Endpoint Management and Security

How IBM BigFix, Mobile First Protect and Trusteer Apex Protect Endpoints against Exploits & Compromise

John Beal – National Security Saas Leader
Security Systems Software
jbeal@ca.ibm.com
Despite existing tools, breaches continue to rise

Lack of visibility and control contributes to security breaches and financial loss

"Major global bank compromised and millions of depositor records stolen due to missed server upgrade cycle"

$3.8M global average cost of a data breach*

You can’t fix what you can’t see

Incident response is the No. 1 factor to reduce the cost of a data breach

As Mobile Grows, Threats Grow

In 2014 the number of mobile phones (7.3 billion) will exceed the number of people on the planet (7 billion)^1.

138 billion apps were downloaded in 2014^2. By 2017 50% of employers will require BYOD^3.

Mobile malware is growing. Malicious code is infecting >11.6 million mobile devices at any given time^4.

Mobile devices and the apps we rely on are under attack. 97% and 87% of top paid Android and iOS apps have been hacked^5.
Siloed IT Operations and Security Teams

Disparate tools, manual processes, lack of integration and narrow visibility

IT SECURITY
- Scan for compliance status
- Create security policies
- Identify vulnerabilities

IT OPERATIONS
- Apply patches and fixes
- Implement security and operational policy
- Manual process takes weeks / months
Why Other Approaches Fail

**Architecture**
- Slow, scan-based architectures
- Limited coverage
- Not cost-effective at scale

**Complexity**
- Heavy, resource-intensive agent(s)
- Multiple products, multiple agents
- Not Internet-friendly

**Resources**
- Too much admin and infrastructure
- Little pre-built content
- Each task detracts from higher value projects
Perimeter defenses are not enough against today’s attack chain

1. Attacker phishes a 3\textsuperscript{rd} party contractor or employee

2. Attacker uses stolen credentials to access portals

3a. Attacker finds & infects internal unpatched or vulnerable file server

3b. Malware retrieves PI or sensitive data

4. Retailer POS systems

5. Malware sends CC data to internal server; sends custom ping to notify

6. Stolen data is exfiltrated to FTP servers

Internal network

Firewall

Windows/Linux file server

Attacker FTP servers (external)

Web portals
What any Unified Endpoint Management should address:

**Any device.**
Identify and respond to any device accessing your corporate data—regardless of what type it is or whether it’s personal or corporate-owned.

**Any location.**
Manage and secure every unique device—whether it’s on or off your corporate network—anywhere on the planet.

**Any time.**
Get real-time visibility and control of every device on your network. Find and fix problems in minutes—before they become major disruptions.
What an Endpoint Architecture should provide:

**Single intelligent agent**
- Continuous self-assessment
- Continuous policy enforcement
- Minimal system impact (<2% CPU, <10MB RAM)

**Single server and console**
- Highly secure, highly available
- Aggregates data, analyzes and reports
- Manages up to 250K endpoints per server

**Flexible policy language (Fixlets)**
- Thousands of out-of-the-box policies
- Best practices for operations and security
- Simple custom policy authoring
- Highly extensible/applicable across all platforms

**Lightweight, easily configurable infrastructure**
- Designate agent as a relay or discovery point in minutes
- Provides built-in redundancy
- Leverages existing systems/shared infrastructure
MobileFirst Protect: enabling devices, apps, and content

✓ Proven delivery approach with both on-premise and cloud-based EMM offering
✓ Securely enables mobile productivity without burdening end-user experience
✓ Seamlessly integrates with all of your existing infrastructure
✓ Simple & fast with an exceptional customer experience

Because of HIPAA issues regarding personal student information and records, the ability to remotely lock and wipe any lost devices provides an added layer of security to iPads used in therapy and other clinical settings. We feel confident knowing our devices are always secure.

~Beth Greer, Bancroft

Client: Bancroft

300+
Number of iPads used by clients and staff

15 - 20
Hours of monthly IT time saved

<5 Minutes
The amount of time to securely enroll a new device

300+
The number of educational and clinical apps managed

1
Number of consoles needed to securely manage all iPads
Mobile First Protect (Maas360) Differentiators

1) Overall Security Capability
   World Class Datacenters: FISMA, CSA, SOC 2 Type II Certified
   Encrypted Containers: AES-256 Bit, FIPS 140-2 Compliant

2) Our Architecture and Data we DON’T store is KEY!
   NOT introducing a point of failure
   Emails/Sensitive info not stored on our cloud

3) Ease of Use and Customer Experience
   Full Production Trial in minutes - Fastest to Try, Easiest to Buy
   No charge for support, implementation, training, maintenance

4) Strategic Partnerships
   IBM and Apple – July 2014
**IBM Mobile Portfolio**

- **IBM App Scan**
- **IBM Security Access Manager for Mobile**
- **Predictive Analytics**
- **Identity & Access Controls**
- **Secure Corp Access**
- **Event-based Compliance**

**Worklight** integration for increased security and app lifecycle management workflow value.

**Qradar** integration for bilateral real-time event notifications.

**Trusteer** to add additional threat protection capabilities to the MaaS360

**Collaboration Solutions (Lotus)** integration for increased user productivity and containerization.
Trusteer Apex - Turnkey Service

Low impact endpoint agent plus expert services

Global Updates

• New protections based on dynamic intelligence
• Transparent endpoint updates

Exception Handling

• Reduce false positives
• Whitelisting of known good apps and processes

Threat Analysis

• Analysis by an extensive team of APT experts
• Malware research
• Help with remediation

Policy Administration

• Initial policy creation
• Ongoing policy review
• Policy change management
IBM BigFix and IBM Trusteer Apex
Create the most robust enterprise endpoint security solution available!

- Extend BigFix ROI by stopping exploits before patches are available
- Continuously monitor and protect endpoints
  - Enforce secure configurations
  - Deploy security patches
  - Detect and mitigate advanced malware infections
- Effectively respond to security incidents

Apex stops zero-day exploits – protects in the window between attack and fix

Everyone goes back to work on higher value projects

BigFix Incident Response quarantines infected machines

BigFix enforces secure configurations

Patch available: BigFix ensures it is quickly deployed on all endpoints

Apex identifies and mitigates malware infections in real-time

IBM Trusteer Apex and IBM BigFix
Mobile Threat Management (Trusteer)

Stop mobile malware on iOS & Android devices
Set security policy controls against malware
Automate remediation with compliance engine
Alert user & responsible parties
Detect jailbroken & rooted devices with over-the-air updates
## Disrupting the Attack Chain

<table>
<thead>
<tr>
<th>Break-in</th>
<th>Latch-on</th>
<th>Expand</th>
<th>Gather</th>
<th>Exfiltrate</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Break-in Diagram" /></td>
<td><img src="image2.png" alt="Latch-on Diagram" /></td>
<td><img src="image3.png" alt="Expand Diagram" /></td>
<td><img src="image4.png" alt="Gather Diagram" /></td>
<td><img src="image5.png" alt="Exfiltrate Diagram" /></td>
</tr>
</tbody>
</table>

### ATTACK CHAIN

<table>
<thead>
<tr>
<th>Break-in</th>
<th>Latch-on</th>
<th>Expand</th>
<th>Gather</th>
<th>Exfiltrate</th>
</tr>
</thead>
<tbody>
<tr>
<td>QRadar correlates application, network and user activity; alerts on attempted and actual intrusions</td>
<td>Apex prevents malware from installing; QRadar/BigFix detect, prioritize and remediate vulnerabilities</td>
<td>QRadar detects abnormal traffic patterns on the network; alerts security personnel</td>
<td>QRadar detects user logins and database activity revealing abnormal access to sensitive servers</td>
<td>QRadar detects abnormal data transfer; Incident Forensics investigates attack; BigFix quarantines / fixes endpoints</td>
</tr>
</tbody>
</table>
IBM understands the demands of managing a global heterogeneous IT infrastructure

• **433,000 IBM employees** in over 120 countries.

• Deployment to over **750,000 endpoints**

• Drive savings well above our initial **US $10million estimate**

• **A 78 per cent decrease** in endpoint security issues

• IBM is also in the process of deploying IBM Endpoint Manager for Mobile Devices across its entire mobile workforce of over **120,000 staff**

• IBM Endpoint Manager is being deployed across many global outsourced accounts
IBM CIO Office on-boards 15,000 Devices the First Day After Deploying MobileFirst Protect

- 70,000+ users migrated in one month
- $500,000 projected savings due to migrating to SaaS
- 48,000+ users registered in 15 days
- 200+ users per hour* in first couple of days
- < 500 help desk calls – less than ½ of 1%

Be FIRST with IBM MobileFirst
Top issues

1. Establishing Real Time Compliance on Endpoints
2. Current tools were not designed for this onslaught of attacks.
3. When a Breach occurs, you could end up in the news!

What should I do?

1. Schedule a demo/trial: For Mobile we can turn your trial into production with a flip of a switch.
2. Get help from a well established vendor (many smaller companies go under)
Why IBM?

IBM’s Unified Device Mgt, is a UNIQUE solution in the market today

- True Cross platform solution: 90 supported OS’es: Unix, Linux, Mac, Windows and Mobile.
- Real Time Visibility and Control: distributed Intelligence. **This is NOT Scan and Poll!**
- 1 “Pane of glass” single console view for everything, across everything
- Untouched Scalability: 250,000 end points, 1 single management server.

Why does that matter? Who cares? And Why do we win?

- Whether server, desktop, or both: we typically replace 8-12 other agent based tools. Tool consolidation addresses: Silo management, visibility gaps, and growing costs of multiple tools (one customer has 62 different tools to manage servers)
- Unified Device Management is extremely lightweight and fast to deploy: services impact is light and predictable
- Customers continue to struggle with security Threats. IBM is the cure!

Incumbent systems can’t ‘see’ all endpoints – And Customers can’t fix what they can’t see!
For more information

www.unifiedendpointmanagement.com

https://twitter.com/IBMEndpoint

https://www.youtube.com/IBMEndpoint/playlists
Learn more about IBM Security

Learn more! Download the 2015 Cyber Security Intelligence Index

2015 Ponemon Cost of Data Breach

Download: IDC Canada: Determining How Much to Spend on your IT Security.
https://ibm.biz/IDCWPEN

Connect with our experts

Blog SecurityIntelligence.com

Follow us on Twitter @ibmsecurity