Playbook
Trusted Applications

Elevator Pitch: Mobile, cloud and web applications are transforming technology. They hold the promise of rapid innovation, greater customer intimacy and increased productivity. This rapidly changing landscape creates new threat and data security challenges to the Enterprise. Blue Coat's Trusted Application Center allows the enterprise to manage applications and associated risk: identify applications, monitor usage, quantify risk, enforce scalable policy control, accelerate performance and secure their critical data.

What to Look For – Customer Pain Points

Shadow IT – cloud and mobile – creating fear around data security and malware

- Individual employees and orgs outside of IT and using mobile/ cloud apps in the workplace without IT consent
- Data security risk – employees may be placing company data in unsecure cloud storage services
- Applications are very promiscuous – tracking location, using logins, accessing contacts and storing critical information outside of company control. There are too many to manage
- Usage of mobile devices introduces huge new network impacts from OS, app and content downloads
- Example: A large bank worried they cannot control file sharing (Dropbox, Evernote)
- Example: Design/manufacturing company scared that apps upload documents containing intellectual property

Risk of malware and data loss from "guest networks"

- BYOD and consumer apps introduce potential malware and acceptable use exposure
- Hospitals, universities, K-12, retail establishments and even insurance offices with retail locations, or any business that hosts large numbers of visitors
- Control malware and acceptable use; don't want "guests" or BYOD on corporate internal network

Fear that apps built for customers open up their data center to exploits and malware

- Projects to create or extend customer focused mobile/web applications create new vulnerabilities
- Apps for customers to use open up paths from the outside world into most protected data centers
- Applications for mobile and web require high levels of protection against malware and other exploitation

Customer Initiatives and Projects

General Enterprise: Mobile/Cloud Innovation and Shadow IT

- **CIO**: Leverage Mobile/Cloud to lower costs, increase speed of IT to meet new demands of the business
- **CSO**: Identify data leak and compliance risk from online storage and unauthorized applications/shadow IT. Establish governance for cloud and mobile apps
- **Data Security Architect**: Evaluate tools to report on usage of online storage and other cloud applications
- **Security Architect**: Deployed containerization (e.g., Good) and/or device level MDM protect corp data and devices. Now focusing on: 1) protect corp mobile against malware 2) open up network to consumer apps and BYOD devices
- **Network/Security Ops**: Provide insight into use of cloud and mobile apps; existing tools difficult to use, or don't provide a clean view

Higher Education/K-12 – BYOD

- **Chancellor/Superintendent**: Create open campus learning environment, enable research, and protect School or University reputation. CIPA reqs dictate K-12 students must be protected
- **IT Director/VP**: Enable dynamic mobile environment to diverse student/faculty
- **Academic Faculty/Students**: Focus on how apps and mobile devices are used securely
- **Security Architect**: Design secure network services that are open, yet maintain security that scales to support textbook to app transition
- **Network and Security Operations**: Respond to diverse demands of faculty and students, yet maintain effective operations

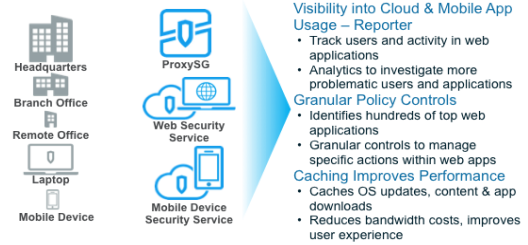
Retail – Guests in the Store

- **CMO**: Create a highly enriched "click and mortar" customer experience that leverages mobile apps and ties in massive user and demographic analytics for buying decisions
- **Network and Security Architects**: Enable business vision, assure security of environment, and with network performance to create superior user experience
- **Network and Security Operations**: Transparent technology that won't break apps and ensure the sheer number of apps don't create operational challenges

Customer: Financial Services – Customer Facing Apps

- **CMO**: Creating applications to get closer to customer (intimacy) and lower costs (bank from home)
- **Security Architect**: Designs how to protect the enterprise data/systems from this connection to the outside world
- **Security and Network Operations**: Implement the policy and protections, monitor ongoing operation, incidence response

See & Control Web Applications – Hybrid Proxy Solution



Best Practice Sales Strategies

Issues in SaaS and Mobile Apps position: ProxySG, Web Security Service, Mobile Device Security (MDS), with Reporter

- Discuss how TODAY our hybrid proxy model covers your network, guest networks and remote networks, with a large list of mobile/web applications, including to control over granular actions within Web Apps (e.g. flle uploads)
- Reporter provides visibility into who is accessing what type of applications – Dropbox, Facebook, as well as malicious and suspicious sites

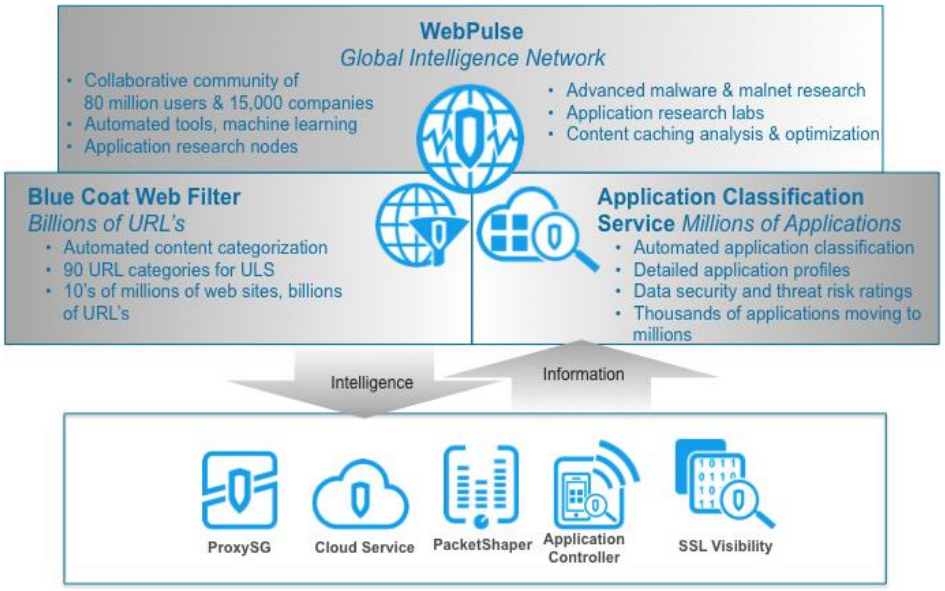
Extend Value with Emerging Application Classification Service (ACS) and Application Controller

- Position ACS as an emerging service to vastly expand coverage and intelligence of mobile and cloud apps, including highlighting data privacy and threat risks
- Communicate that the service will be available to ProxySG/Cloud in the future, but used first by Application Controller, a new all traffic, all ports product

Customer-facing Apps: Position ProxySG as Reverse Proxy with CAS/MAA and Security Analytics

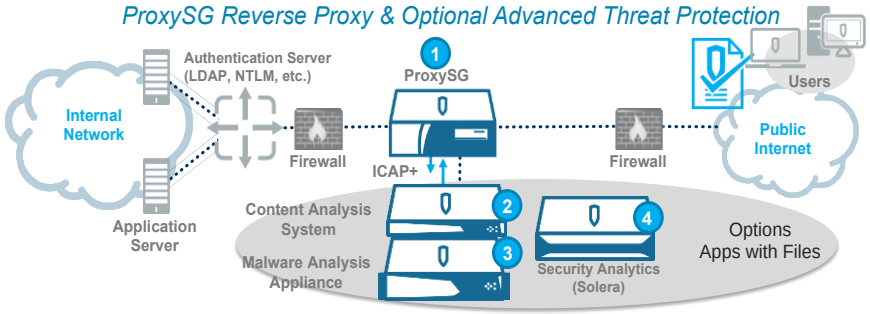
- ProxySG protects internal systems when Enterprises deploy customer-facing apps. Proxy processes connections from apps, rewrites URLs, caches content, sending files/data to CAS/MAA to assure no malware enters
- CAS scans files against known bad (AV) and known good (whitelisting), MAA analyzes for unknown malware
- Security Analytics is used to record transactions for any future investigations

Playbook
Trusted Applications



Protect Internal Infrastructure While Extending Web/Mobile Applications to Customers:

ProxySG Reverse Proxy & Optional Advanced Threat Protection



1. ProxySG proxies the external connection, serves content from cache to accelerate performance, rewrites URL's to protect internal data structures; Web Application Protections protect against injection attacks, cross site scripting and more…
2. For applications with inbound documents or files, ProxySG strips any files from the transaction, forwards to the Content Analysis System (CAS). CAS compares against known good (whitelist) & known bad (anti-virus signatures), sending results back to Proxy.
3. CAS can send unknown files to the Malware Analysis Appliance to sandbox for malicious behaviors.
4. The Security Analytics Platform can record entire transactions for later forensics analysis in case of breach.

Qualifying Questions

What cloud applications does your company rely upon? What risks do you see with employees accessing unsanctioned cloud and mobile applications?

In what ways are you leveraging mobile/cloud apps for customers to use? What challenges do you find in securing that data? What performance issues/impacts do you see?

How is your company addressing mobile devices? (Corp. and/or BYOD?) What is your mobile device strategy regarding access to your network? How do you secure mobile device data?

Discovery Questions

Mobility and Cloud Applications

- How is your company using mobile and cloud apps for innovation? What complexities has this added to data security and malware concerns?
- What cloud-delivered SaaS applications does your organization use?
- Which applications are users accessing outside of corporate standards? Corporate visibility? Security concerns?
- What do you use for application visibility?

Large "Guest Networks"

- How do you extend internet connectivity to guests? What protections do you have for malware and acceptable use exposure?
- What about employees who bring their own devices – to what network do they connect?
- What strategy do you employ to protect networks from malware for guests?
- Do you have different acceptable use policies for these networks compared to your internal?

Extend Customer Apps for Mobility and the Web

- In what ways have you/are you looking to create or extend customer-focused mobile/web apps?
- What vulnerabilities, risk and challenges does this create?
- How do you protect your data center environment from those outside connections?
- What files or are being uploaded into your data center from those apps?
- How do you ensure they are not malicious?

Playbook
Trusted Applications

Emerging Case Studies in Mobile/Cloud Adoptions

Large Bank

- Data security issues: they block cloud storage on Proxy, but want better visibility of usage, blocks and understand risks of various services
- Compliance issues: they lock down traders and brokers devices, but can't control personal devices (BYOD) are afraid of compliance risks

Unified School District K-12

- Have large number of tablets with controls configured…but student's hacked controls. Now need to monitor usage, enforce acceptable use block "bad" content to comply with CIPA and enforce "productivity policies" for students

Manufacturing Company

- Data Security to identify risky apps like Zoominfo that access and upload corporate contact repositories

Retail

- Want to track customer usage of apps in-store, to better understand pricing comparisons and to enable couponing and other targeted marketing

Case Studies in Reverse Proxy Deployment

Automotive Manufacturer

- Lease financing application is front ended with Reverse Proxy for protection. Check document submittals for embedded threats

Global Banks and Financial Services Companies

- Banking app deployed via mobile phones includes submittal of checks for deposit. We protect internal data structures by rewriting application URLs, provide sophisticated content forwarding policies, including ability to strip and scan attachments to prevent known and unknown malware from penetrating their data center

By Use Case	Value Measurement Questions
Shadow IT Risk – Mobile/Cloud/ Web App Visibility and Control	• How widespread is use of mobile and cloud applications in your environment? Do these increase data security and malware risk? • What are the potential costs/impacts of key intellectual property that are intentionally or mistakenly uploaded to public cloud resources? • What are the impacts of malicious or leaky applications accessing corporate data resources?
Innovation and Adoption of Mobile/Cloud Applications	• Does your current application and IT infrastructure meet all the needs of the businesses and employees, as quickly as required? • How would mobile and cloud applications lower costs and create a more flexible IT infrastructure? • What productivity and time to market improvements could be realized with more aggressive adoption of public cloud/mobile applications? • How would you measure and effectively manage the risk of new applications?
Extension or Deployment of Applications for Customer Use	• What benefits do you see from mobile applications that tie you closer to your customers? How would you increase revenue from understanding their habits better or making it easier to do business with you? • What costs could be reduced by moving more completely to web and mobile applications? • Given your focus on customers, what importance and protections do you put in place to make sure their data isn't stolen? How do these same applications that get you closer to them also open new vulnerabilities? • What benefits come from accelerated delivery of content and documents to the customers when they use those applications?
Accelerated Delivery of Applications for Employees and Customers	• Have mobile and cloud applications made their way into your corporate network? • How have networking capacity/costs network increased due to OS downloads, downloading of applications and updates, downloads of content? • How has contention for resources impacted your mission-critical applications?
Customer Applications Delivered in Store	• What sort of applications or content are you evaluating to enrich customers in-store/on-site experience? • How would video enrich? What about apps delivered on site? • How much would you invest in infrastructure to make that experience instant and rich?

Playbook
Trusted Applications

Mobile/Cloud App Competitive Analysis	Blue Coat	Palo Alto Networks	McAfee	Sky High Networks
Web and Mobile Application Definitions	✔	✔	✔	✔
Generate Source Information	✔	✔	✔	✗
Automated App Classification Service/ Categorization	✔	✗	✗	✗
Risk Ratings and Scalable Policy	✔	✔	✗	✔
All Ports, All Traffic Enforcement	✔	✔	✗	✗

Handling Objections

Mobile/Cloud Apps

We already deploy secure containers or MDM technology

- MDM are typically deployed on corporate-owned devices, do not cover BYOD scenarios. Virtual containers protect company data on the corporate or BYOD device, but do not protect corporate networks / servers from BYOD or Application access

We don't have active projects to accommodate "public apps" on corporate or BYOD devices

- MDM's have moved to a small "white list" model, but that limits adoption / innovation with mobile devices and apps
- Users leverage desktop apps, BYOA and corporate controls on desktop

Reverse Proxy	Blue Coat	F5	Radware	Imperva	McAfee
Complex Policy	✔	✔	✔	✔	✔
Caching	✔	✔	✔	✗	✗
Top 10 OWASP	✗	✔	✔	✔	✔
PCI Compliance	✗	✔	✔	✔	✗
File Stripping for Content Analysis	✔	✗	✗	✗	✗
AV & Whitelist Scanning	✔	✗	✗	✗	✔
Malware Analysis Sandbox	✔	✗	✗	✗	✔
Recording for Analytics Forensics	✔	✗	✗	✗	✗

Handling Objections

Reverse Proxy

We need more advanced protections

- While full Web Application Firewalls offer a broader suite of inline protections, any applications where files are submitted need to have those files analyzed for malware

We need load balancing as well, and can leverage the load balancing for other protections

- Blue Coat does not have load balancing functionality, but can be deployed in back of simple load balancers
- We provide very robust content policy language to protect internal systems, plus the ability to strip and analyze attachments for malware – both for known and unknown malware

Key Blue Coat Differentiators

Unified Policy and Reporting Across All Locations/Uses	While competitors have the ability to identify web applications and granular control of operations, Blue Coat is able to deploy across appliance, cloud and mobile cloud environments. This provides a unified policy construct that follows the user, and delivers comprehensive reporting users and applications no matter where they go
Detailed Reporting and Analytics on Web Application Usage	Reporting allows you to track usage of key application types like online storage and track who is uploading content. Analytic workflows can cross-correlate these users/behaviors to those accessing suspicious and malicious destinations, identifying your riskiest users that can lead to tighter policy control
Automated Application Classification Service Built to Scale	Many vendors identify applications, but Blue Coat is building an automated service to expand coverage to millions of applications. Drawing from experience of WebPulse. The Automated application service will provide "WebPulse like" technology for mobile application classification
Reverse Proxy – Advanced Policy	ProxySG has a very flexible policy language that works with the Proxy functionality to enable complex operation to protect Web Applications. Actions like rewriting URLs to protect internal data structures; applying special policy to IP addresses from risky countries; forwarding content based on policy rules. That flexibility creates a powerful security framework
Reverse Proxy – File/ Attach Analysis to Detect Known Malware	The ProxySG can strip files and content from application sessions and check against known malware signatures; in fact, we can check against two AV engines (customers choice) to protect against known malware
Reverse Proxy – Full Malware Analysis and Forensics for Unknown Threats	For files that are not known bad – and warrant additional analysis. We can sandbox those files to look for latent malicious behavior with the the Blue Coat Malware Analysis Appliance and/or record all transaction info. with the Security Analytics platform for identification of threats and/or later forensic investigation

Deployment Differentiators

Mobile and Cloud Applications – Existing and New Customers

- Current list of 300+ of most popular Web and Mobile Applications are part of the Blue Coat Web Filter product, no additional charges
- Reporter is an add-on product to analyze ProxySG logs, providing advanced reporting on Web Application usage
- Application Classification Service (ACS) is an add-on subscription that expands current list of 300+ Web and Mobile Applications to thousands – and adds risk indexes per application – in 2014. It will build towards millions in the future
- ACS will be available on ProxySG, but delivered first on the Application Controller
- Application Controller – the new all ports all traffic appliance – are currently available for qualified Beta participants

Protect Infrastructure with Proxy Reverse Proxy

- Reverse Proxy front ends application servers. It is simply a configuration of the ProxySG Proxy Edition product
- New capabilities like Web Application Protections, GEO IP are currently part of the Blue Coat Web Filter Subscription and embedded ProxySG functionality
- AV signature scanning and Whitelists are an add-on products ProxyAV or Content Analysis Sytek
- Optional sandboxing for unknown malware is a separate Malware Analysis Appliance
- Optional recording of transactions is fulfilled with a separate Security Analytics Platform