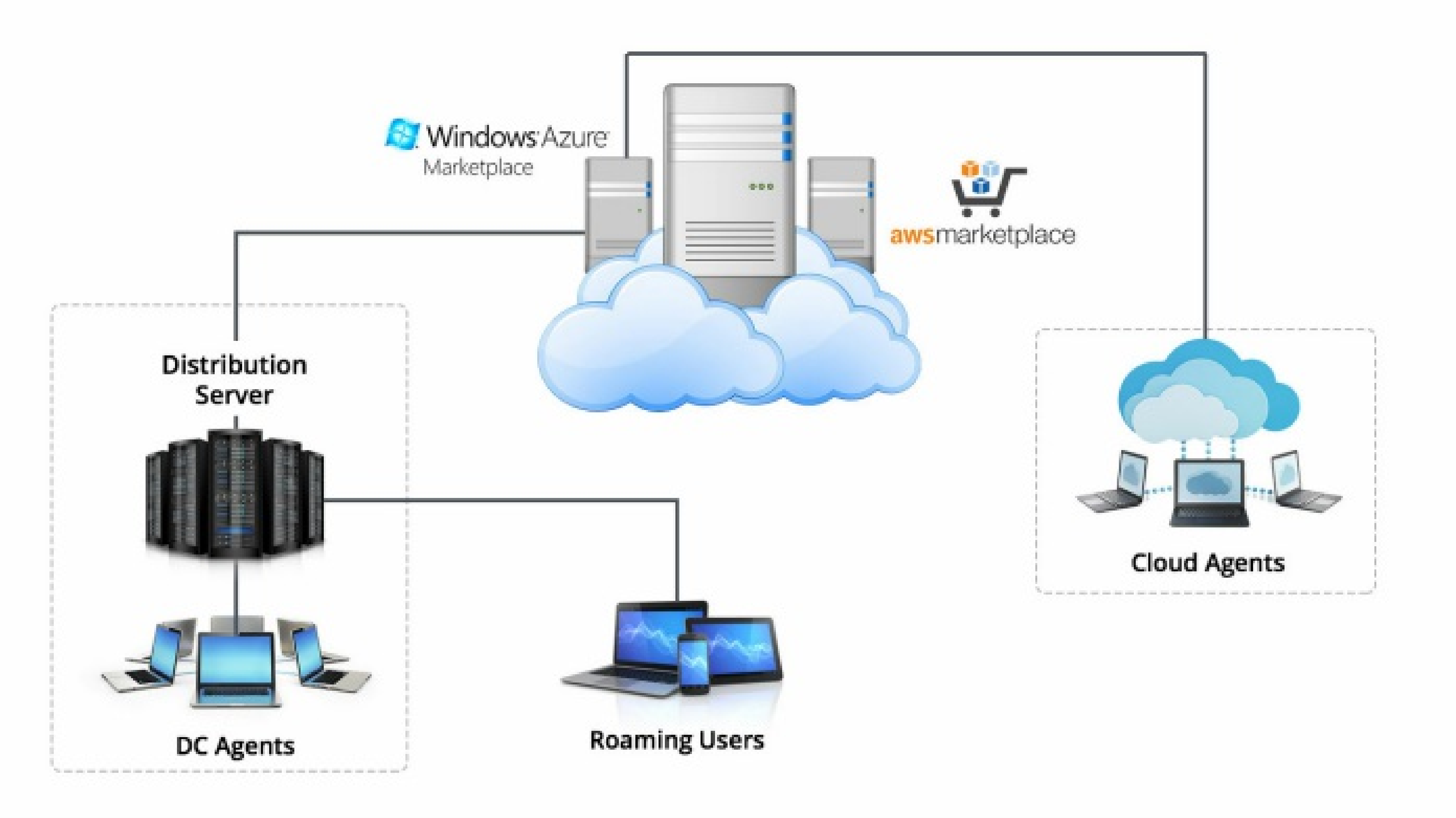


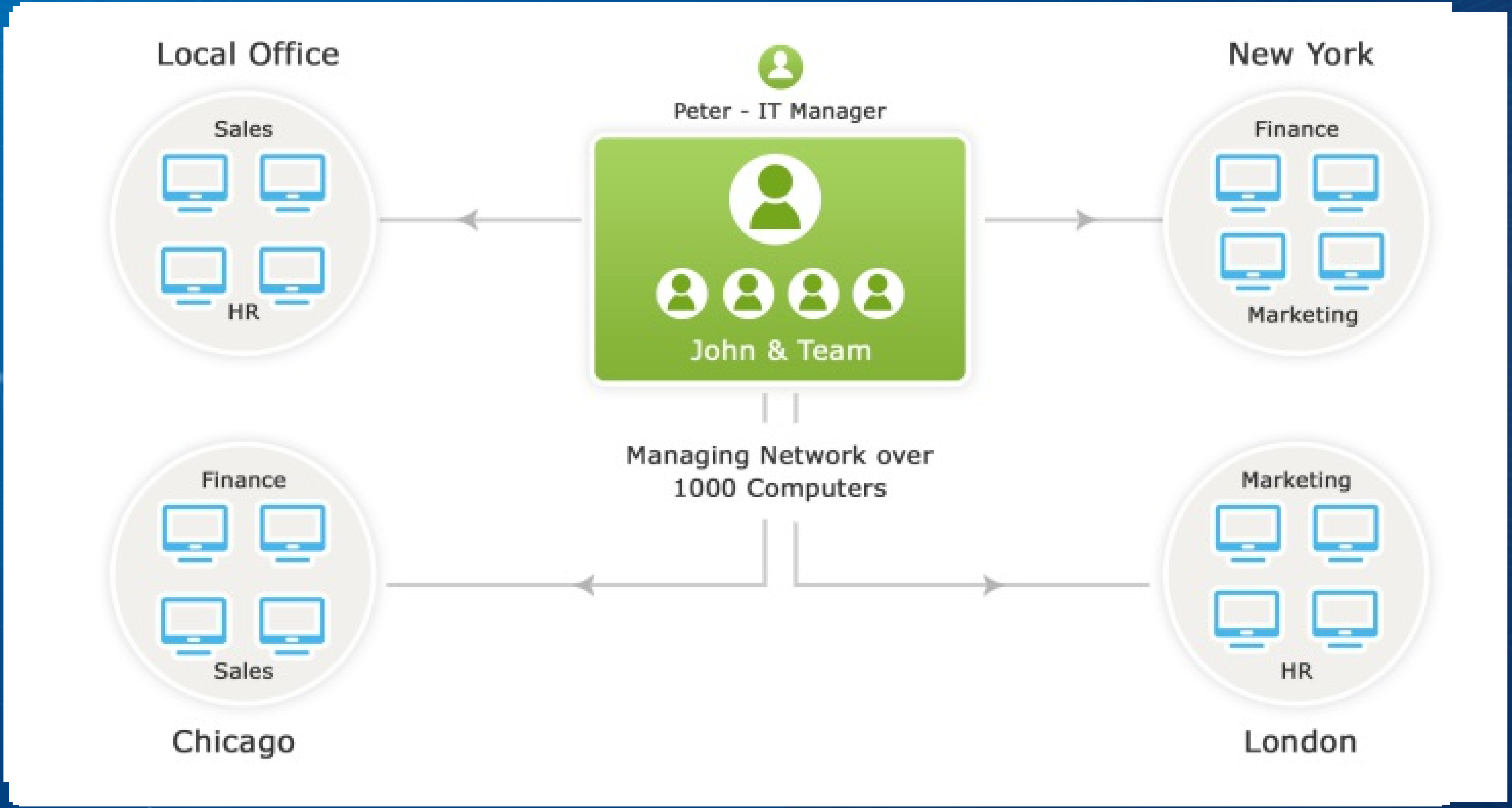
- Plan and prepare using preview (*definitely not for production*)
- Test and deploy (*In the targeted test and user systems*)
- Automated deployment in production network



Supported OS

Over 1000+ applications can be patched across ***Windows, Mac, Linux,*** and ***third-party*** applications.


Windows Azure Marketplace
aws marketplace
Distribution Server
DC Agents
Roaming Users
Cloud Agents


Local Office
Sales
HR
Peter - IT Manager
John & Team
New York
Finance
Marketing
Managing Network over
1000 Computers
Finance
Sales
Chicago
Marketing
HR
London

Objective: Set up patch management

Scan and test on pilot group of computers
Approve patches
Deploy to production computers
Automate deployment in stages
Run reports

Other Patch Management Offerings

ManageEngine

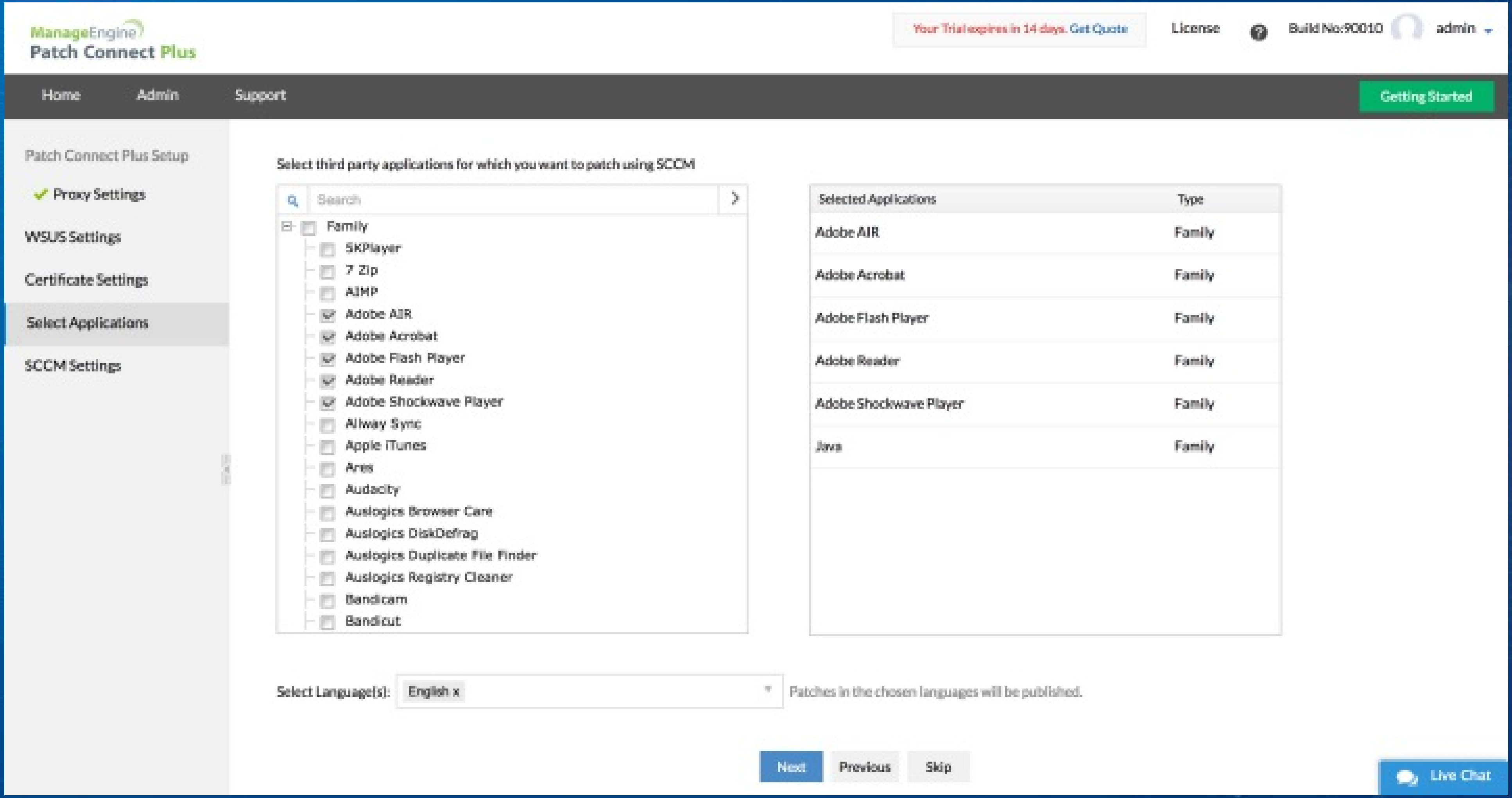
Patch Manager Plus

Automate patch management for **Windows**, **Mac**, **Linux** & **3rd party apps**

ManageEngine

Patch Connect Plus

Patch your 3rd party application using **Microsoft SCCM**



Patch Connect Plus Setup

- ✓ Proxy Settings
- WSUS Settings
- Certificate Settings
- Select Applications
- SCCM Settings

Select third party applications for which you want to patch using SCCM

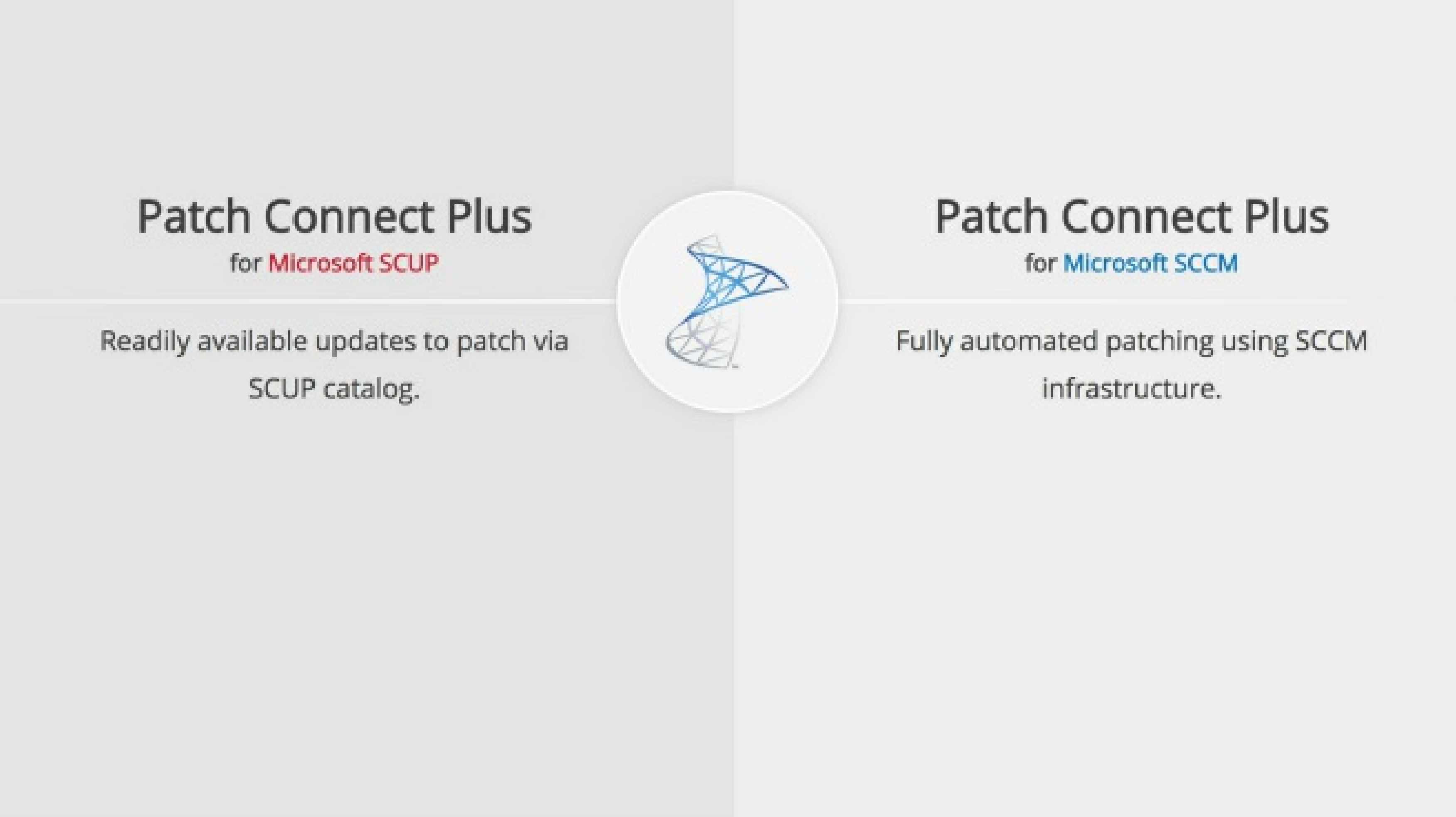
Search

- □ Family
  - □ 5KPlayer
  - □ 7 Zip
  - □ AIMP
  - ☑ Adobe AIR
  - ☑ Adobe Acrobat
  - ☑ Adobe Flash Player
  - ☑ Adobe Reader
  - ☑ Adobe Shockwave Player
  - □ Allway Sync
  - □ Apple iTunes
  - □ Ares
  - □ Audacity
  - □ Auslogics Browser Care
  - □ Auslogics DiskDefrag
  - □ Auslogics Duplicate File Finder
  - □ Auslogics Registry Cleaner
  - □ Bandicam
  - □ Bandicut

Selected Applications	Type
Adobe AIR	Family
Adobe Acrobat	Family
Adobe Flash Player	Family
Adobe Reader	Family
Adobe Shockwave Player	Family
Java	Family

Select Language(s): English x

Patches in the chosen languages will be published.



Patch Connect Plus

for Microsoft SCUP

Readily available updates to patch via SCUP catalog.

Patch Connect Plus

for Microsoft SCCM

Fully automated patching using SCCM infrastructure.

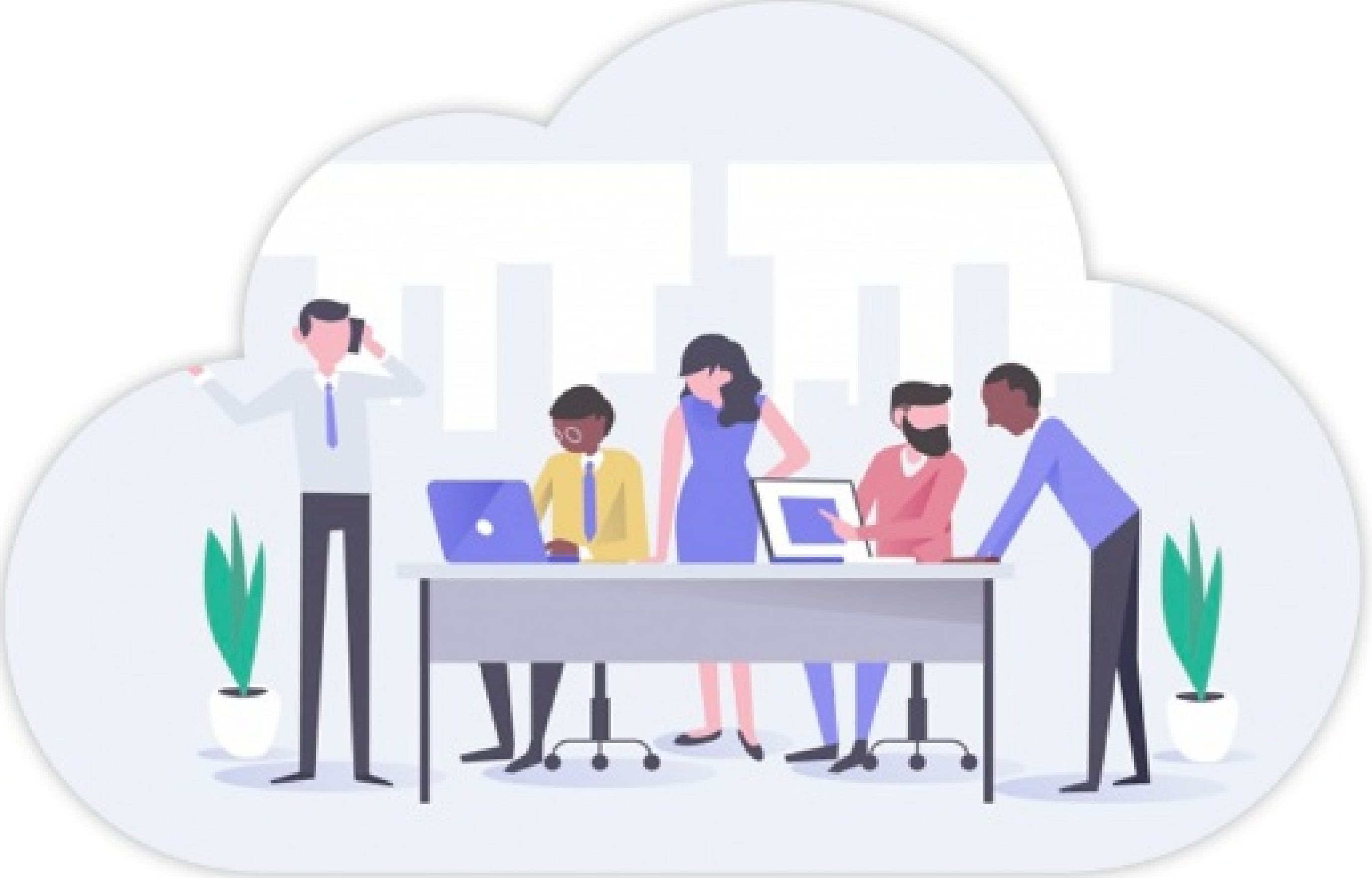
Browser security plus

Some interesting numbers on **cloud adoption** and **browser usage** across organisations

928 cloud applications

per organization

Symantec Internet Security Threat Report 2017



SMBs run

83%

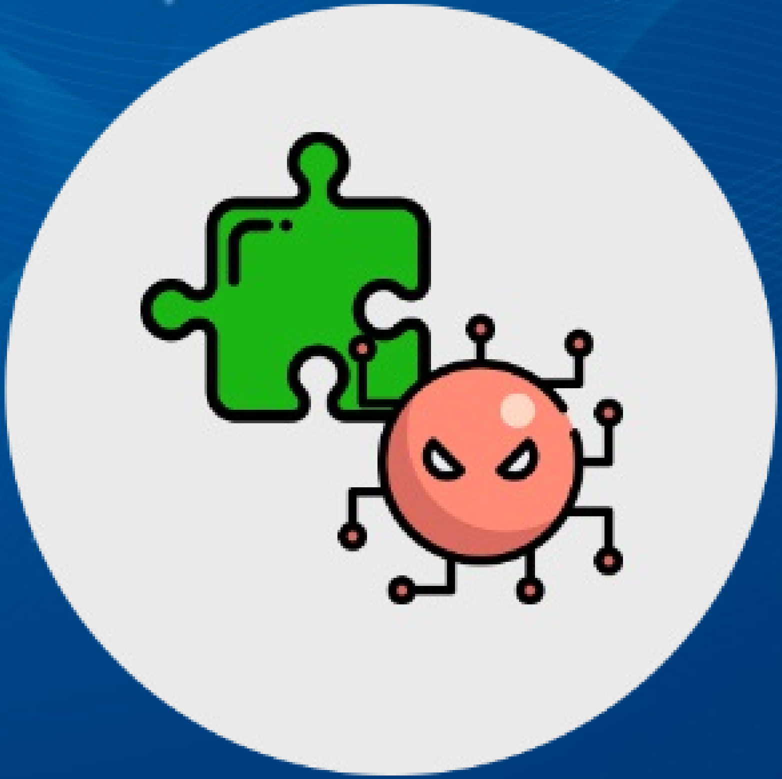
workload in cloud

Source: Rightscale 2017 State of the cloud report

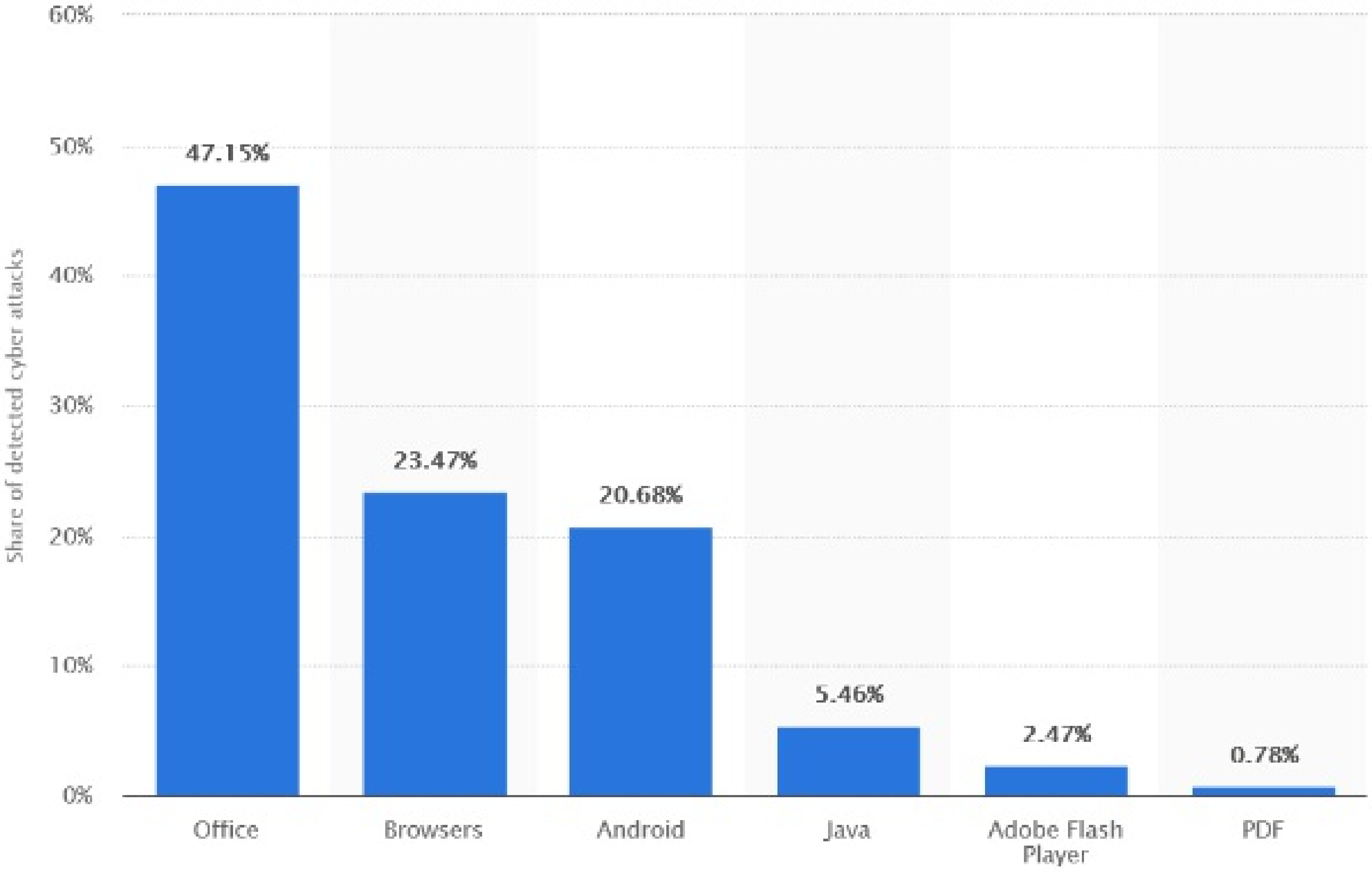
chrome

There's always two sides to a coin

Data breach through add-ons



Most commonly exploited applications worldwide as of 1st quarter 2018

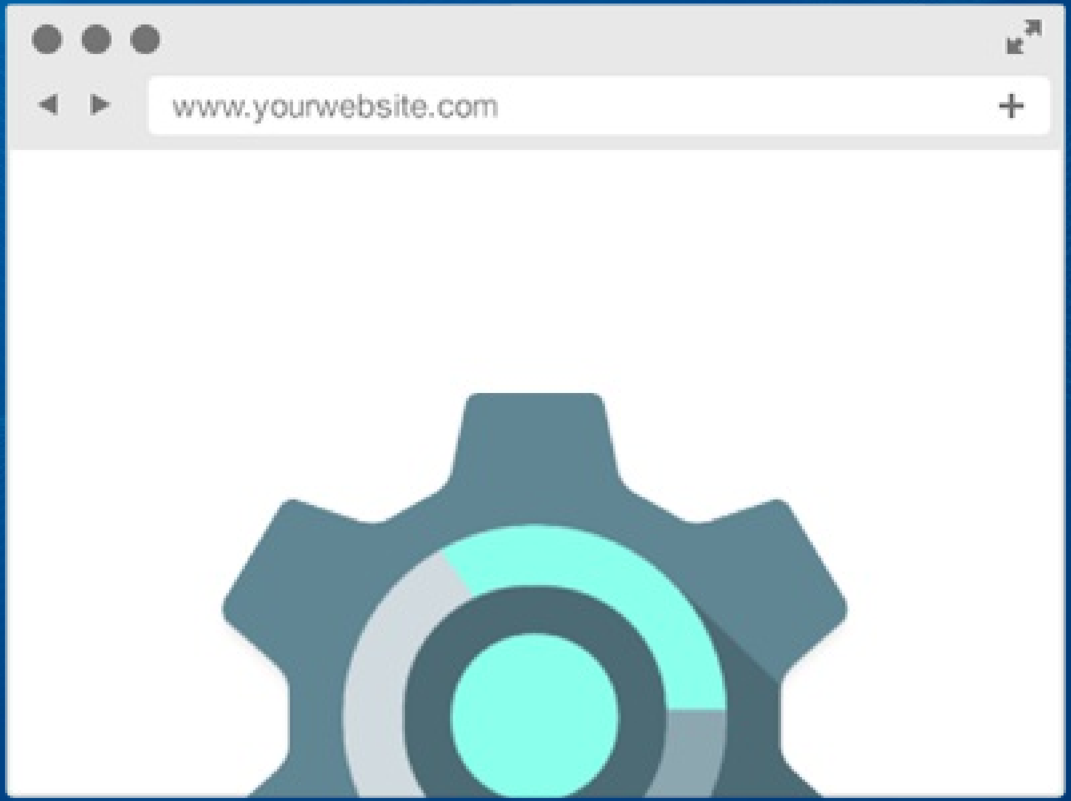


Source: Statista Most commonly exploited applications worldwide as of 1st quarter 2018

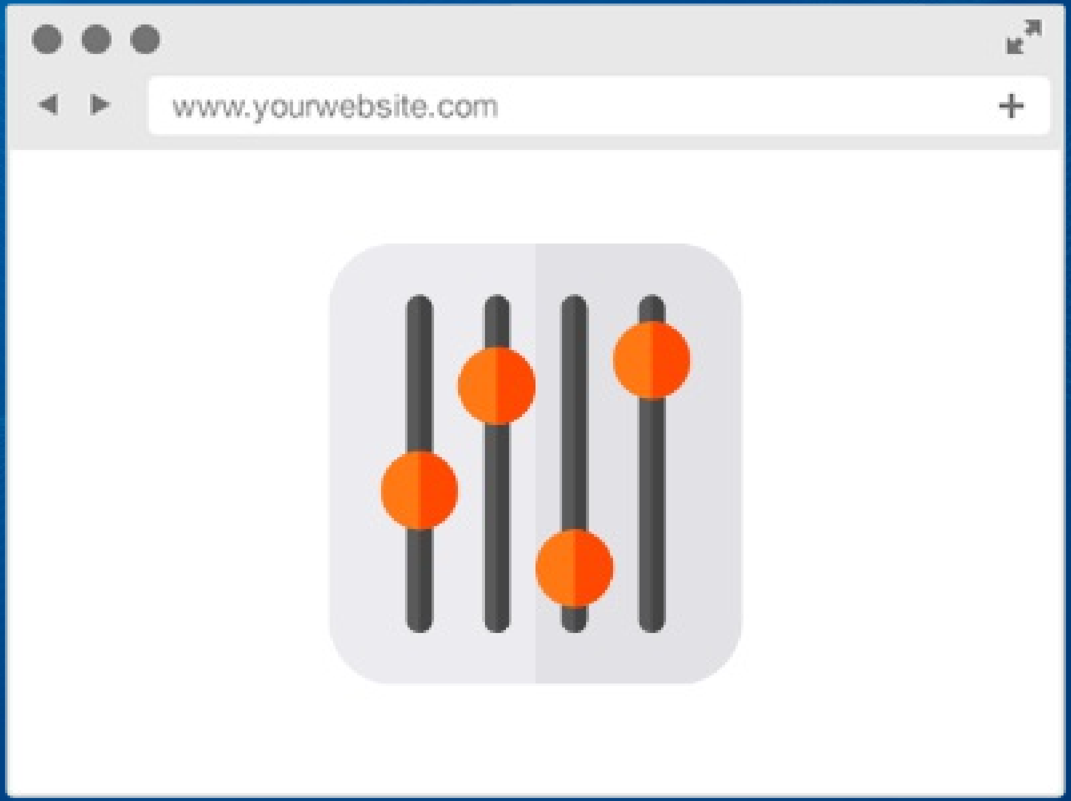
ManageEngine

Browser Security Plus

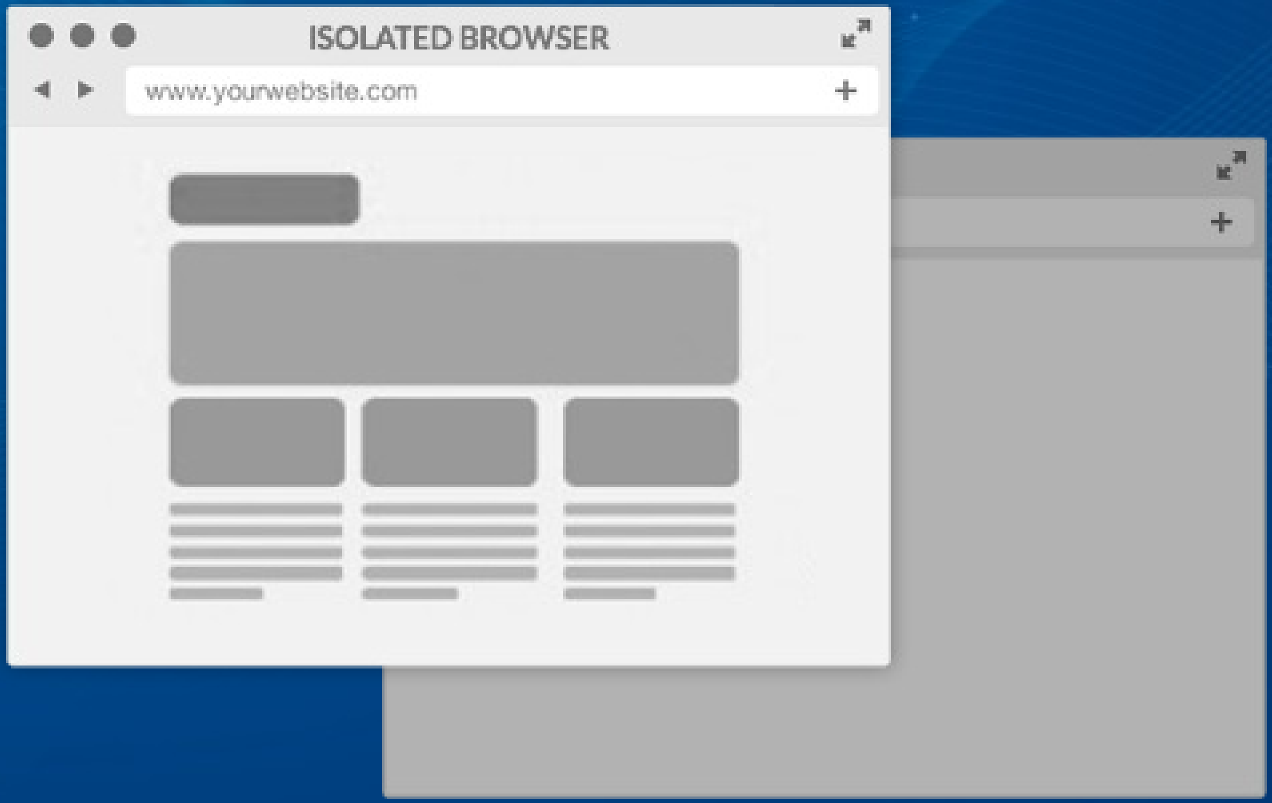
Deploy browser configurations and security policies



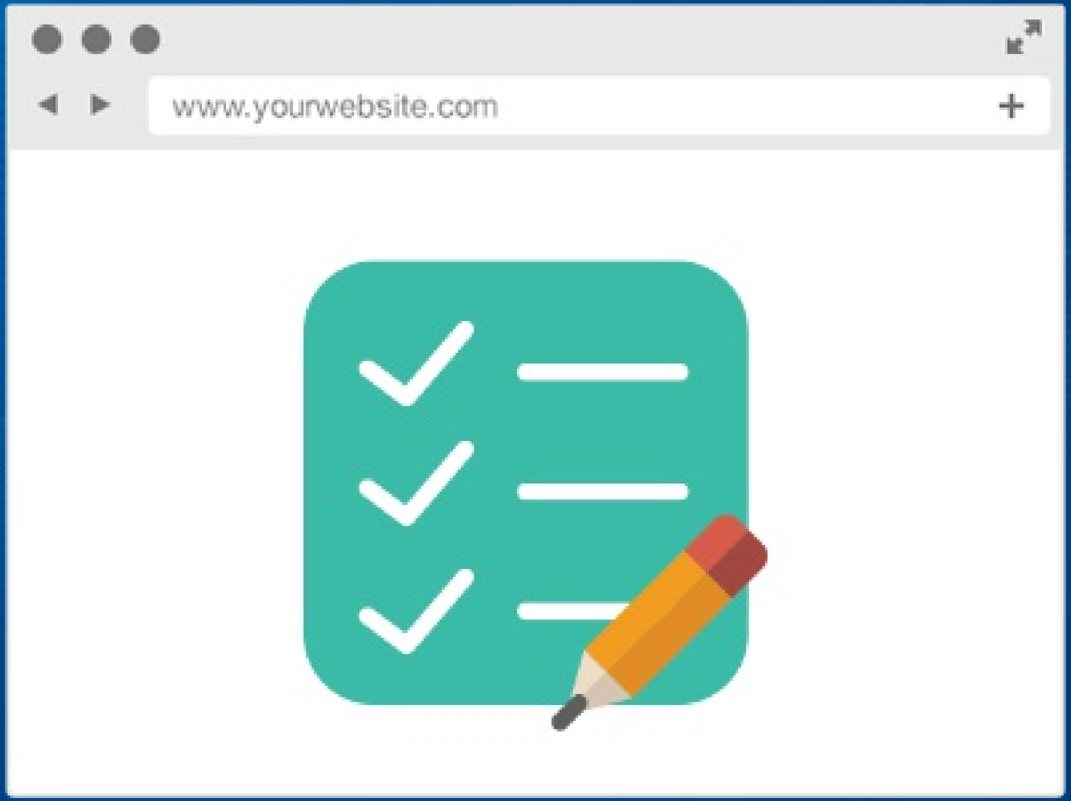
Manage and control browser add-ons



Isolate browsers: Render untrusted sites in a virtual browser



Ensure compliance to STIG, CIS and self imposed standards

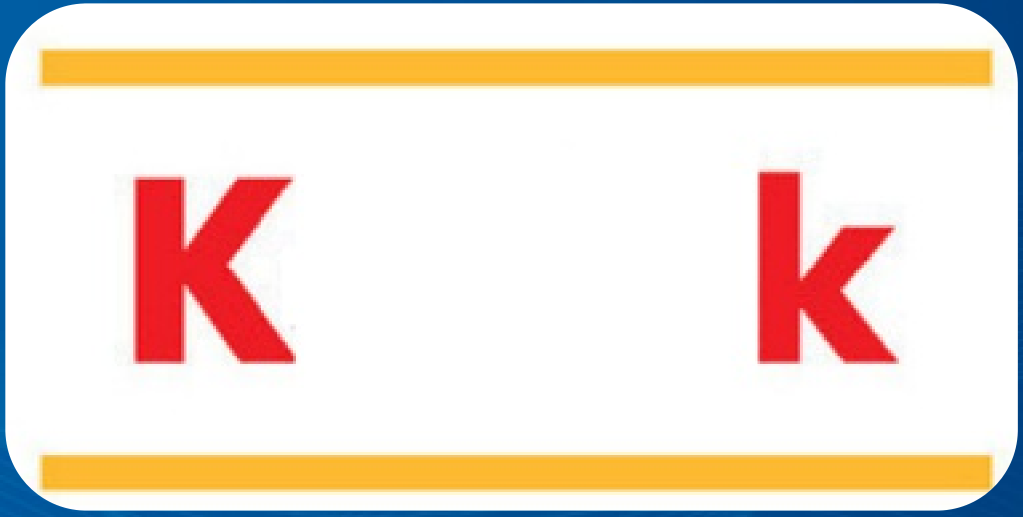


Conclusion

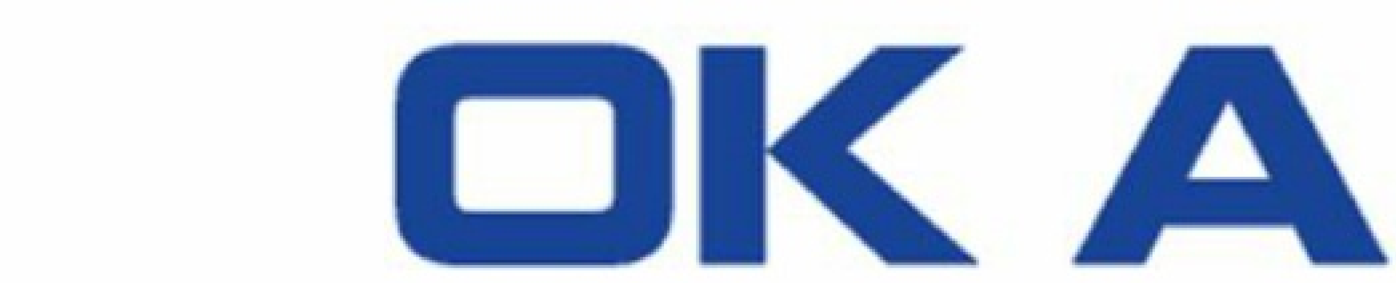
By managing browsers the same way endpoints like desktops and mobile devices are managed, enterprises can seal their network from possible attacks at its most used threshold.

And a free edition supporting
25 devices for ever

Mobile Device Management


K k

Y o!®


OK A

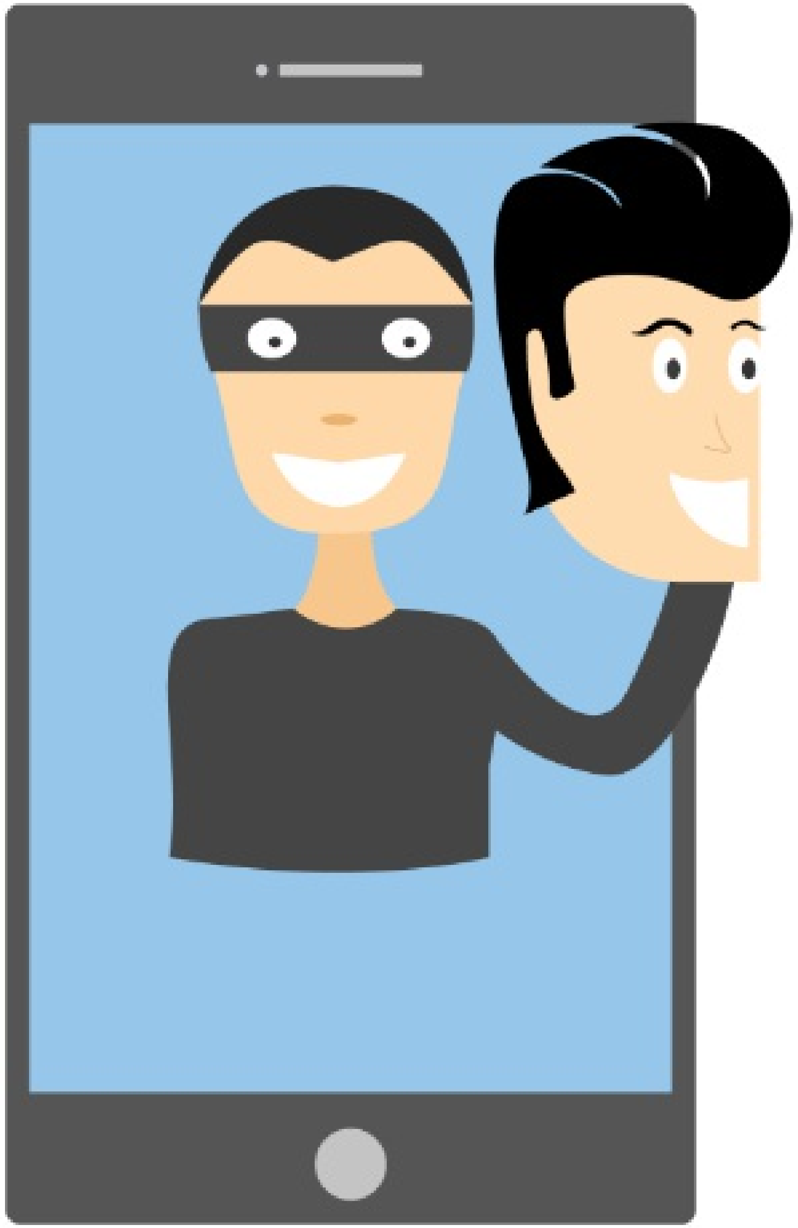
We aren't a mobile-first/mobile-only enterprise so why do we need MDM?

Do you..

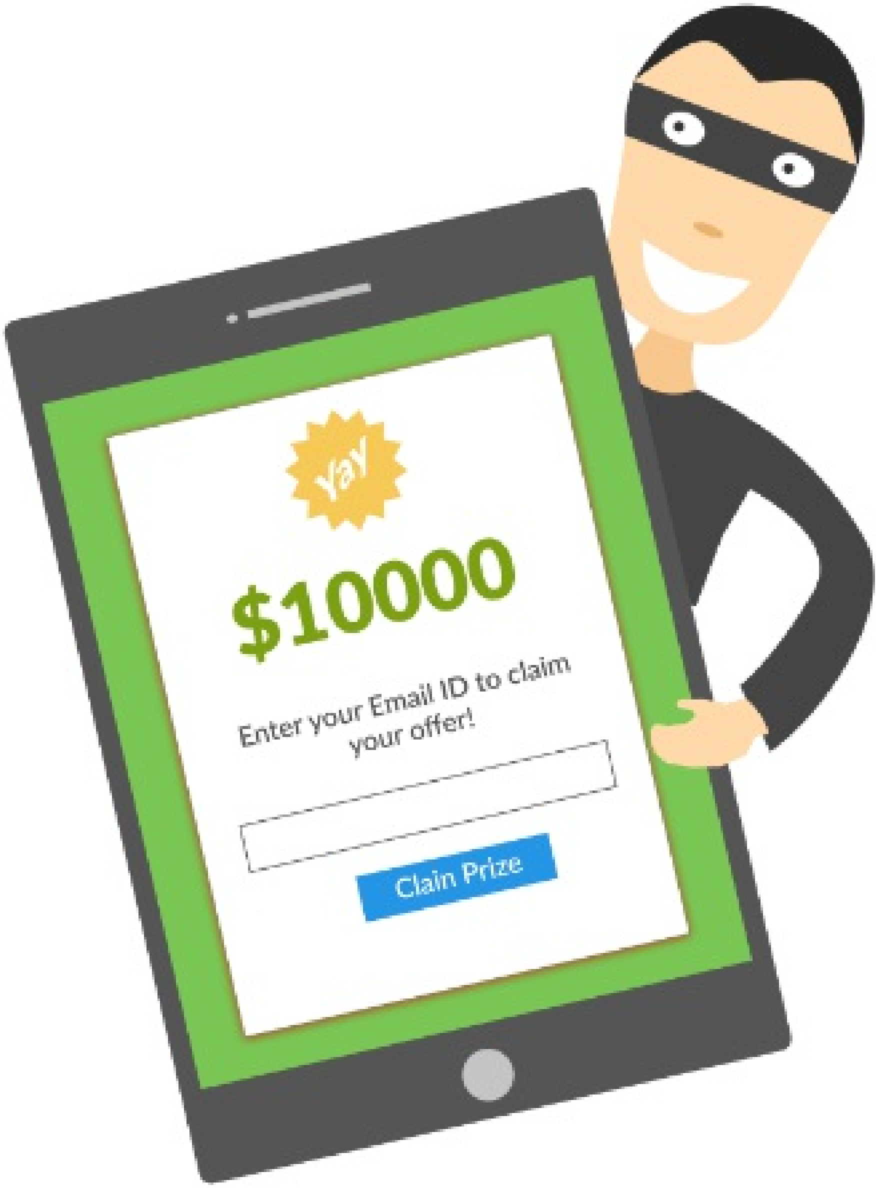
- occasionally use a mobile device at work - either personal or corporate?
- need mobile clients of SaaS products for your tasks?
- have e-mail, calendars etc,, configured on your device?

DATA PROTECTION
CRYPTOMINERS
CYBERWARS
SAAS PRODUCTS
DATA PROTECTION
SAAS PRODUCTS
CLOUD SERVICES
DATA SAFEGAURD
CYBERSECURITY
PHISHING
CYBERATTACKS
RANSOMWARE
DATA PROTECTION
CYBERWARS
DATA SECURITY
CYBERATTACKS
CYBERATTACKS
MALWARE
DATA SAFEGAURD
SAAS PRODUCTS
MALWARE
CYBERSECURITY
CYBERWARS
CRYPTOMINERS
MOBILE SECURITY
RANSOMWARE
SAAS PRODUCTS
MOBILE SECURITY
MALWARE
CLOUD SERVICES
CRYPTOMINERS
CYBERWARS
MALWARE
RANSOMWARE
RANSOMWARE
CYBERSECURITY
MOBILE SECURITY
DATA SAFEGAURD
DATA SECURITY
SAAS PRODUCTS
MALWARE
PHISHING
CLOUD SERVICES
MOBILE SECURITY
DATA SAFEGAURD
CRYPTOMINERS
CYBERATTACKS
CYBERSECURITY
MALWARE
DATA SAFEGAURD
MALWARE
PHISHING
MOBILE SECURITY
CLOUD SERVICES
CRYPTOMINERS
CYBERWARS
PHISHING
CYBERWARS
PHISHING
RANSOMWARE
CYBERATTACKS
PHISHING
MOBILE SECURITY
RANSOMWARE
CYBERATTACKS
CYBERSECURITY
CLOUD SERVICES
DATA SECURITY
DATA PROTECTION
PHISHING
CRYPTOMINERS
CLOUD SECURITY
DATA SECURITY
CRYPTOMINERS
RANSOMWARE
MOBILE SECURITY
PHISHING
MALWARE
CLOUD SERVICES

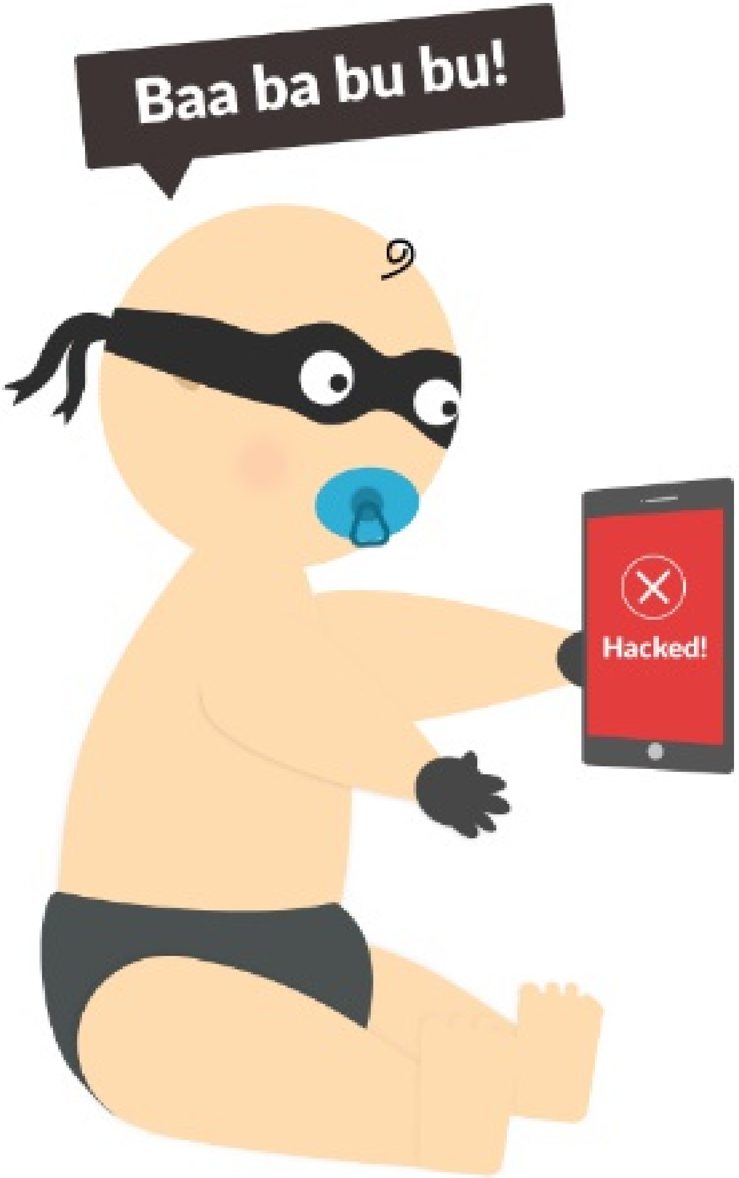
Data Theft



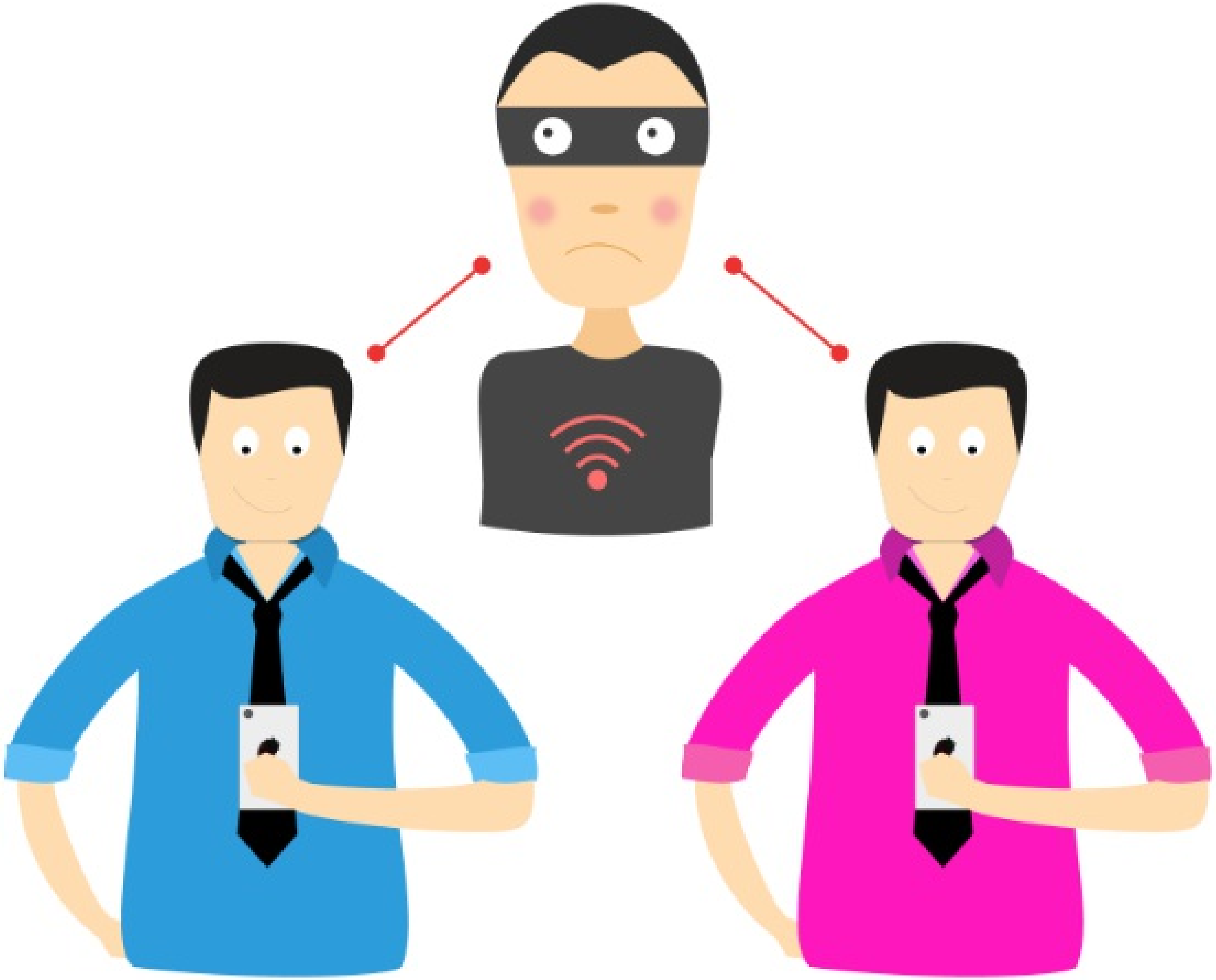
Social Engineering



Outdated devices



Wi-Fi Interference



Physical Theft

Introducing Mobile Device Manager Plus

PLATFORMS SUPPORTED

ANDROID

IOS

WINDOWS

mac OS

tvOS

CHROME OS

DEVICE TYPES

- SMARTPHONE
- LAPTOP/DESKTOP
- TABLETS
- TELEVISION
- IPODS

INTEGRATIONS

SPICEWORKS

SERVICEDESK PLUS

ZOHO CREATOR

ZOHO CRM

DEPLOYMENT METHODS

ON-PREMISES

CLOUD

DESKTOP CENTRAL ADD-ON

EDITIONS

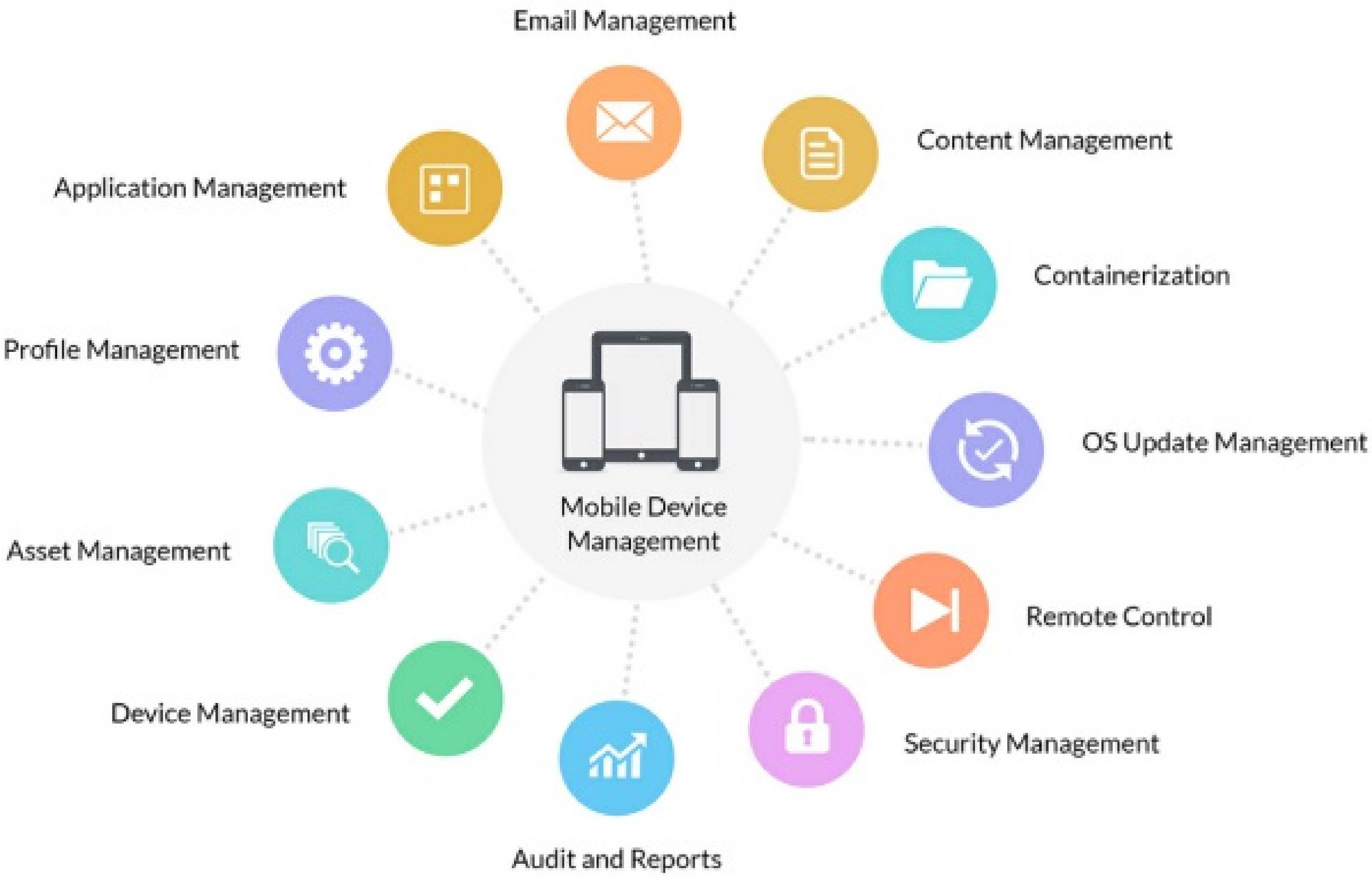
STANDARD

PROFESSIONAL

PATENT

LOST MODE USING SMS COMMANDS

Feature highlights



Real time scenarios

Scenario 1

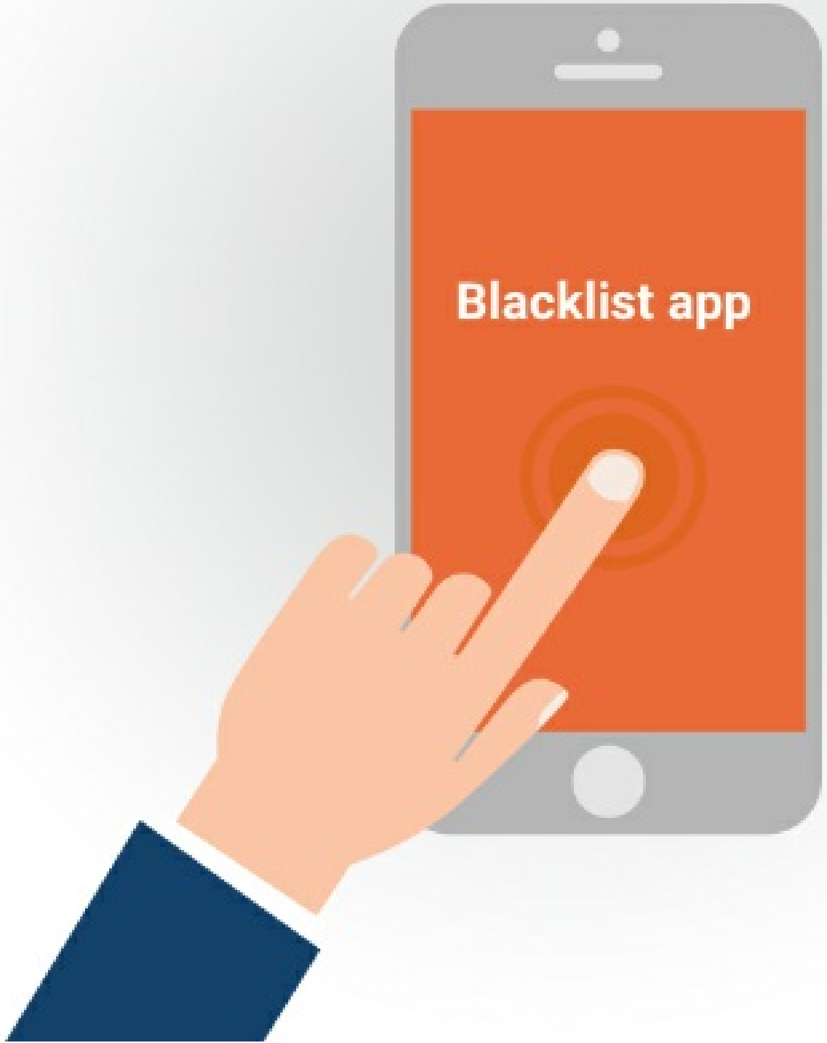
Prevent access to malicious websites

Scenario 2

Seamless installation of apps

Scenario 3

Blacklist specific apps. Example: Dropbox



Scenario 4

Securely share and view the confidential documents

Scenario 5

Handling a lost device

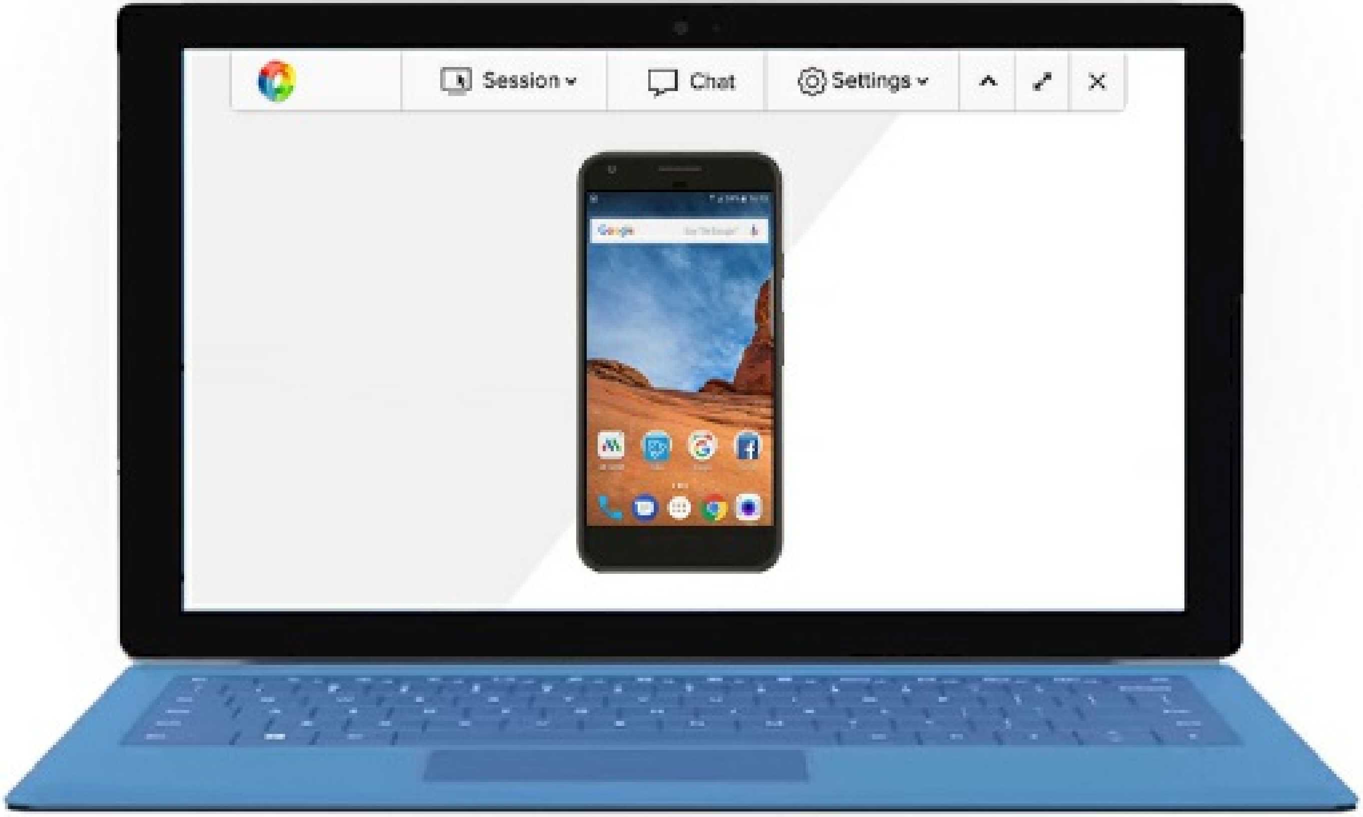
Scenario 6

Make a device use a single app. Example: Uber

Real world scenario

Scenario 7

Accessing the device remotely



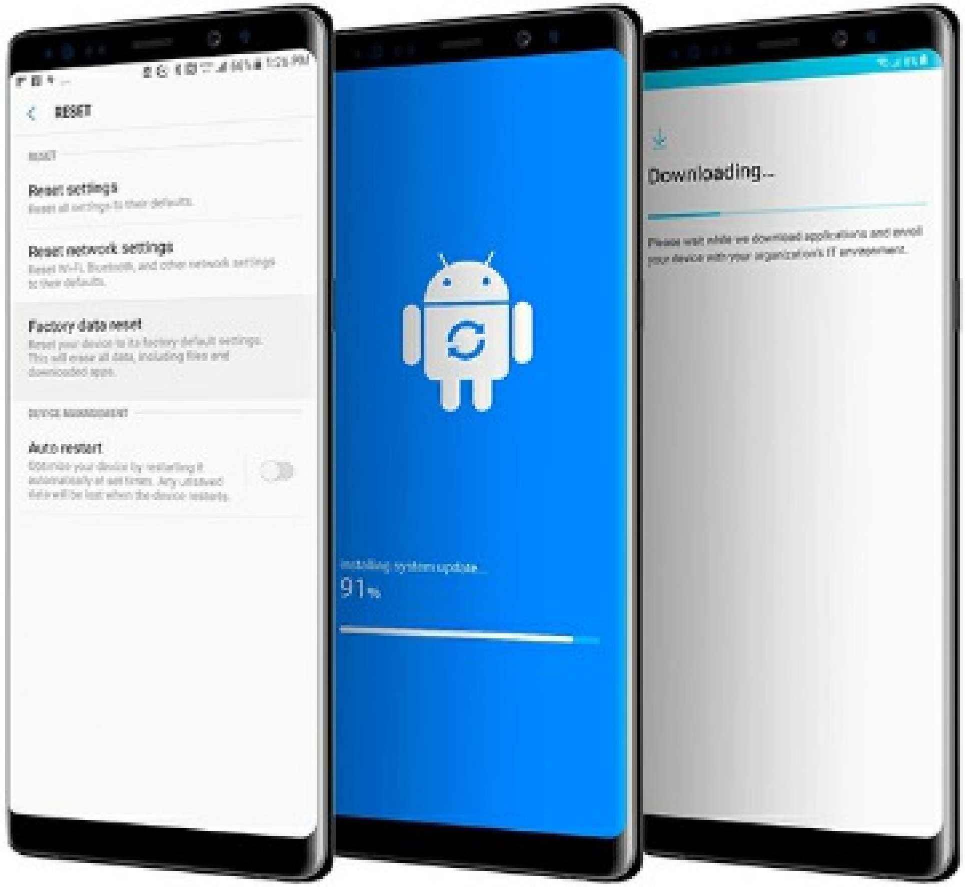
ManageEngine

Scenario 8

Schedule OS updates

Scenario 9

Enroll devices quickly



RESET

RESET

Reset settings
Reset all settings to their defaults.

Reset network settings
Reset Wi-Fi, Bluetooth, and other network settings to their defaults.

Factory data reset
Reset your device to its factory default settings. This will erase all data, including files and downloaded apps.

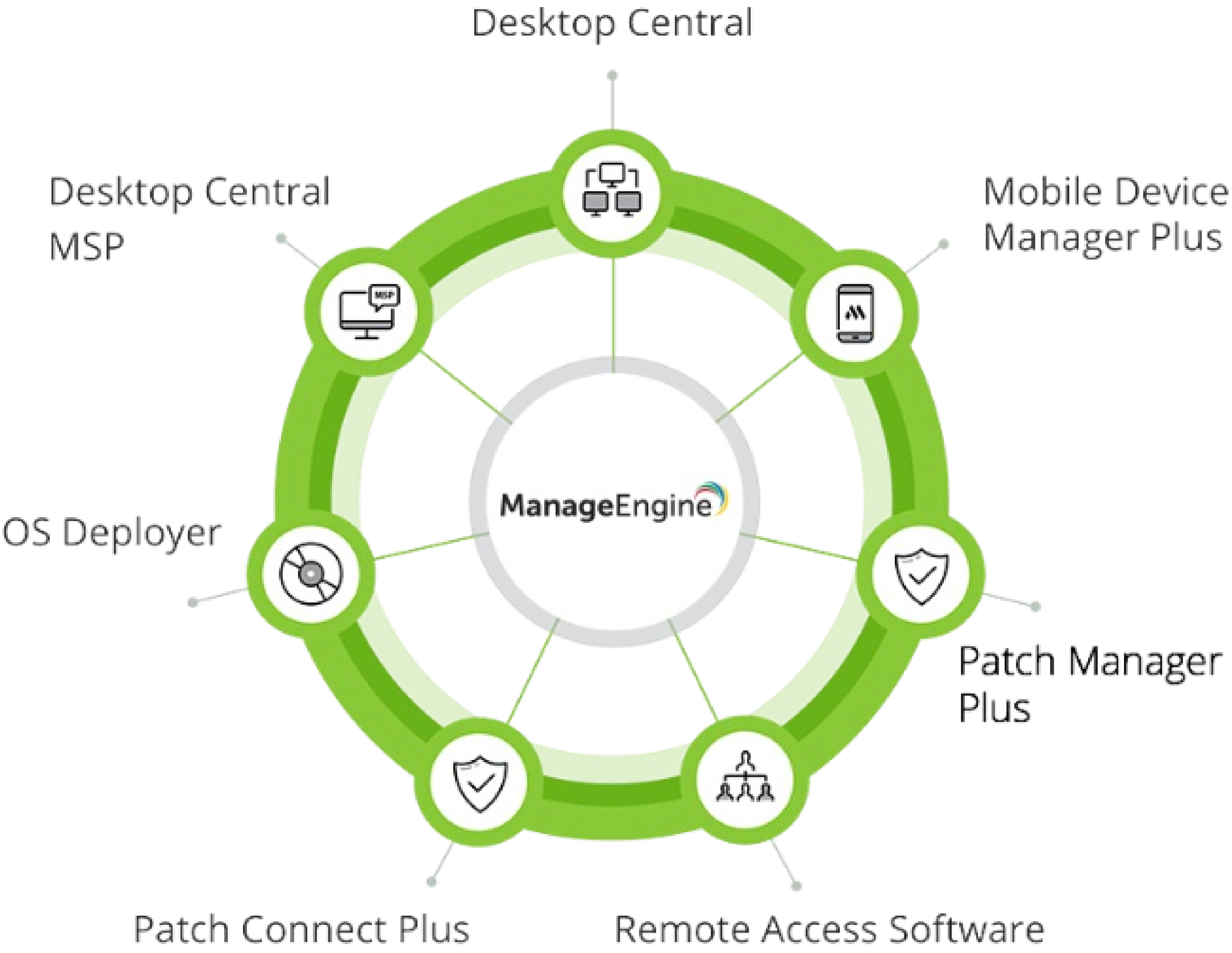
DEVICE MANAGEMENT

Auto restart
Optimize your device by restarting it automatically at set times. Any unsaved data will be lost when the device restarts.

Installing system update...
91%

Downloading...

Please wait while we download applications and enroll your device with your organization's IT environment.


Desktop Central
Desktop Central MSP
Mobile Device Manager Plus
ManageEngine
OS Deployer
Patch Manager Plus
Patch Connect Plus
Remote Access Software

Questions

Thank you

ManageEngine

www.manageengine.com