Corrata

ENTERPRISE MOBILITY CONTROL

Visibility and Control for Mobile Devices

ABOUT CORRATA

THREAT DEFENSE AND USAGE CONTROL FOR MOBILE DEVICES

Award winning software provider

Headquartered in Dublin, Ireland

Significant traction with enterprise customers

Partnerships with EMM vendors and device manufacturers

Recognition from analysts and practitioners

Team with exceptional track record in mobile

Backed by leading venture/angel investors

TECHNOLOGY PARTNERS

MobileIron

vmware airwatch

SAMSUNG

CITRIX

Microsoft

IBM

INDUSTRY RECOGNITION

Gartner

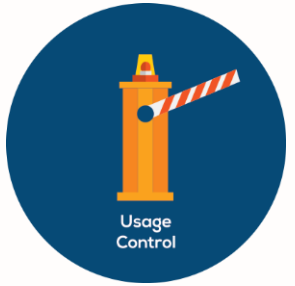
DEVICE VISIBILITY AND CONTROL FOR IOS AND ANDROID

THREAT DEFENSE

Protect devices and users from threats with real-time visibility and control over all device traffic

SECURITY STATUS

Assess security status of devices by combining configuration information with network behavioral data



CONTENT FILTERING

Block access to malicious and inappropriate content and high bandwidth applications

APPLICATIONS

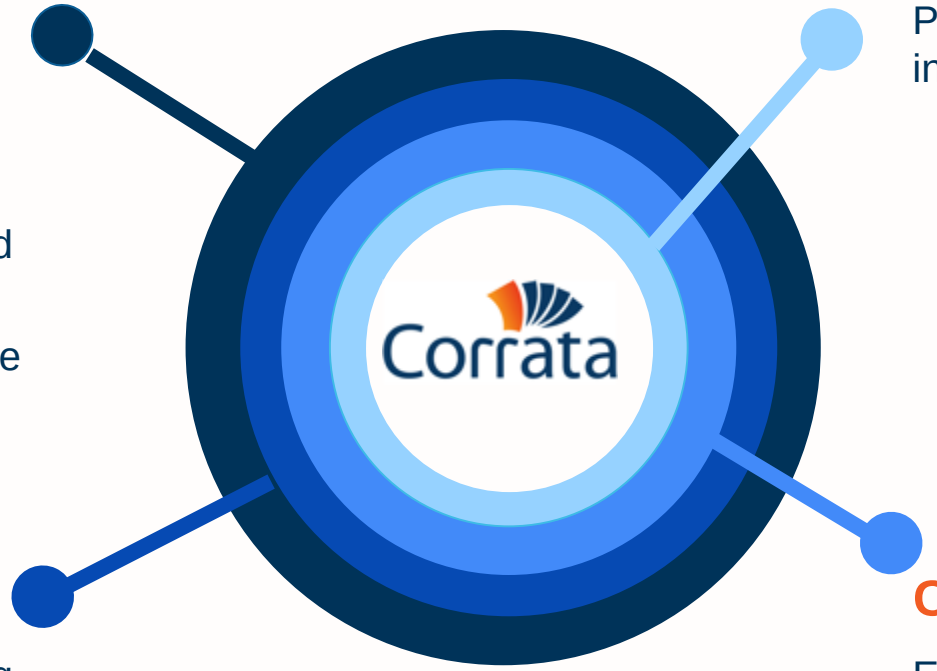
MOBILE SECURITY

Prevent phishing attacks and malware download

Identify at risk and compromised devices and infrastructure

Rapid response to newly discovered threats

Visibility of activity across your entire device estate



ACCEPTABLE USE

Prevents access to malicious and inappropriate content

COST REDUCTION

Reduce mobile data costs by cutting consumption of high bandwidth non business content

COMPLIANCE

Enforces compliance with policies on usage of SaaS and cloud storage

BENEFITS OF ON DEVICE TRAFFIC CONTROL

FASTER, MORE RELIABLE CONNECTIVITY

No change to how data gets to and from the device, no additional networking complexity

MORE SECURE, MORE PRIVATE

No compromise to the security of enterprise data or the privacy of employee content.

MORE TRAFFIC, MORE BEARERS

All protocols, all ports, http and non http traffic, Wi-Fi and Mobile

TODAY'S MOBILE THREAT LANDSCAPE

Clear range of threats which must be defended against

Today Smartphones and tablets represent 60% of all connected devices

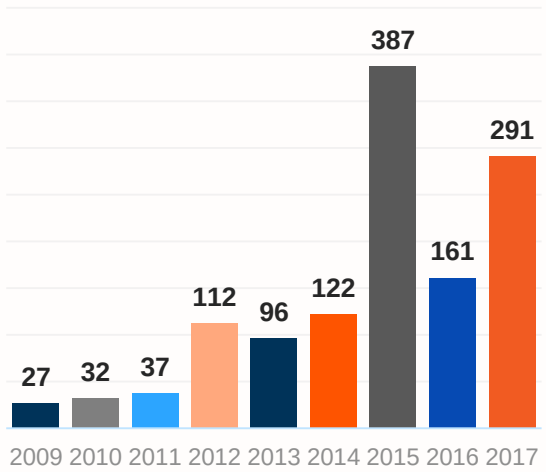
Large numbers of vulnerabilities continue to be discovered in both Android and IOS

Multiple infection paths: app stores, sdks, sideloaded apps, mms, bluetooth, Wi-Fi

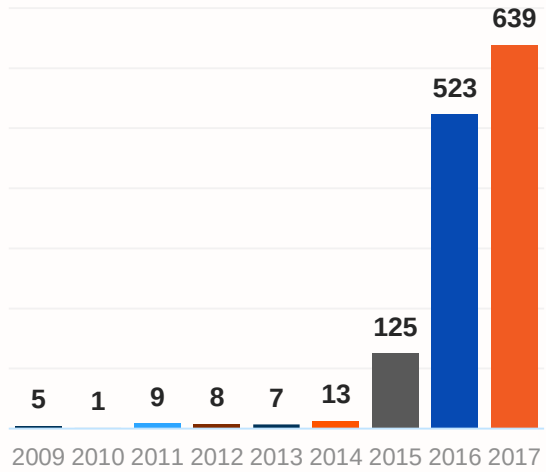
Mobile malware growing over 100% year on year

Multiple channels for mobile phishing attacks: email, sms, social media, mobile apps

Wi-Fi is and will remain fundamentally insecure



IOS Vulnerabilities by Year



Android Vulnerabilities by Year

Sources: AV Test report,

SOLUTION


THREAT
DEFENSE
SECURITY
STATUS
DATA USAGE
CONTROL
CONTENT
FILTERING

MOBILE THREAT DEFENSE

Protect against known or newly discovered threats

Protect against the full range of phishing attacks on mobile: email, sms, social media, app based

Filter malicious sites and content

Prevent downloads from unofficial app stores

Immediate blocking of newly identified threats including CnC infrastructure, malicious SDKs and malware

Search for Indicators of Compromise

Regular updates based on the latest threat intelligence

Investigate and respond to new discovered attacks

Integrate with SIEM

TECHNOLOGY

Hackers Hide Cyberattacks in Social Media Posts

By SHEERA FRENKEL MAY 28, 2017

SECURITY STATUS

Detect at risk or compromised devices and infrastructure

Real time monitoring of security sensitive device settings

Reporting of malware infection

Patch and security update status

Analysis of device behavior to detect previously unidentified threats

Integration with EMM for device quarantine

Protect against insecure Wi-Fi by monitoring encryption status of sensitive applications

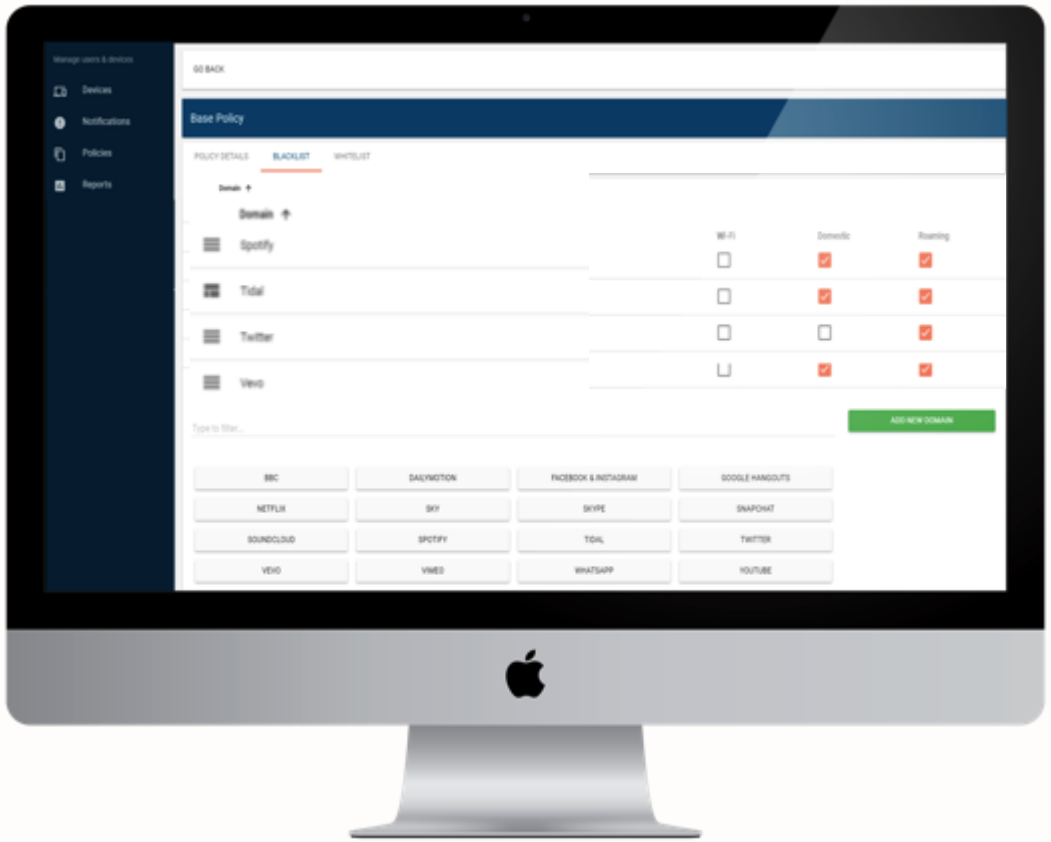
USAGE CONTROL

Enforce data use policies tailored to the needs of your organization

Set per device caps on domestic and roaming usage for individuals and/or groups

Whitelist business critical apps i.e. allow usage even when cap is reached

Blacklist high bandwidth non business applications such as social media or video streaming services



CONTENT FILTERING

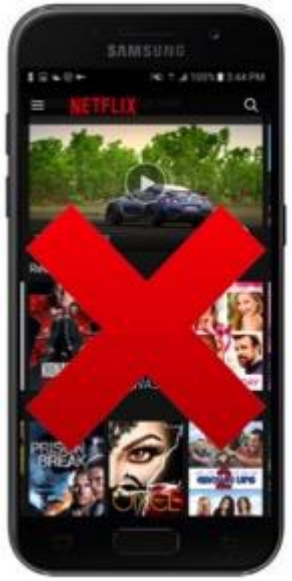
Ensure compliance with acceptable usage policies

Filter access to inappropriate content

Protect end-users against phishing and other malicious sites

Block usage of unapproved cloud services

Prevent usage of high bandwidth non business apps over cellular connections



VIDEO STREAMING

PHISHING SITE

INAPPROPRIATE CONTENT

HOW IT WORKS

ENROLL DEVICES

Application is downloaded from App Store to configure device and provide end user functionality

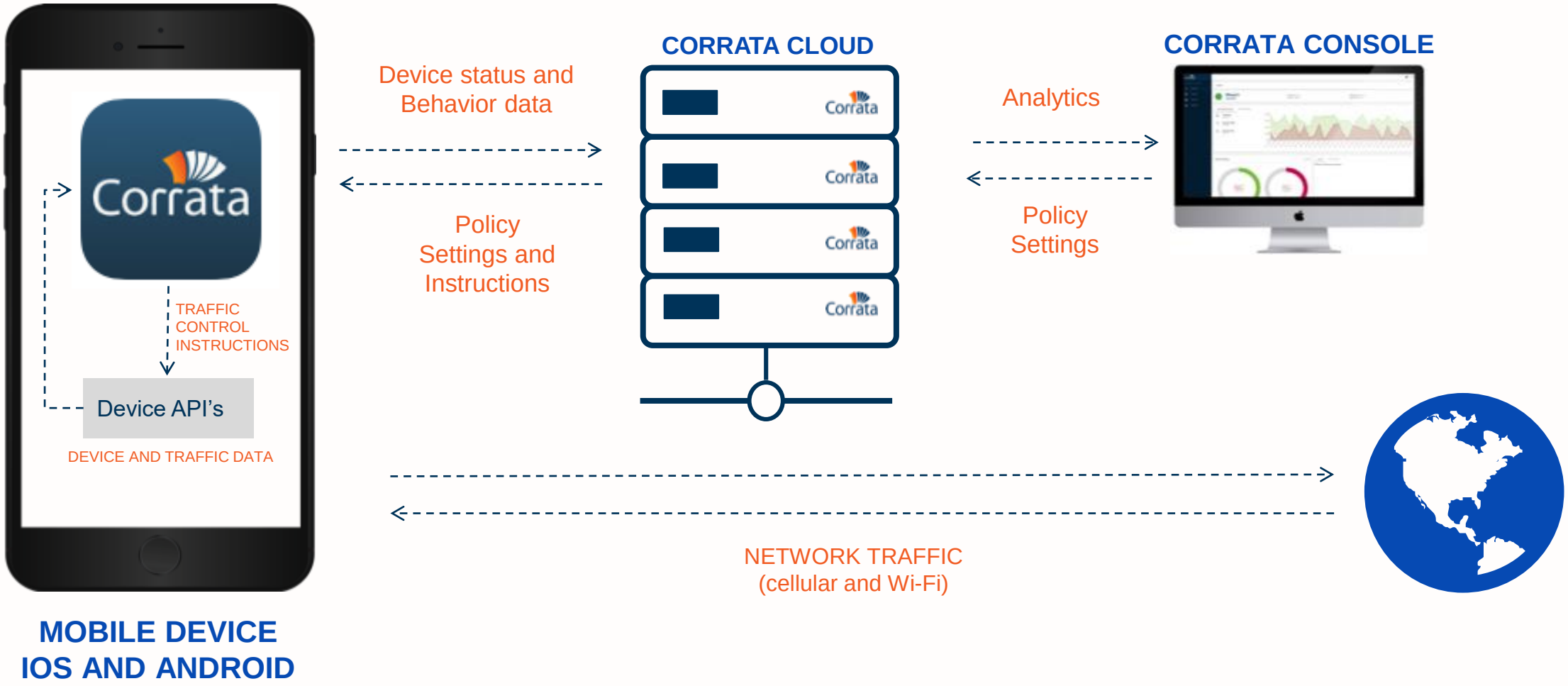
APPLY POLICY

Policy rules are applied on device blocking traffic to/from malicious sites, CnC servers, harmful apps, unofficial app stores, inappropriate content etc

MONITOR & CONTROL

Cloud component enables monitoring of end-point security status and control of on device agents

TECHNOLOGY OVERVIEW



CUSTOMER SUCCESS

Corrata’s customers cover a variety of verticals and organization size

END

web: www.corrata.com

e-mail: info@corrata.com