Playbook
Mobility

Elevator Pitch: Enterprise deployment of smartphones and tablets has now become the standard business practices and a critical component to stay competitive and maintain agile workforce. Extending enterprise content security to smartphones and tablets is now a key requirement without which employees cannot use these devices securely or inadvertently expose the corporate network to malware and attacks. Blue Coat ensure the secure use of smartphones and tablets with enterprise grade solution that secures the use of these devices as well as overall enterprise network and assets.

What to Look For – Customer Pain Points

Smartphones leave a big hole in current risk posture

- Traditional AV and firewall security are not readily available for smartphones and available mobile security is not enterprise grade
- On-device security SW drains battery and degrades performance to the point of it being unusable
- Investments in Mobile Device Management (MDM) solutions do not block malware or viruses and is not interoperable with many content security solutions

Increased liability from smartphone use in the office

- No enforcement of acceptable use policy
- Employees use 3G/4G cellular network and bypass corporate Wi-Fi for any blocked sites or downloads
- Even when employees connect to our corporate Wi-Fi, it's unclear whether existing infrastructure will secure against mobile threats
- The company could be liable in a lawsuit if employees are exposed to unacceptable content accessed on a enterprise issued device

Employees demanding use of apps we cannot secure

- Unlike the use of browsers, we don't have enterprise level secure for Apps on iOS and Android devices
- MDM solution which enable installation or removal of apps are too intrusive – it is not realistic to uninstall Facebook App for example, across every device because of viruses posted on a particular Facebook page

Pressure to support BYOD, even with high risks

- Employees want choice in devices and complain if BYOD is treated similar to guest Wi-Fi where employees have access to Internet but not corporate resources
- Can't enforce installation of on-device security because devices are owned by the employees and not the enterprise

Customer Initiatives and Projects

Improve employee productivity

- C-level initiative to empower employees to use the device that offers the highest productivity due to employee personal adoption and preference
- Improve remote and field worker productivity with devices inherently designed to be mobile and get online using wide range of connectivity options

Standardize on Apps to streamline business

- C-level led initiative including development of Apps to simplify day-to-day operations and creation of Enterprise App store
- With simplicity of Apps, reduce cost of training employees on how to use 3rd-party applications
- Reduce license cost of 3rd-party SW applications
- Simplify management of "approved" app using enterprise App store

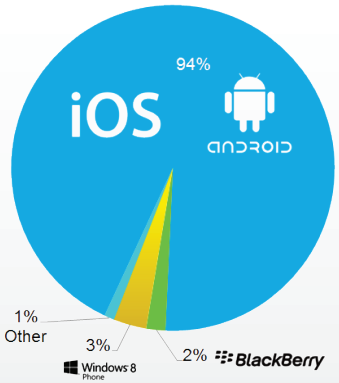
Reduce operational cost

- C-level initiative to replace manual/paper process and/or consolidate multiple devices for cost saving and simplified management
- Replacing paper documents and manuals with portable electronic device – Airline pilots, field sales team, field support team, etc.
- Consolidate multiple devices such as push-to-talk, barcode scanner, GPS navigation and database access to a single device – manufacturing, delivery service, restaurant service, etc.

BYOD Initiative

- Project led by various organizations including HR to improve employee satisfaction
- Project can also be led by COO/IT as a replacement to corporate issued devices resulting in cost savings
- CMO led BYOD project can be for purpose of brand promotion/recognition to differentiate from others in the industry

Smart Phone Units Shipped 2013



Best Practice Sales Strategies

Partner with MDM Vendors

- Many enterprise has already selected or in the process of selecting an MDM vendor. Partner with them and co-present the solution
- BC and Airwatch solution is the only integrated and comprehensive solution available for iOS
- In the case of Android device, Blue Coat MDS can be deployed by any MDMs; no special integration with MDM vendors is required

Mobile Security as an Extension of Enterprise Security

- Blue Coat mobile security solution leverage the same security analytics (WebPulse) as on-premise appliances – all enterprise-grade security
- Current BC customers can benefit from the same policy enforcement, URL categorization and malware detection they are familiar with on ProxySG

Cannot Have an Enterprise Smartphone Rollout Without Security

- If enterprise have already rolled out smartphone support w/o content security, they are already behind
- Many enterprise are delaying smartphone/tablet rollout specifically due to security. BC mobile security solution will enable the rollout

Playbook
Mobility

How Does the Blue Coat Mobility Device Security Service Support the Enterprise?

Device
- iPhone and iPad
  - iOS v5, v6 & v7
- Android Devices
  - Android 4.0+

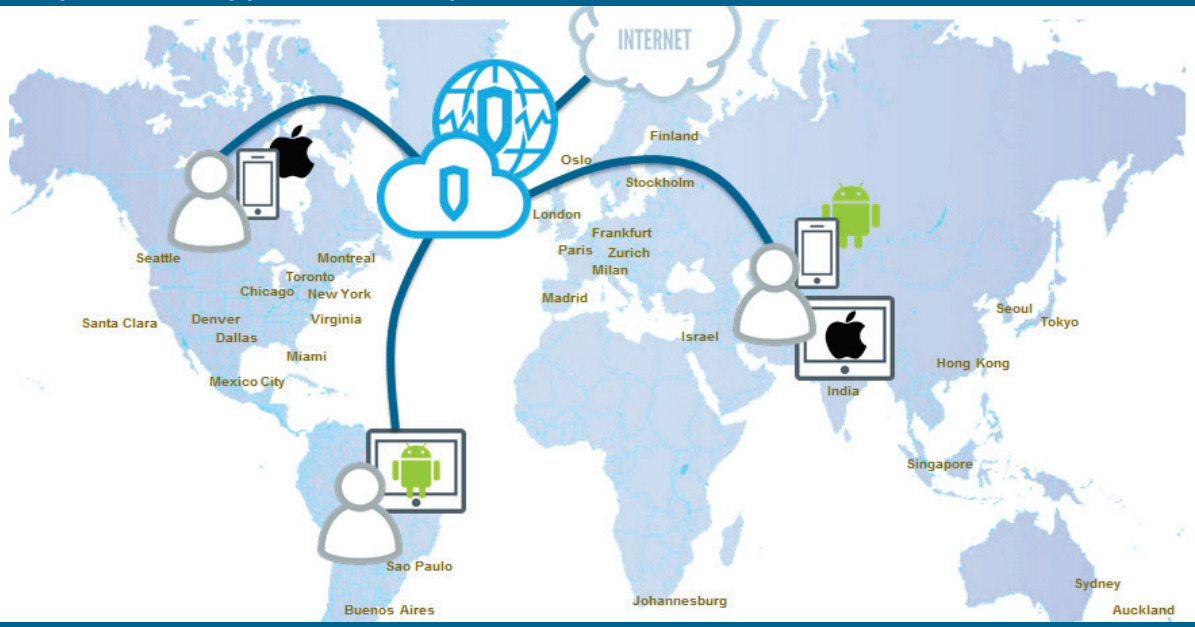
Connection to BC cloud
- Encrypted IPSec

App Controls
- Web Application
- Mobile Browser App
- Native App
- Operation Control

Security
- WebPulse
- Negative-Day Defense
- URL Filtering
- Real-time Analytics
- 2-stage AV

Reporting
- Cloud-based
- On-premise

Policy Management
- Policy Sync



Qualifying Questions

What security initiatives are you considering to support smartphones and tablets to protect the enterprise? Budgets and deadline goals?

How do you secure the use of apps that are being used on smartphones and tablets?

What steps have you taken to secure smartphones or tablets when connected to 3G/4G or some network other than corporate Wi-Fi?

Discovery Questions

Smartphones degrade risk posture
- Which smartphones or tablets (iOS or Android-based) are issued to employees?
- How do you secure the use of smartphones and tablets by your employees against malware and viruses?
- What plans do you have or have you already implemented a MDM solution to manage tablets and smartphones? If so, how does the MDM solution interoperate with content security solutions?

Increased liability from smartphones
- What Acceptable Use Policy(ies) are you able to enforce today when employees are using any corporate devices within the office?
- Can you enforce AUP on smartphones and tablets when used in the office?
- How do you enforce AUP when employees use 3G/4G instead of corp WiFi or leverage co-worker's mobile hotspot?

Employee demand for non-secured apps
- Do you have enterprise App initiative?
- How do you ensure your employees do not inadvertently download malware or viruses via native apps?
- What limitations are you able to put on the use of particular Apps for security reasons, short of uninstalling the App?

Pressure to support BYOD
- What BYOD initiative are in the works or planned for the near future?
- How are corp resources enabled from an employee's personal device?
- How do you ensure the personal devices do not spread malware or viruses in corp network?
- What complaints do you hear when you propose limiting access to corporate resources from personal devices?

Playbook
Mobility

Cloud Customer Success	
Santander CONSUMER	• Only solution with Negative-Day Defense • Long-term vision and continual expansion of datacenters (30+)
ignition GROUP	• Hybrid Management and Reporting • In-country Datacenter • Multiple connectivity option to the cloud
Beal Bank	• Multi-dimension Category • Dual AV scanning included in the cloud • Hybrid model – Policy Synchronization
Celanese	• On-premise and SaaS solution offering from single vendor • Simple integration with other solutions
WIPRO	• Global coverage and high performance • Robust and consistent security across all products and service via WebPulse
cbp	• Hybrid deployment benefit with consistent features from both on-premise appliance and cloud service
ATS American Traffic Solutions™	• Ability to inspect and secure HTTPS traffic • iOS support for iPhones and iPads
MULESHOE INDEPENDENT SCHOOL DISTRICT	• Comprehensive security service including AV • Malnet-Awareness • iOS support for iPhones and iPads

By Use Case	Value Measurement Questions (identifying cost of the problem)
Barrier to Deployment of Smartphones	• How urgently do you need to rollout smartphones along with the necessary security? • How would you rate the advantage your competitors would have if they rolled out smartphones today? • How long would it take you to catch up with them?
Only MDM Solution Deployed So Far	• How do you ensure users don't inadvertently "walk" viruses in to the office on their smartphone and inadvertently spread it? • How many man hours would it take to reimage infected systems? • How much of a delay would you expect if the content security solution you selected is not interoperable with your MDM solution?
Meeting Regulatory Compliance	• Would you be able to pass regulatory audit w/o quantifiable security solution deployed for smartphones and tablets? • Would you be able to show reports to "prove" all users and devices (including smartphones) are in compliance? • What would be the impact to the business if you fail regulatory audit due to the security (or lack there of) for smartphones and tablets? • How much man hour would you save if you had a tool that can generate reports on all users (in the office, remote PCs as well as smartphone and tablet) users?
Granular App Controls	• Would you be able to limit the use of Apps if it's uncovered that users were being lured to download malware/virus? • How many man hours would you save if you could simply limit App operations so other smartphones would not download and spread the same virus? E.g., temporarily suspend download operations from online storage sites.
Employee Sat	• Can you market your organization as one who provide high employee sat by enabling employees to use their device of choice? • How much brand recognition and competitive advantage would you be able to garner?

20% reduction in exposure to mobile malware originating from web ads	Secure Android smartphones and tablets against over 300 different families of malware	Save IT resources by eliminating need for manual Blacklist with accurate categorization	Secure against all mobile attacks originating from mobile malware delivery networks

Playbook
Mobility

Handling Objections

We already have MDM deployed to "secure" smartphones and tablets

- MDM solutions can configure device and remote lock and wipe the device in case of theft or loss but cannot enable secure use of the device
- You need a security solution that can identify a malicious URL, malicious links posted on social media and block viruses from being downloaded

We deploy iPhones and iPads which are secure against viruses and malware

- iPhones and iPads can easily download and transmit malware viruses intended for the device itself or other systems based on different OS
- iPhone and iPad users can easily fall victim to attacks like scams, spams and identify thefts which can gather credentials to access and steal corporate intellectual property

We already deploy AV engine on smartphones

- On-device security like AV engine must sacrifice security for user experience hence many contents are simply not scanned leaving security gaps
- Varying connectivity throughput limit the timely downloads of signatures to the device

We deploy secure browser

- Traditional browsers only account for a small use case of typical smartphone and tablet users
- Comprehensive security must also secure the use of Apps installed on the device

We only enable whitelisted apps to be installed so don't need to worry about malware

- Whitelisted apps ensure the apps themselves are not malicious apps in disguise but they are still susceptible to download and transmission of viruses and malware if the end-user is lured to malicious user or site

Key Blue Coat Differentiators

WebPulse	Collaborative threat intelligence
Negative-Day Defense	Malnet-awareness enables security from malware and viruses even before the attack actually happens. Blue Coat is the only security vendor to identify and continually monitor malnets
Granular App Control	Granular App control is a requirement for mobile security and the ability to configure policies that span all types of apps (Web app, mobile web apps and native apps) is a key requirement for many enterprise. Coverage across all apps ensure no security gaps exist
Dual AV Engine	Blue Coat is the only security vendor that includes two inline AV scanning included in the service without additional cost
iOS and Android Device Support	Only Blue Coat offers support for both iOS and Android-based smartphones and tablets with same policy enforcement in the cloud
Fully Meshed Network	Blue Coat Mobile Device Security Service is based on a fully meshed, fully redundant cloud service ensuring uninterrupted service
Encrypted Connection to Datacenters	All connection from the smartphones and tablets to the nearest Blue Coat cloud datacenters are encrypted to ensure the highest level of security and confidentiality
ISO 27001 and SSAE 16 Certified Service	All Blue Coat datacenters are ISO certified and follows the strictest guidelines to ensure the security of the service and customer data with routine audits
MDM Integration	Only content security vendors to integrate with AirWatch to enable deployment of comprehensive iOS security to iPhones and iPads

Competitive Analysis	Blue Coat	F5	
iOS Global HTTP Proxy	✔	✔	✔
iOS VPN OnDemand	✔	✔	✗
Integration with MDM for iOS VPN OnDemand	AirWatch	✗	✗
Android IPSec VPN	✔	✗	✗
Device(s) per License	2	1	1
Universal Policy	✔	✔	✗
Datacenters	30+	15	44
Fully Meshed Datacenters	✔	✔	✗
ISO 27001	✔	✔	✗
SLA %	99.999	99.99	99.99
Inline AV	✔	✔	✔
Dual AV	✔	✗	✗
Web DLP	✗	✗	✔
Email Security	✗	✔	✔
Email DLP	✗	✗	✔
Bandwidth Control	✗	✗	✔
App Control	✔	✔	✔

How Customers Buy

New Customers

- Subscription-based per user
- Requires basic cloud service subscription
- Requires Mobile Device Security Service Add-on subscription
- Each license supports up to 2 devices per user
  - 2 device can be any combination of iOS and Android-based smartphones or tablets
- Support included in the subscription

Current Cloud Customers

- Purchase MDS Add-on subscription for number of mobile device users