Life on the Edge point

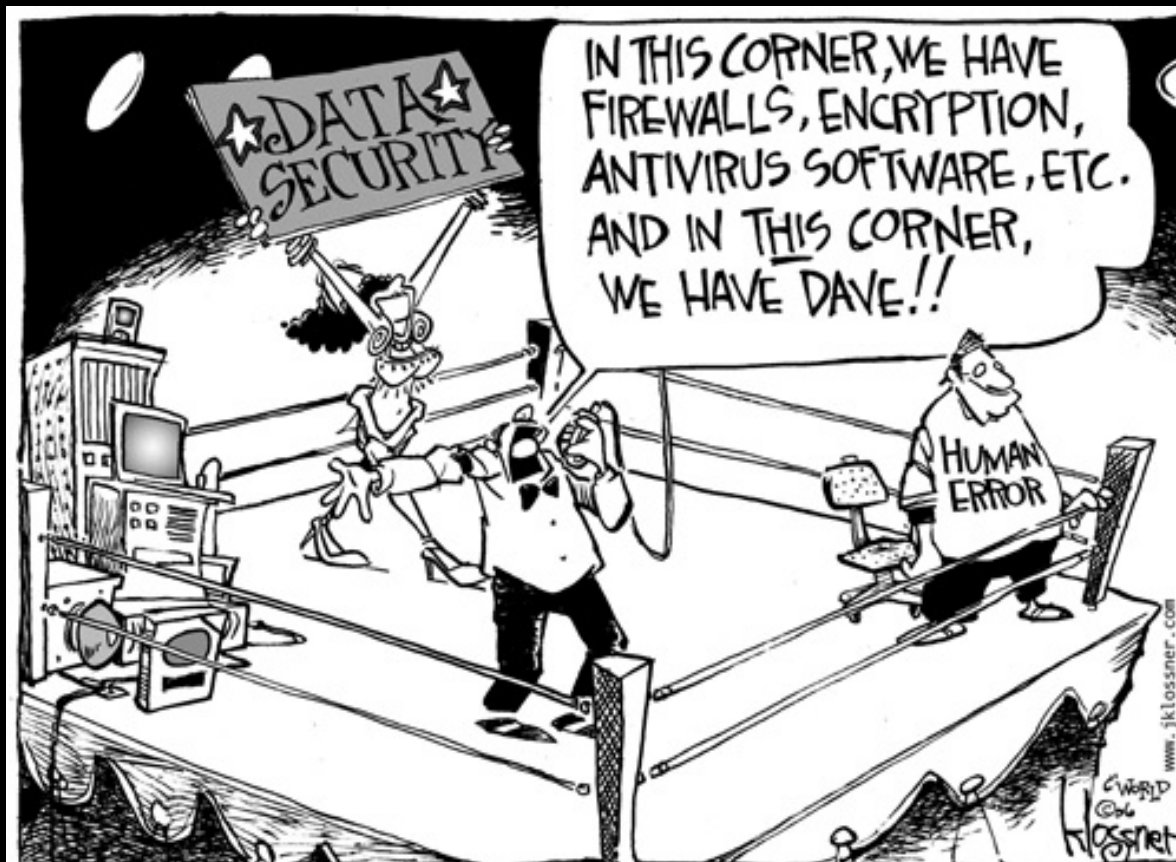*Winning the Battle against Cyber attacks*

John Beal – Endpoint Security and SaaS Leader

Security Systems Software

jbeal@ca.ibm.com

73% of firms discovered cloud usage outside of security policies

11.6M mobile devices are infected at any given time

Sources: 2013, IDC US Cloud Security Survey; 2015, IBM X-Force

RISK INNOVATION

What are we doing about it?

- Adding another tool

- Hoping it's not me

- Building more barricades

- Skipping the basics

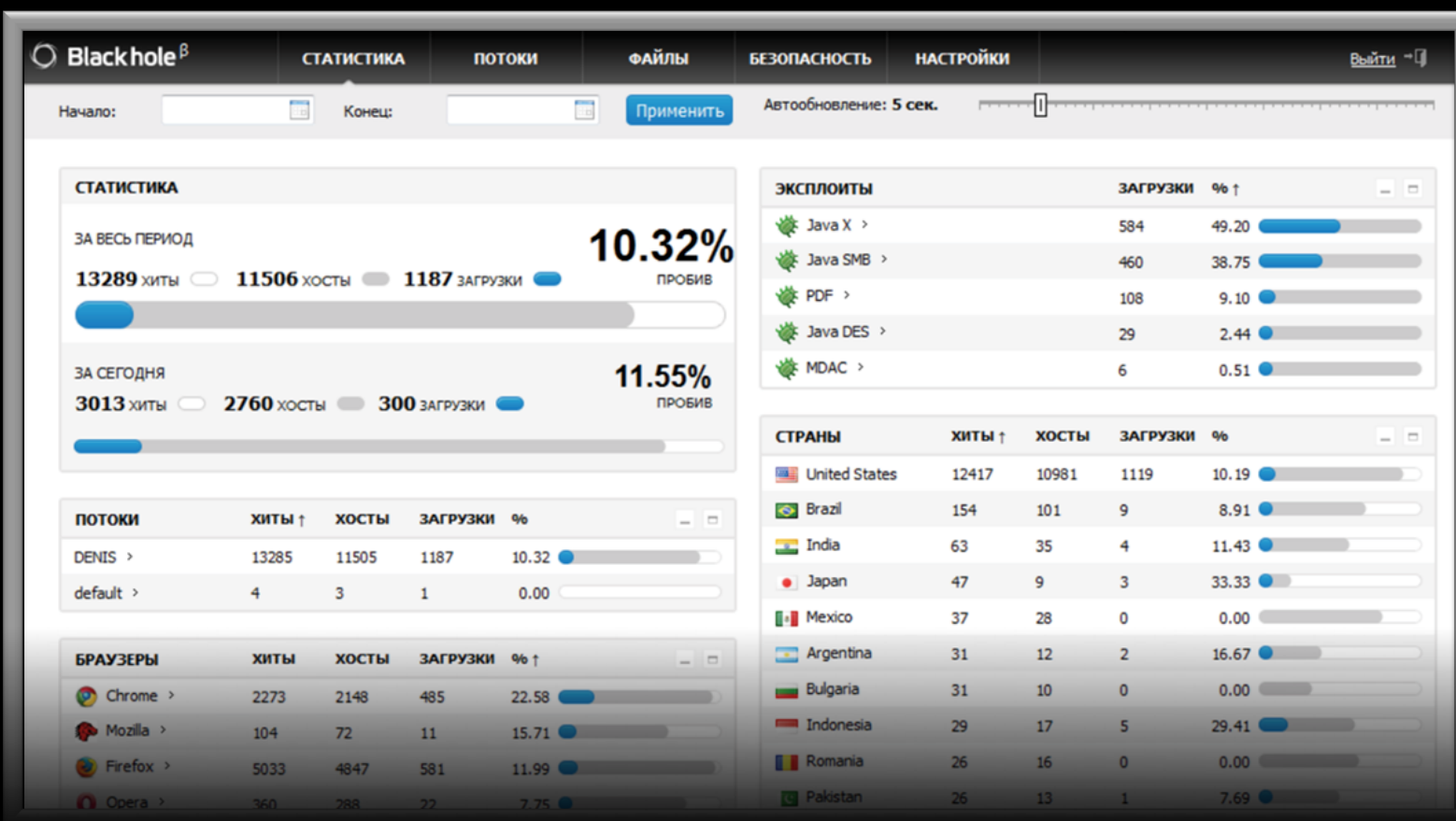- Ignoring privileges

- Blocking the cloud

- Betting on BYOS

A NEW APPROACH TO
SECURITY

Security requires
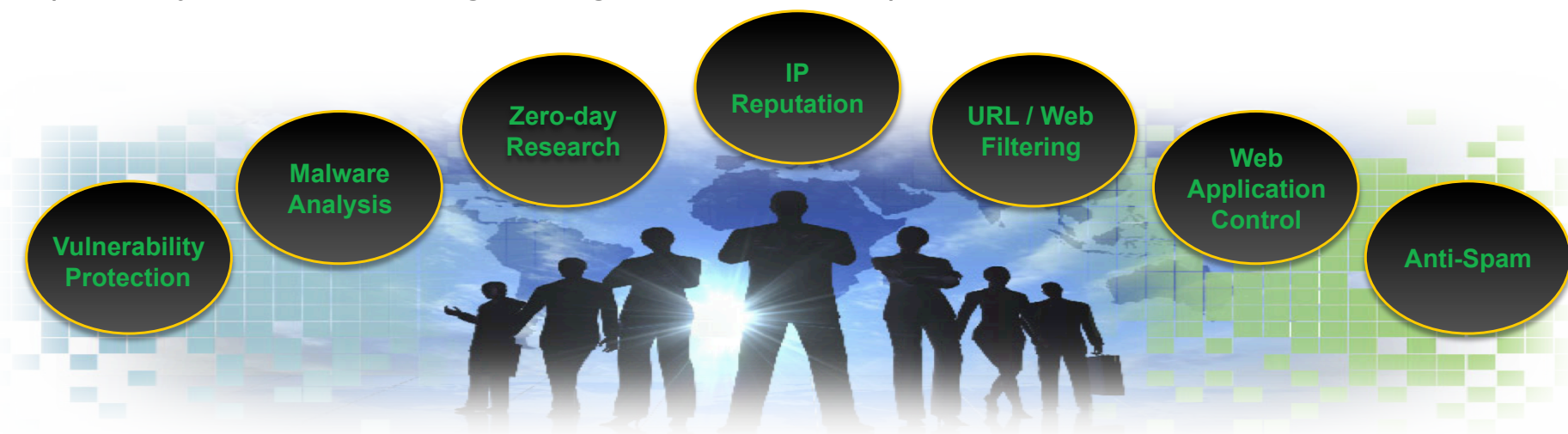**Collaboration**

Cyber criminals use BUSINESS INTELLIGENCE

IBM X-Force® Research and Development

Expert analysis and data sharing on the global threat landscape

- Vulnerability Protection
- Malware Analysis
- Zero-day Research
- IP Reputation
- URL / Web Filtering
- Web Application Control
- Anti-Spam

The IBM X-Force Mission

- **Monitor** and evaluate the rapidly changing threat landscape
- **Research** new attack techniques and develop protection for tomorrow's security challenges
- **Educate** our customers and the general public
- **Integrate** and distribute Threat Protection and Intelligence to make IBM solutions smarter

Collaborate more effectively than the hackers
xforce.ibmcloud.com
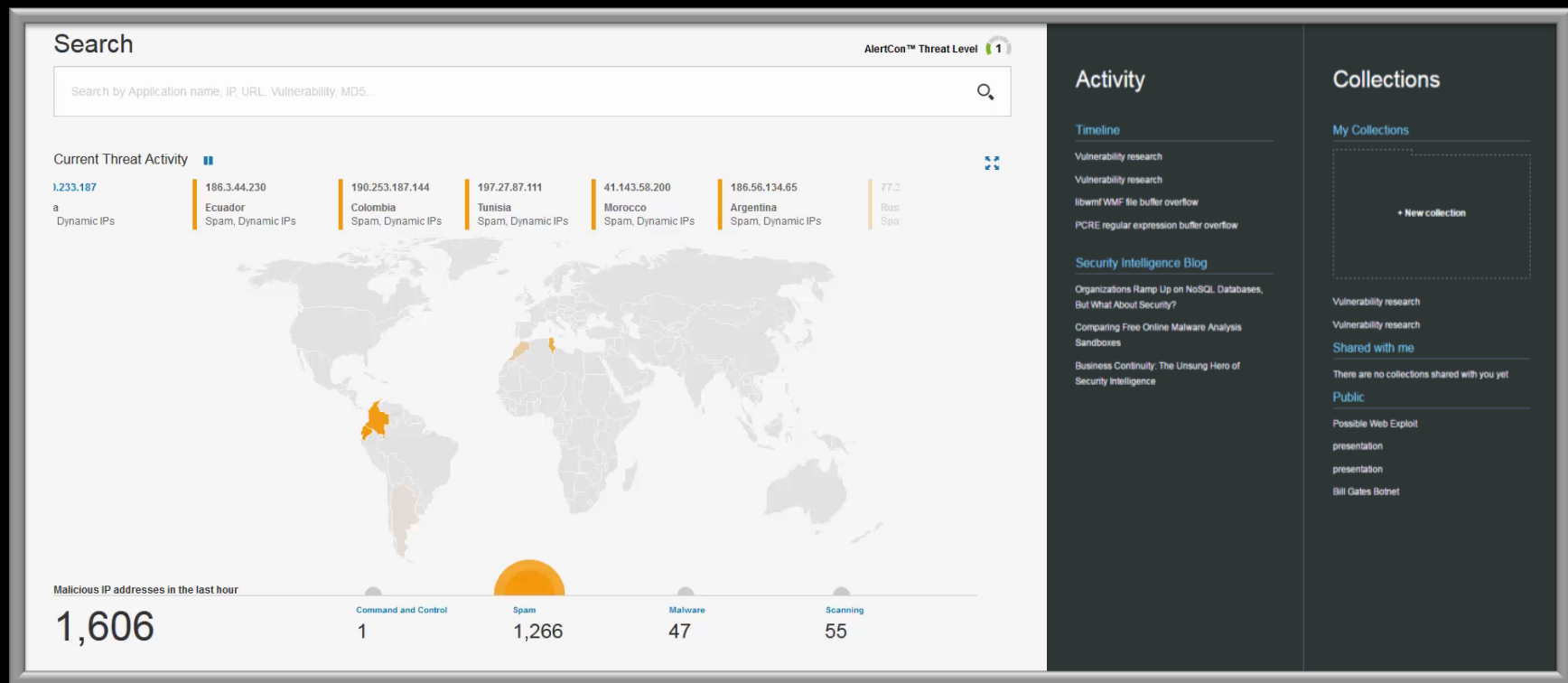
Establish security as an immune system
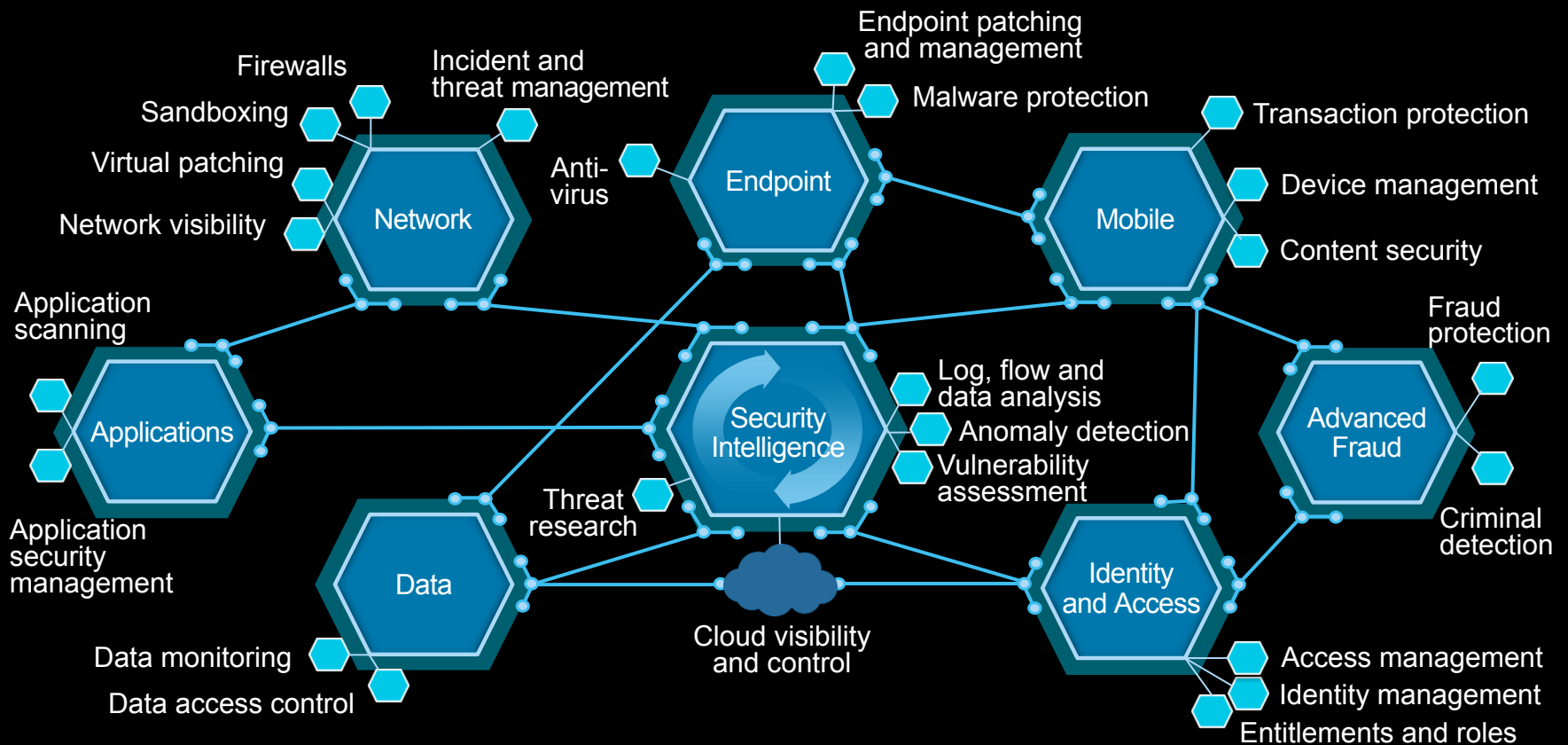
IBM understands the demands of managing a global heterogeneous IT infrastructure

- **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 patches itself in under 48Hrs

- IBM maintains 24/7 Security Compliance on or off the network.

IBM's Unified Endpoint Management :

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.

Clients often discover **35% more endpoints** connecting to their corporate data than previously identified

250,000
The number of endpoints that can be managed in any location across the globe—all from a single server

Up to 90% faster deployment time for patches and upgrades

IBM Bigfix's Unique Architecture:

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
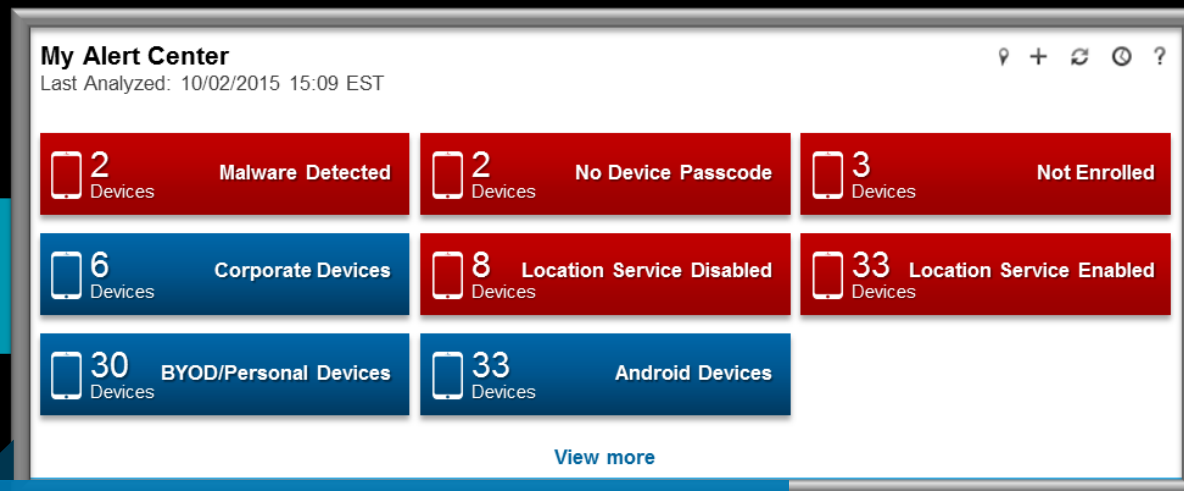- Highly extensible/applicable across all platforms

Lightweight, easily configurable infrastructure
- Designate agent as a relay or discovery point in minutes
- Provides built-in redundancy
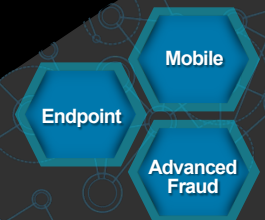- Leverages existing systems/shared infrastructure

Roll out security on 100,000 devices in 6 weeks
IBM internal example

Personal and Consumer

Enterprise

My Alert Center
Last Analyzed: 10/02/2015 15:09 EST

2 Devices	Malware Detected	2 Devices	No Device Passcode	3 Devices	Not Enrolled
6 Devices	Corporate Devices	8 Devices	Location Service Disabled	33 Devices	Location Service Enabled
30 Devices	BYOD/Personal Devices	33 Devices	Android Devices		

View more

Enforce mobile compliance

Mobile

Endpoint

Advanced Fraud

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
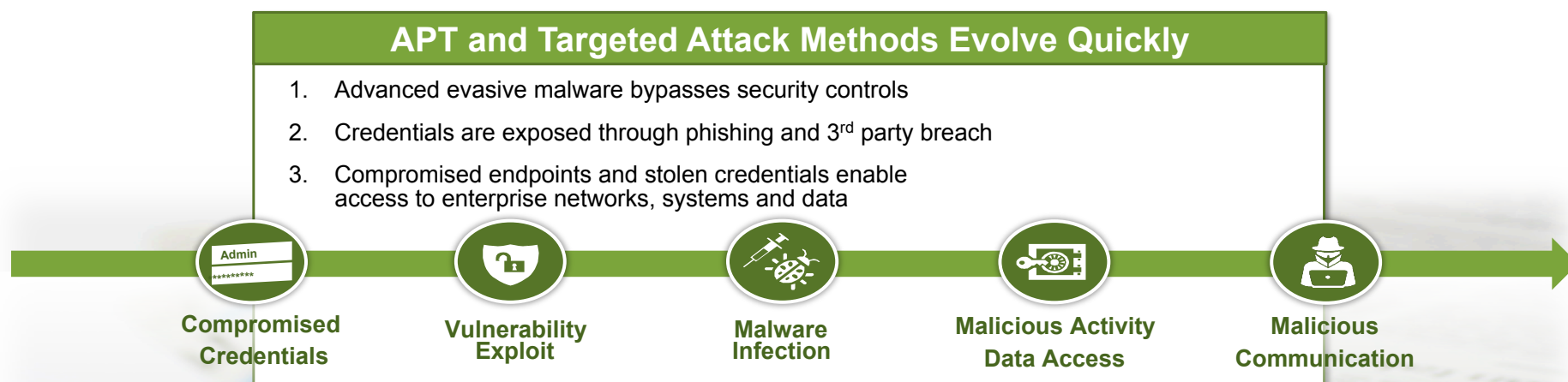The amount of time to securely enroll a new device

300+
The number of educational and clinical apps managed

1
Number of consoles needed to securely manage all iPads

Advanced Malware & Endpoint Protection

Despite existing controls, employee endpoints are compromised and are used as pivot points into the enterprise network

APT and Targeted Attack Methods Evolve Quickly

1. Advanced evasive malware bypasses security controls

2. Credentials are exposed through phishing and 3rd party breach

3. Compromised endpoints and stolen credentials enable access to enterprise networks, systems and data

Compromised Credentials → **Vulnerability Exploit** → **Malware Infection** → **Malicious Activity Data Access** → **Malicious Communication**

Who Hacked Sony? New Report Raises More Questions

JPMorgan Chase Breach Puts Renewed Focus on Malware

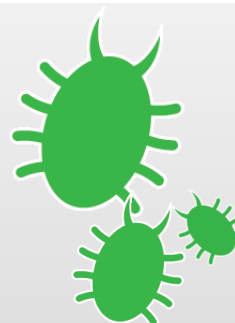**A $1Billion APT Attack – Carbanak May Just Be the Biggest Cyber Heist Ever**

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]

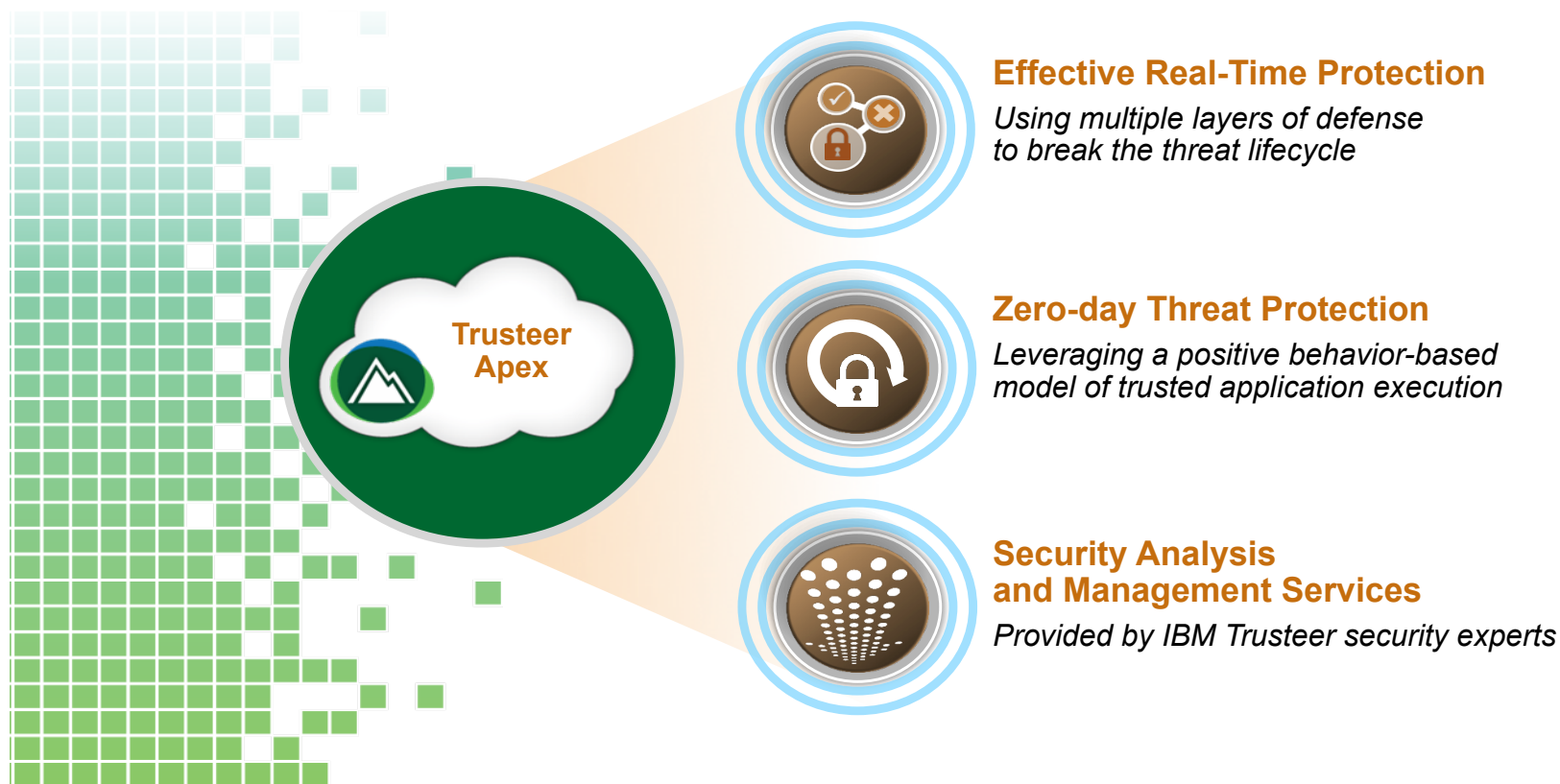**138 billion** apps were downloaded in 2014[2]. By 2017 **50%** of employers will require BYOD[3].

Mobile malware is growing. Malicious code is infecting **>11.6 million** mobile devices at any given time[4].
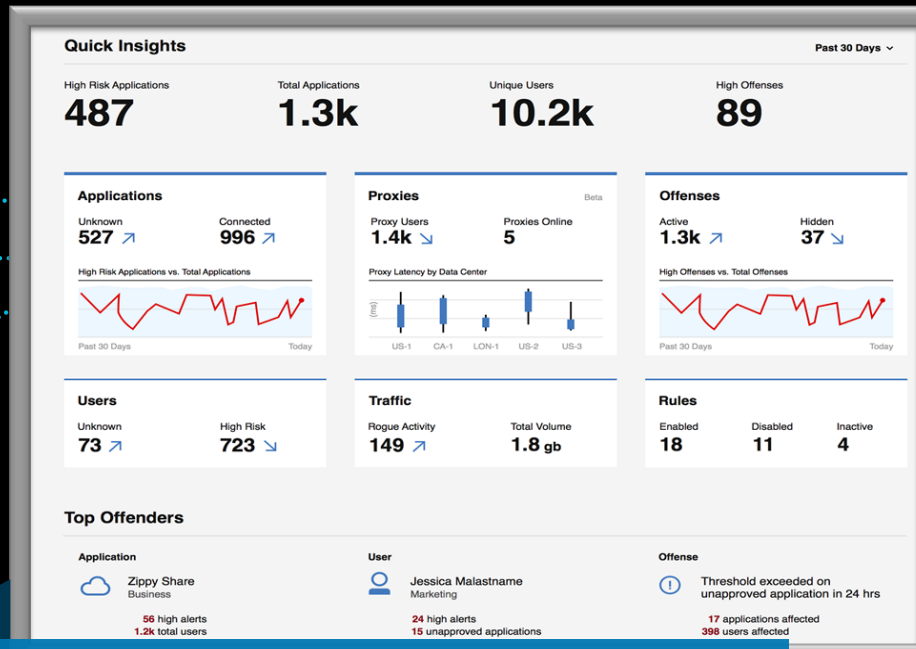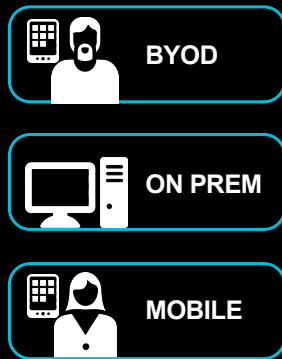
Mobile devices and the apps we rely on are under attack. **97%** and **87%** of top paid Android and iOS apps have been hacked[5].

Preemptive, multi-layered protection against advanced malware & credentials theft

Trusteer Apex

Effective Real-Time Protection

*Using multiple layers of defense
to break the threat lifecycle*

Zero-day Threat Protection

*Leveraging a positive behavior-based
model of trusted application execution*

**Security Analysis
and Management Services**

Provided by IBM Trusteer security experts

Embrace the cloud but not the risk

A new SaaS solution to help securely deploy cloud services

EMPLOYEES

BYOD

ON PREM

MOBILE

IBM Cloud Security Enforcer

RISKY APPS

APPROVED APPS

box salesforce Office 365 workday

DETECT	CONNECT	PROTECT		
Discovery and Visibility	Identity and Access Control	Cloud Event Correlation	Threat Prevention	Policy Enforcement

Why IBM?

| IBM's Unified Device Mgt, is a UNIQUE solution in the market today	Why does that matter and Who cares?
• 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.	• 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!
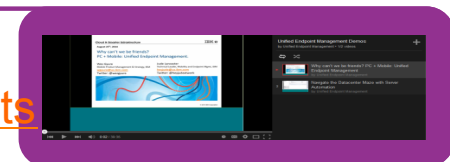
For more information
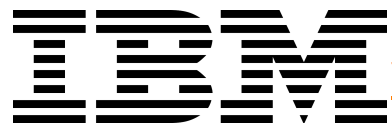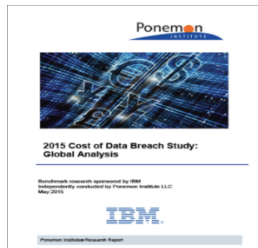
www.unifiedendpointmanagement.com

https://twitter.com/IBMEndpoint

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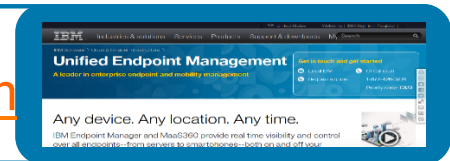
Learn more about IBM Security

Learn more! Download the
2015 Cyber Security Intelligence Index

2015 Ponemon Cost of Data Breach
http://www.ibm.com/security/data-breach

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

Connect with our experts

Blog · Security Intelligence
SecurityIntelligence.com

Follow us on Twitter
@ibmsecurity

IBM Security

Intelligence. Integration. Expertise.