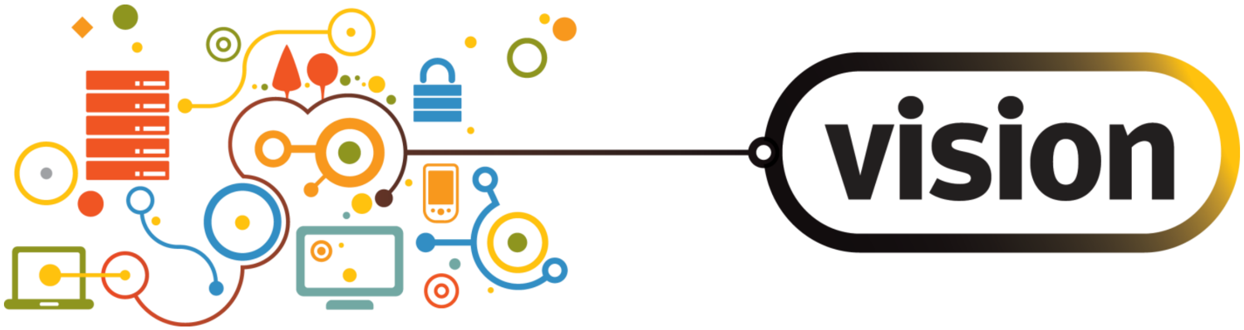


Applications & Data Security

Current Challenges & Leading Practices from HP & Symantec

John Diamant, HP Secure Product Development Strategist & Distinguished Technologist, CSSLP, CISSP

Garrett Bechler, Senior Principal Security Strategist, Symantec, CISSP, CEH

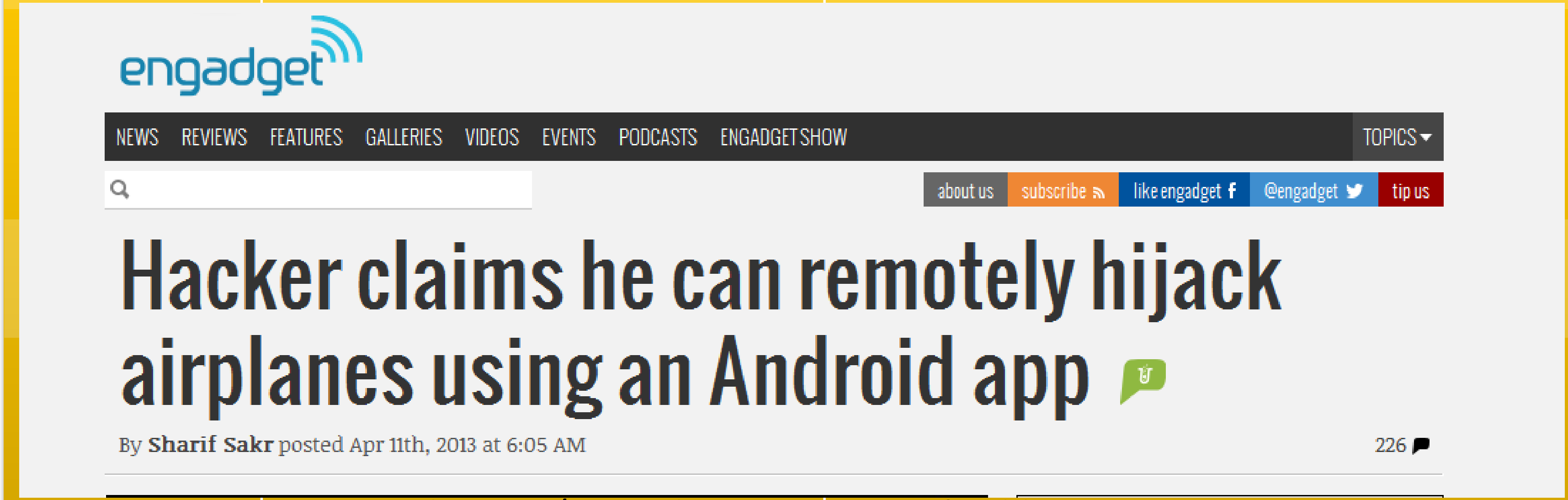
Topics

- Application Security: Weak Cybersecurity Link
- Securing your applications with HP Comprehensive Applications Threat Analysis (HP CATA)
- How Symantec Solutions help secure your Application and Data
- Q&A

Application Security: Weak Cybersecurity Link

Secure Applications & Data: What and Why?

Segment	Application	Concern
Defense	Mission Critical Tactical support Planning support Applications	Mission failure; lives lost Insufficient mission support or resources Military personnel and their families put at risk
	Device Telemetry/Control	Loss of public trust Accidental death or homicide
All	All Websites	Distribution of malware Loss of Trust



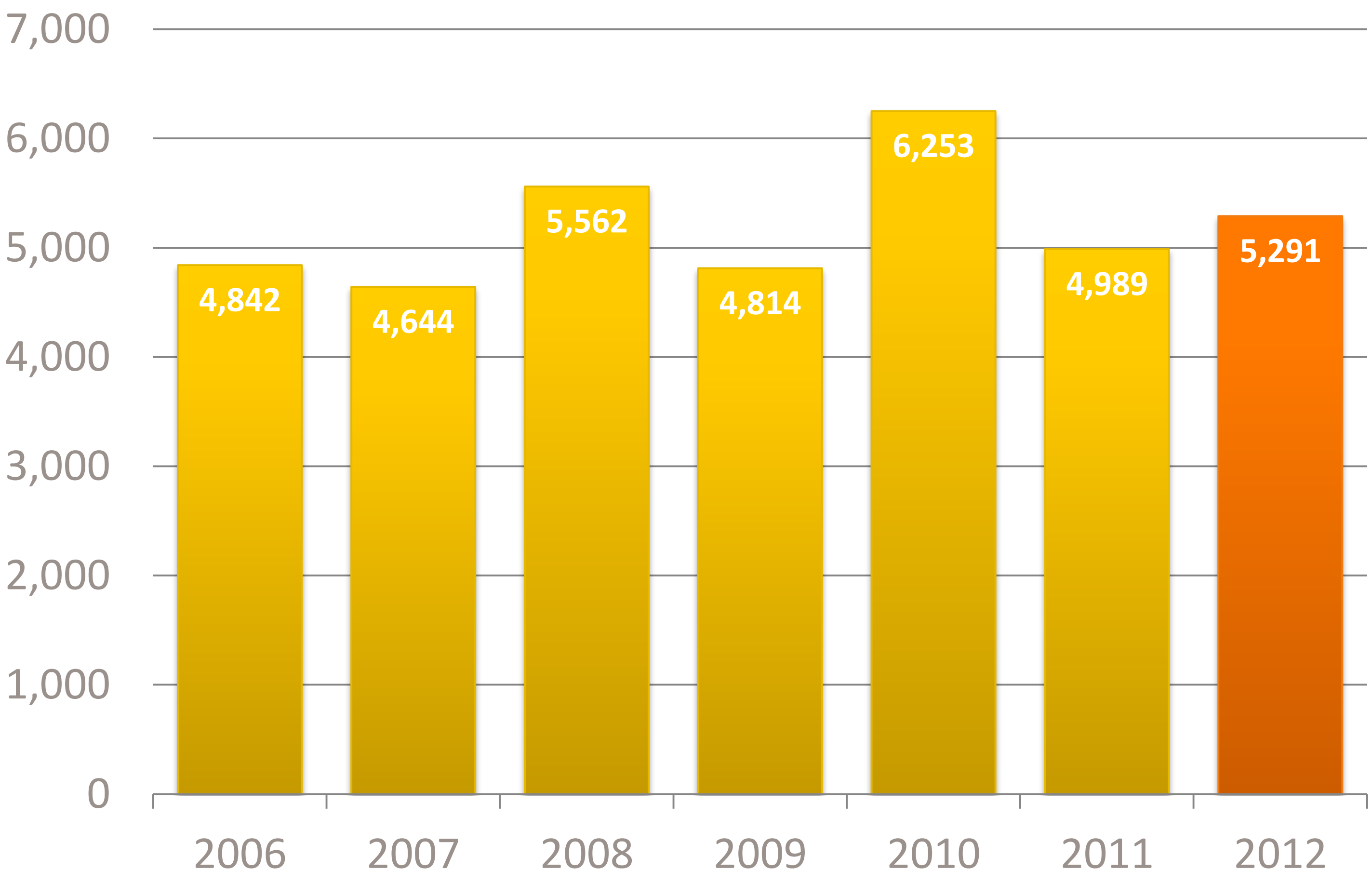
Hacker claims he can remotely hijack airplanes using an Android app

By **Sharif Sakr** posted Apr 11th, 2013 at 6:05 AM

226

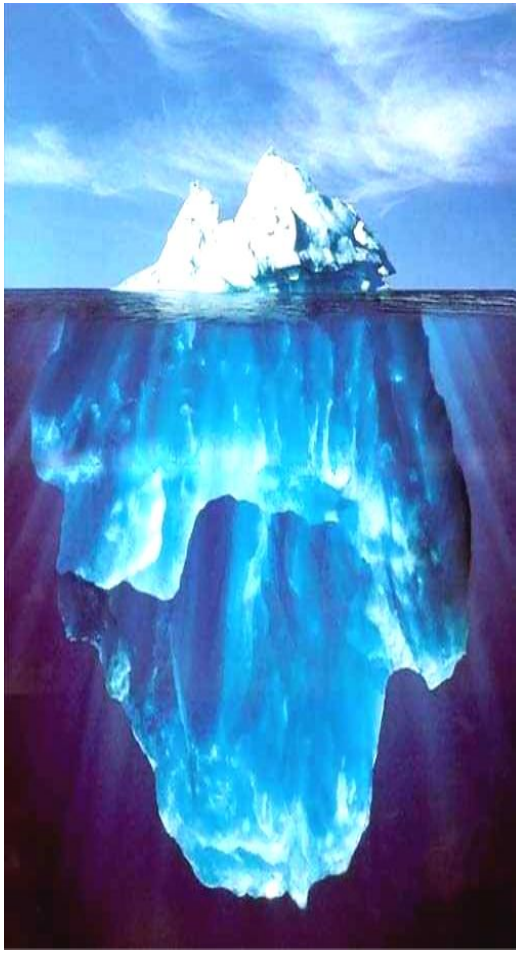
Security: It’s a Real Problem

Published Vulnerabilities over the years



Symantec Internet Security Threat Report

More Defects “Underwater” than those Reported



- Typical applications security approaches are built on known vulnerabilities
- There are >50,000 documented in the National Vulnerability Database

Undiscovered vulnerabilities are huge

- 20X[1] multiplier
- In excess of **1,000,000 vulnerabilities**

Notes: [1]“Public Vulnerabilities Are Tip of the Iceberg,” CNET News

Security: It’s a Real Problem

Regulatory Compliance Costs

Cost of a single PCI violation in 2012. What is $3.5M?

Card Solutions gross revenue for 2012. What is $0?

Security: It’s a Real Problem

Breach Disclosure Costs

Average Cost of Breach?	What is $6.8M*?
VA paid this when exposing 26.5M records?	What is $20M?
The DoD was sued for this for the for Tricare breach of 4.9M beneficiaries	What is $4.9B?

* Ponemon Institute Annual Breach Disclosure Study

Security: It’s a Real Problem

Downtime Costs

26 days Outage

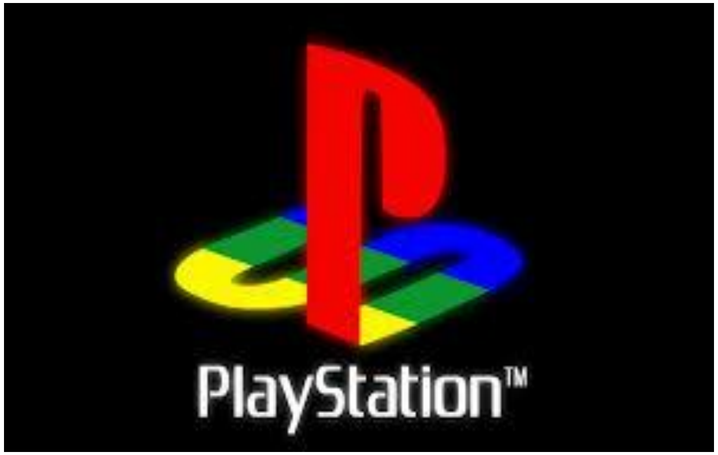
77 million accounts stolen

Called to testify before Congress

$1B lawsuit (eventually dismissed)

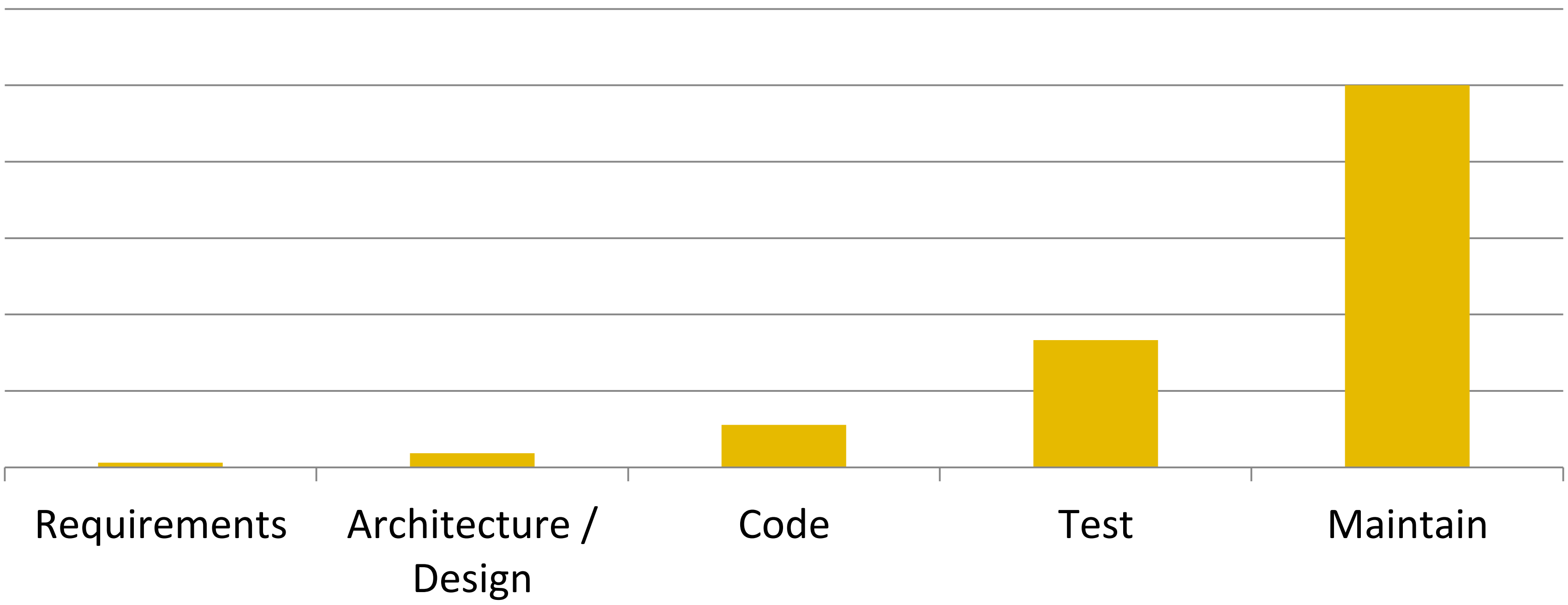
$171M in lost revenues

Reused passwords allow breach of other sites



Security: It’s a Real Problem

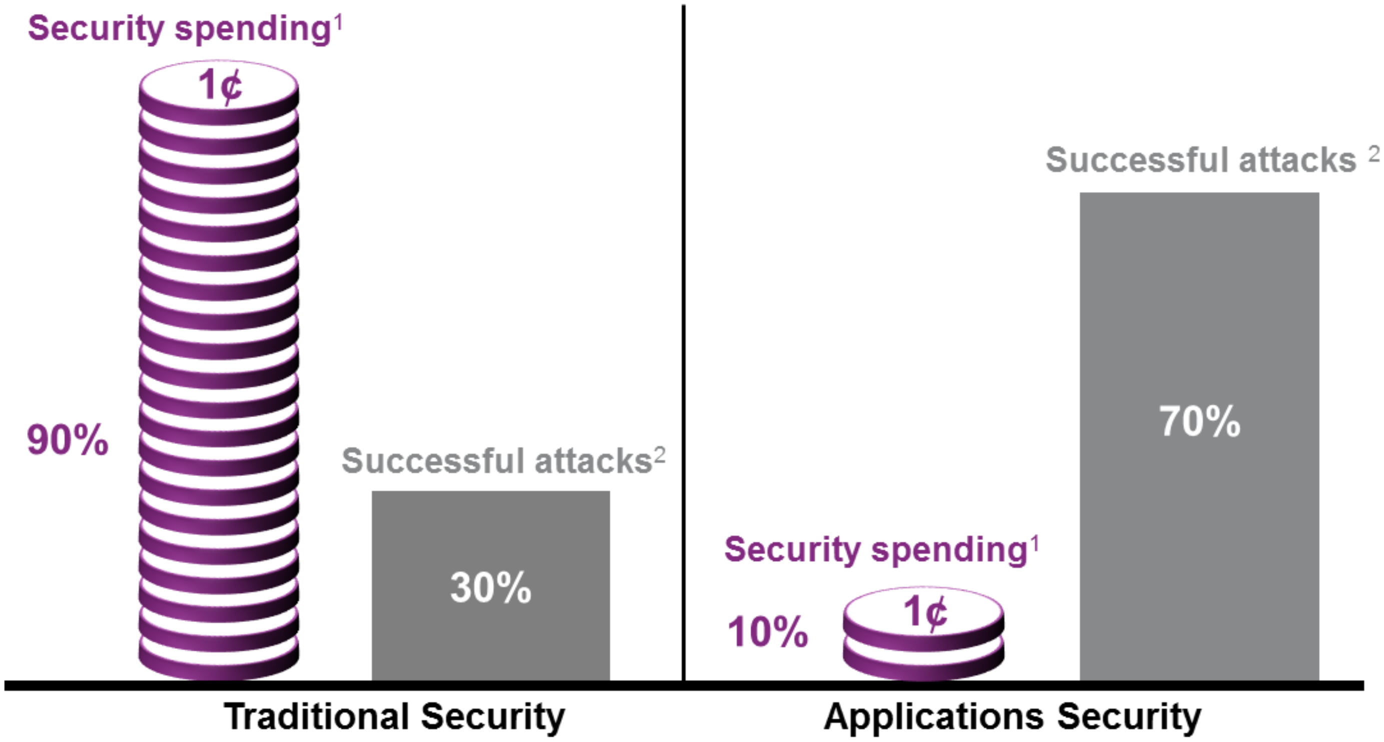
Rework Costs: increase by orders of magnitude (30X-100X) late lifecycle versus early



Why not more:

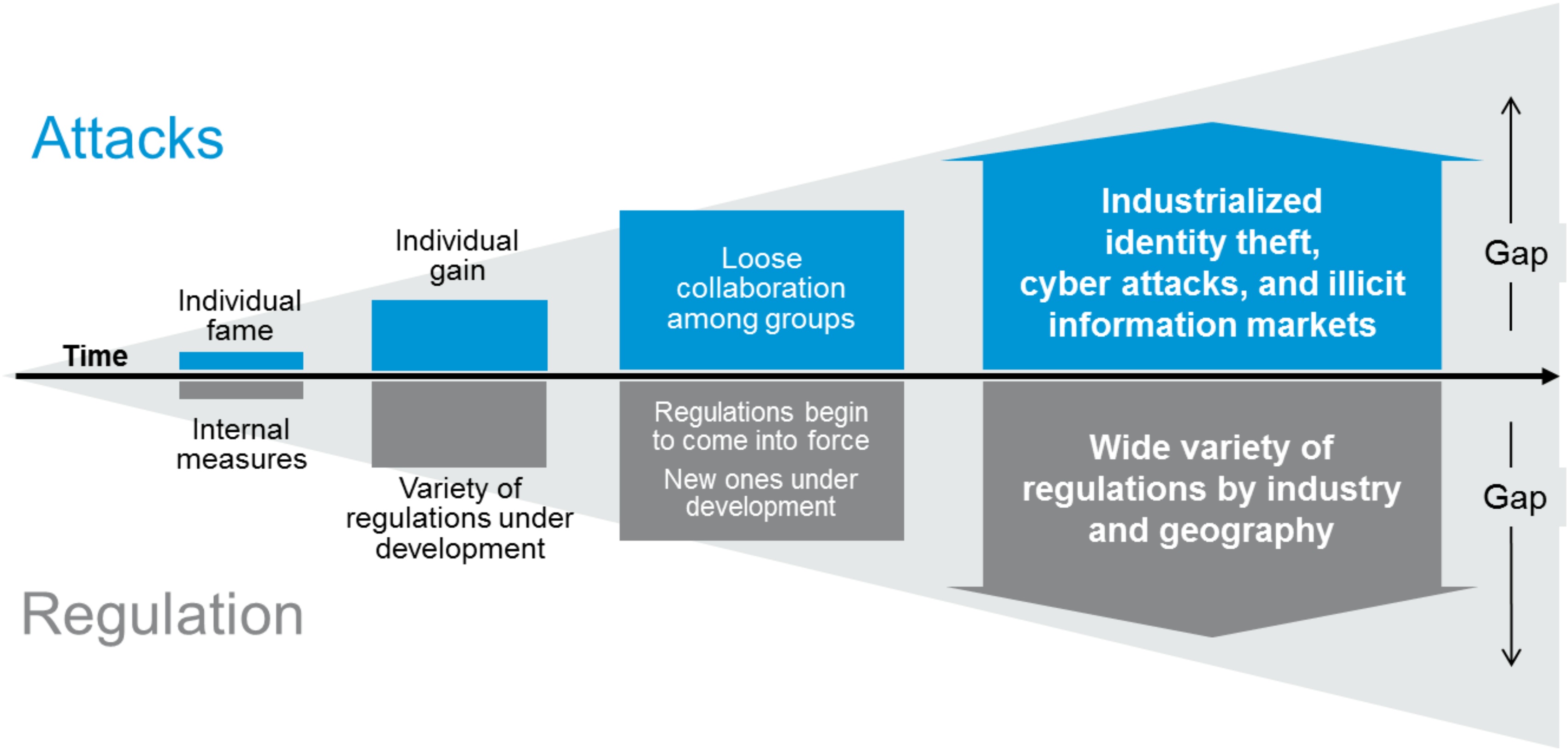
- Time-to-market
- Lack of visibility/process to avoid/find

Security Spending Needs to Reflect Today's Realities



Sources: 1) Gartner IT Security Budgets and Staffing Projections for 2012: Constant Demand and Constant Spending, Mar, 2012
2) Microsoft Security Intelligence Report (SIR), v12, - Dec 2011

Industry-Leading Security is Needed



Attacks

Time

Individual fame

Individual gain

Loose collaboration among groups

Industrialized identity theft, cyber attacks, and illicit information markets

Gap

Internal measures

Variety of regulations under development

Regulations begin to come into force

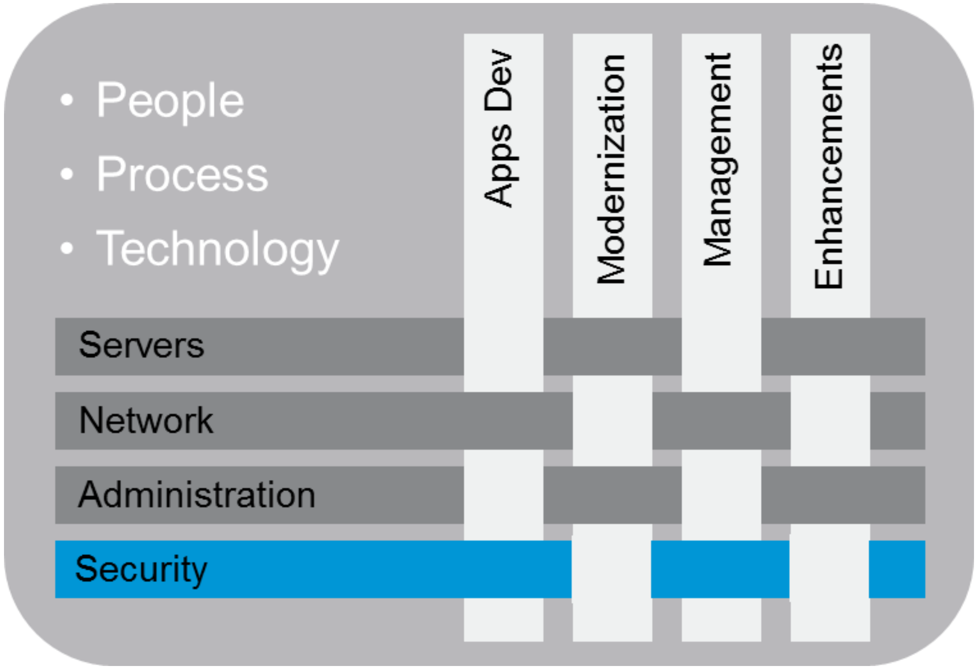
New ones under development

Wide variety of regulations by industry and geography

Gap

Regulation

Today's Security Reality



Security is mainstream and core to the mission

- Woven into the business process
- Included in all decisions and IT projects
- Included at all areas including access points
- Simplified for the end-user

People – e.g. cut and paste

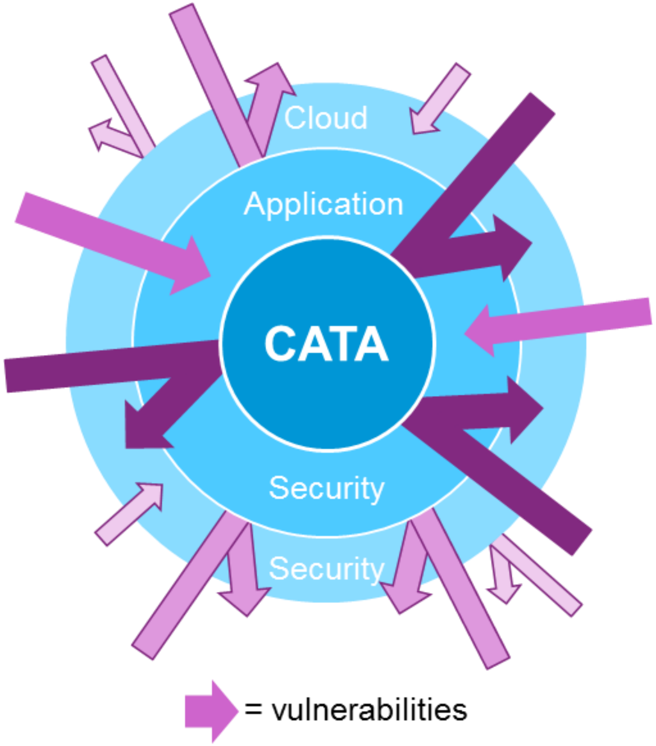
Mobile and Cloud Considerations

Application Security – control resides with the Enterprise

The greatest barrier to cloud and mobile adoption is security

- Cloud and mobile adopters have most influence/control over their own applications
  - Enterprises can only pick a provider or framework, but not make them more secure
  - Enterprises need to address the secure access device as well where they can make them more secure

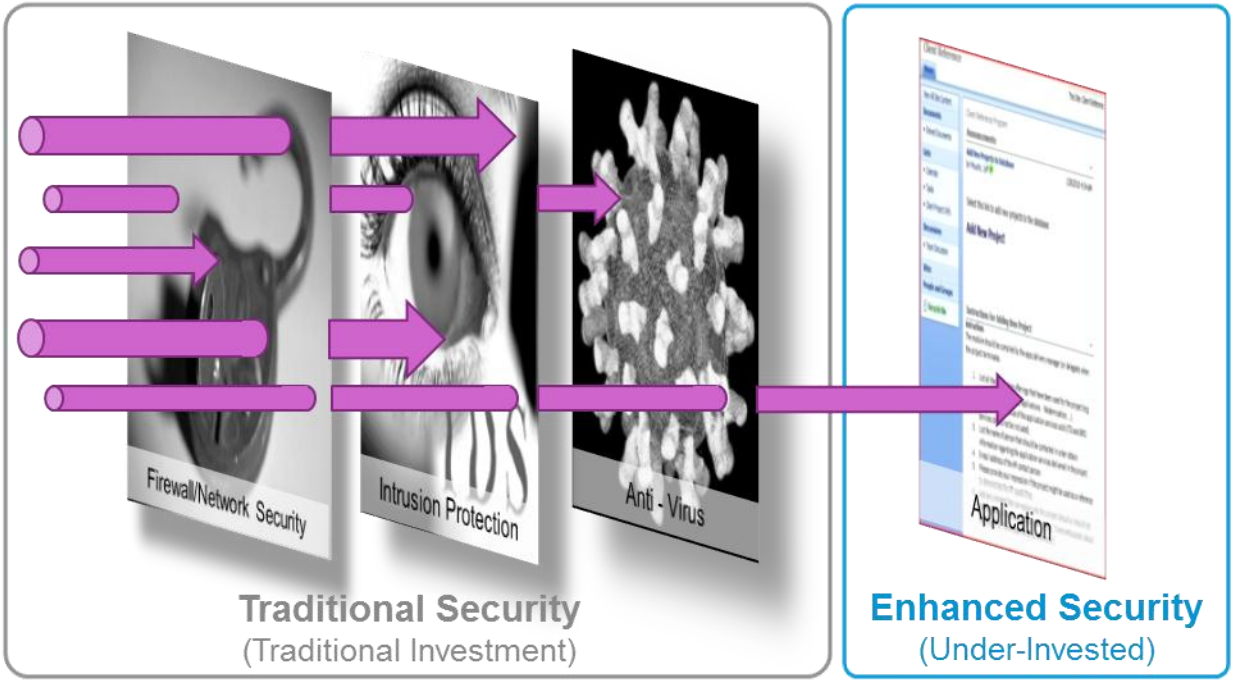
The solution: Applications Security



CATA: HP Comprehensive Applications Threat Analysis

Strong Protection is Needed at all Layers

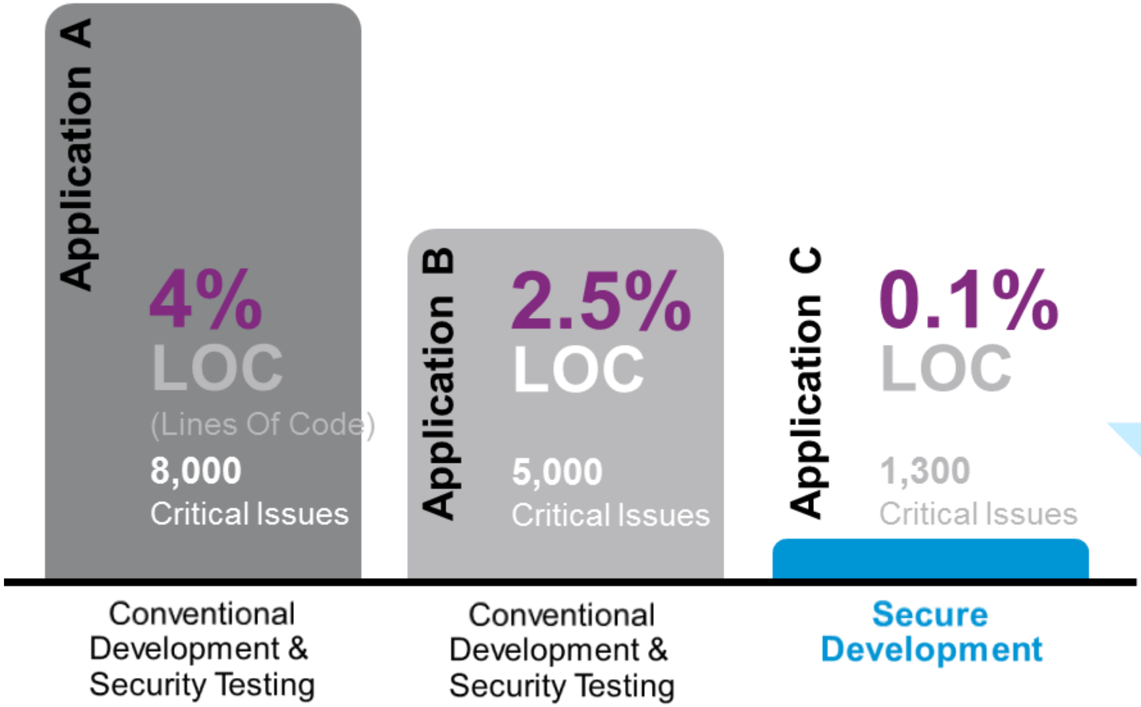
The Enterprise requires flexible, end-to-end security…



More than 70% of successful exploits result from application vulnerabilities

Secure Development – Lowering Cost

U.S. Department of Defense applications examples



- Avoid
- Find
- Fix
- Lessen severity

vulnerabilities

Why Application Security Matters to You

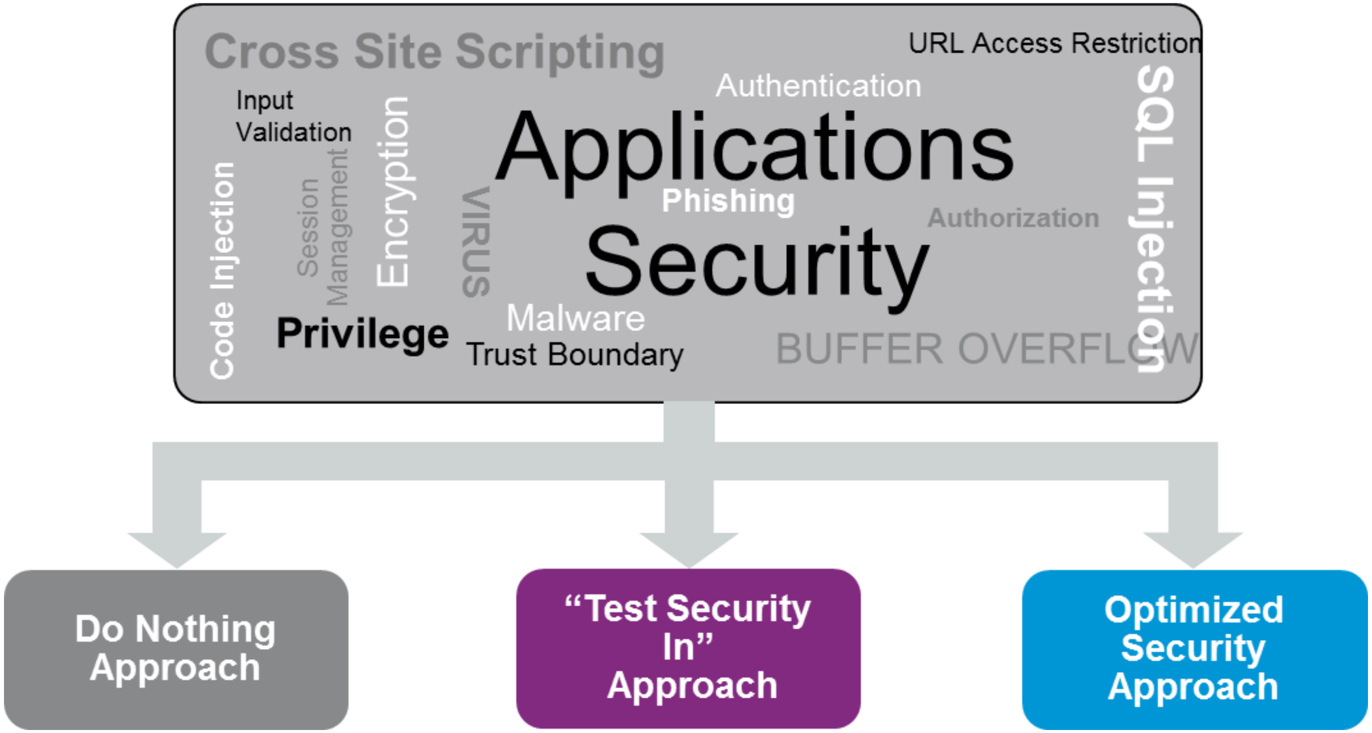
- Is any of your software mission critical?
- What's the cost/impact if your applications are broken into?
- Cloud security
- Mobile security
- Applications transformation
- Applications development
- Applications management

Securing Your Applications

“**Long-term recommendations:** Implement an applications security program […] Implement more strategic and **preventive** security measures, such as **threat modeling**, **secure design**, and code-level analysis, throughout your application lifecycle, from the **requirements** phase to production.”

- *Application Security: 2011 And Beyond* - Forrester Research

Approaches to Solving Application Threats



Applications Security

Cross Site Scripting

URL Access Restriction

Authentication

Input Validation

Code Injection

Session Management

Encryption

VIRUS

Phishing

Authorization

SQL Injection

Privilege

Malware

Trust Boundary

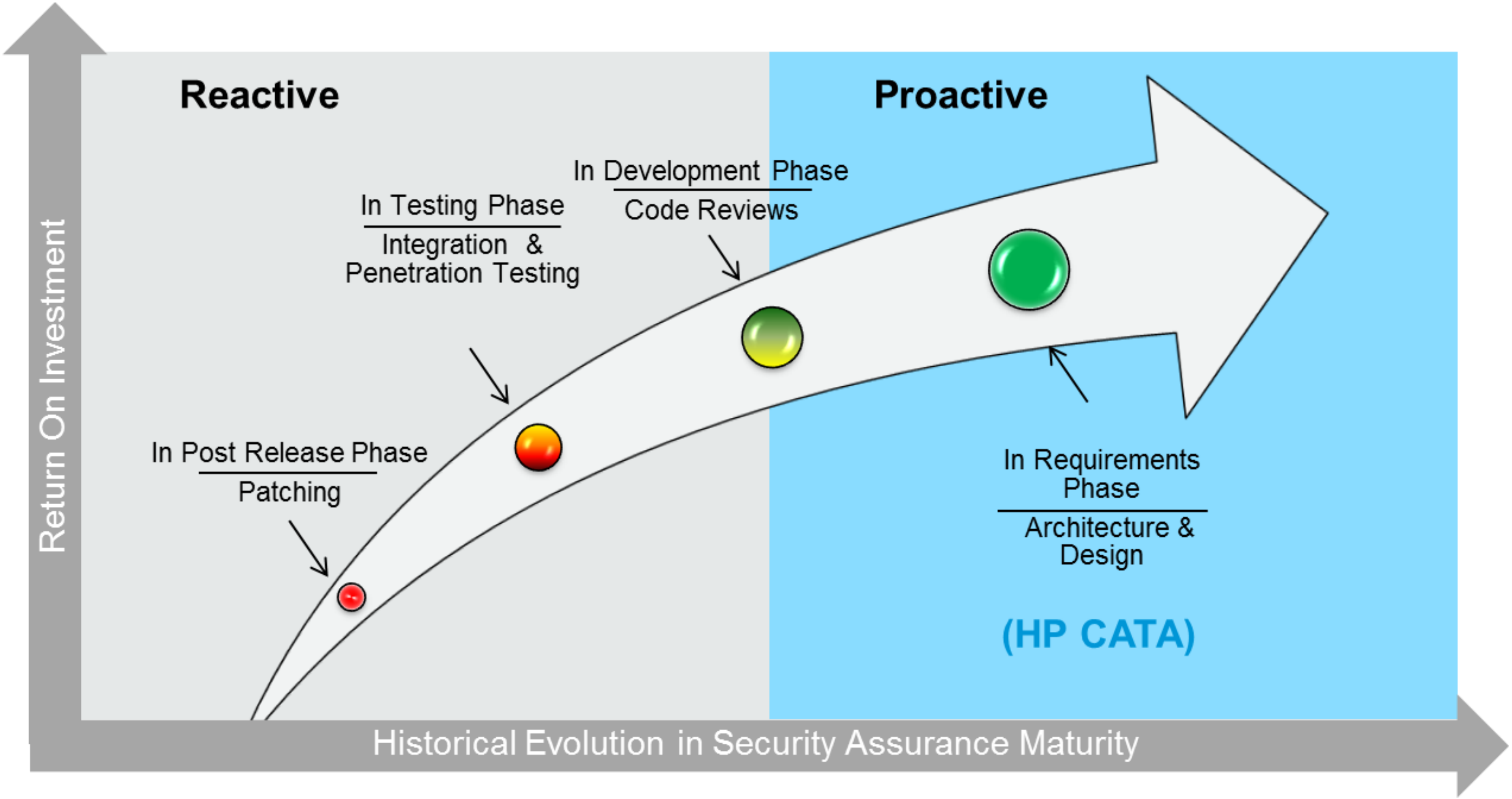
BUFFER OVERFLOW

Do Nothing Approach

“Test Security In” Approach

Optimized Security Approach

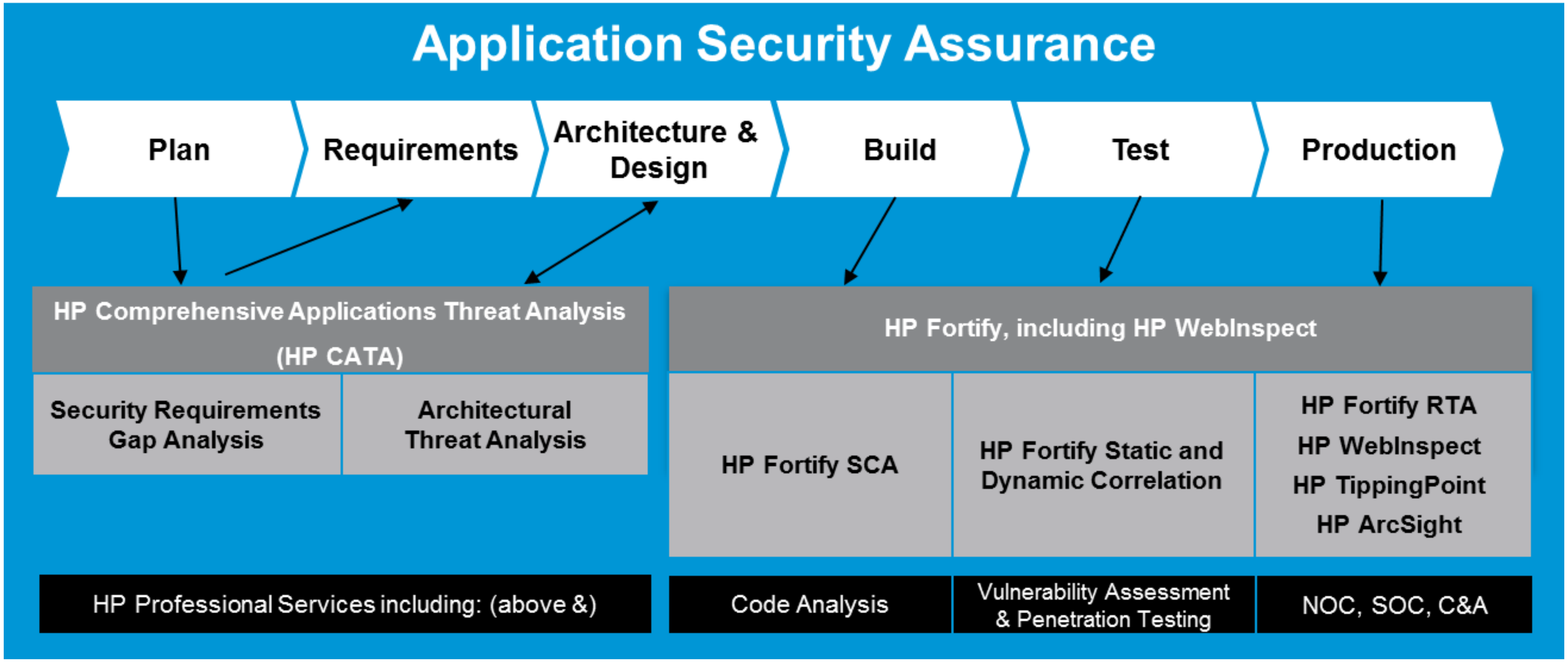
Extending Security Assurance for Today's Realities



Why do Architectural Assurance?

- Architecture is simpler yet more powerful than code
  - Analysis is more straight-forward, reducing cost
  - Analysis is more comprehensive, as the entire architecture can be analyzed
- Build in fault tolerance through architecture
  - Programs won’t be 100% defect-free
  - Resilience to coding defects
- All developers won’t be security experts
  - Sound security architectures limit the risk of vulnerabilities

HP—the only vendor with full lifecycle coverage



Application Security Assurance

Plan | Requirements | Architecture & Design | Build | Test | Production

HP Comprehensive Applications Threat Analysis (HP CATA)

- Security Requirements Gap Analysis
- Architectural Threat Analysis

HP Fortify, including HP WebInspect

- HP Fortify SCA
- HP Fortify Static and Dynamic Correlation
- HP Fortify RTA
HP WebInspect
HP TippingPoint
HP ArcSight

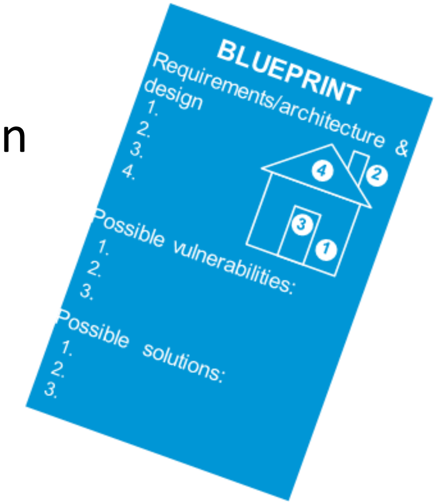
HP Professional Services including: (above &)

- Code Analysis
- Vulnerability Assessment & Penetration Testing
- NOC, SOC, C&A

HP Comprehensive Applications Threat Analysis (HP CATA)

HP CATA At-a-Glance

- HP’s industry-leading, highly effective security quality assessment
- Designed to greatly reduce the problem of security defects in applications
- Reduces applications Total Cost of Ownership
- Builds security into applications, doesn’t merely test it in



Service components:

- Security Requirements Gap Analysis
- Architectural Threat Analysis

Security Requirements Gap Analysis component

Provides analysis of an application to identify often-missed application security requirements…

…that need to be included in technical security requirements imposed by relevant laws, regulations, or practices.

Deliverables:

- Prioritized and vetted list of security requirements or control gaps
- Action plan to remediate

Benefits:

- Avoids costly missed or insufficiently addressed security requirements or controls
- Finds issues much earlier than alternate approaches
- Enables fixing issues with little to no rework cost
- Inexpensive and comprehensive security requirements fit analysis
- Provides inexpensive access to scarce security expertise
- Delivers repeatable, rapid break-even time, high ROI

Threat Analysis: build in cross-architecture resiliency

Avoiding inconsistent and poor security

Weak points (like picket fence above) are very common in application design where obvious indicators of mistakes aren't available

Architectural Threat Analysis findings

🔴 → 🟢

Security Risk Addressed/ Review Progress	Past Behavior	Fix
Least privilege 🔴 → 🟢	All **process** daemons **running** as **root** gaining **full access** to the box and **defects** can **lead** to **unauthorized** code running as **root**	Create **restricted user** account and use it to **run** the process **daemons** **Deploy protection software** to limit the rights of user accounts.
Support for third party certificates 🔴 → 🟢	Using **self-signed** certificates **hinders** customer **validation**, **exposing** customer and servers to **man-in-the-middle attacks**.	**Replaced self-signed certificates** and **provided** means for **validating** the **certificates** correctly
Insufficient authentication strength 🟡 → 🟢	A username and password combination is a very **weak authentication** scheme, and **susceptible to** guessing **attacks and cascading breaches.** **Users may put sticky notes with passwords on their monitors or share passwords between systems**	**implement two-factor user authentication**
World-writable directory 🟡 → 🟢	Web application **configuration files** were **world –writable exposing** them to an external **attacker** to be able to **modify important application characteristics**	Included **file system checks** in build **scripts**. Protect and monitor critical system files with a **critical file monitoring solution**.
Allowing application access from BYOD 🔴 → 🟢	Allowed access to web and mobile applications from non-corporate owned devices. **Data** is frequently **misused** and **stored insecurely violating state and federal regulations** as well as **possible theft or data loss**.	**Implement endpoint security**

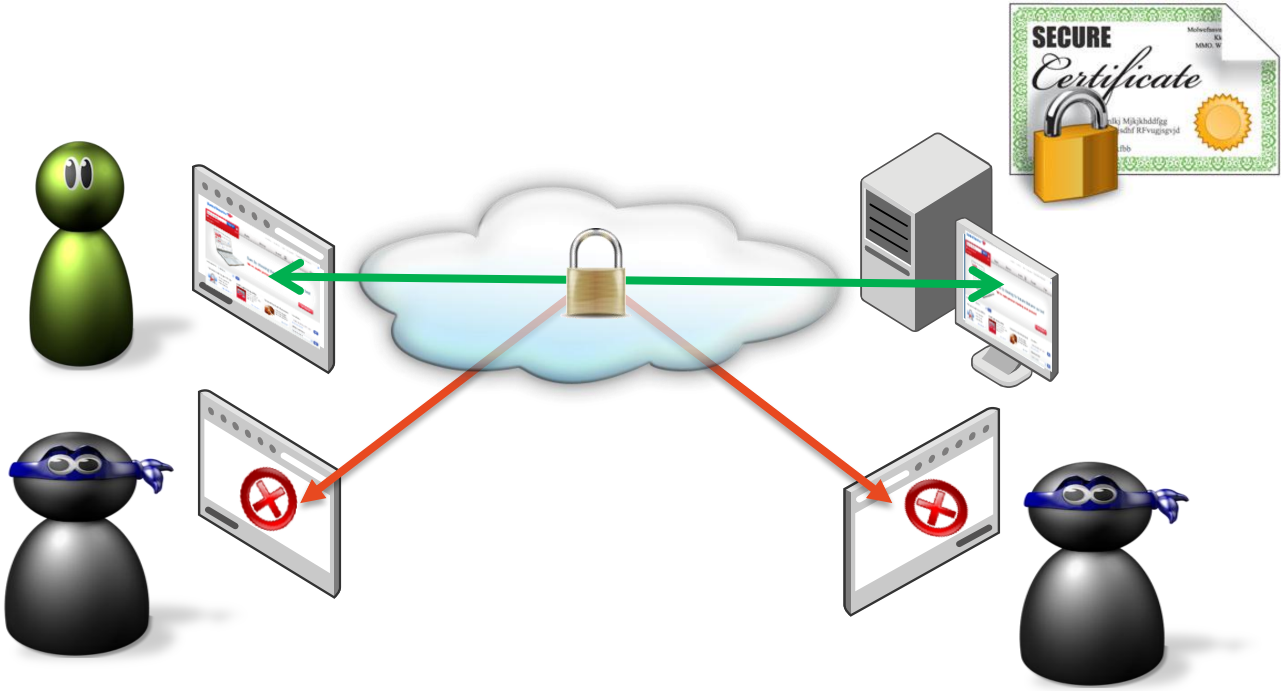
How is this Approach Different?

Reactive approach **(Traditional)**	Proactive approach **(HP CATA)**
Code-oriented	Architecturally oriented
Security validation after code is written	Security modeled in design, before coding begins
Focused on known vulnerabilities	Proactive approach for known & unknown vulnerabilities
“Test security in” (rework)	“Build security in”
Test everything or miss something	Optimized ROI and risk-driven approach
Rely on organically grown security expertise	Utilize expert consultants & leverage available in-house security expertise
Limited security testing to contain cost	Inexpensive high-level assessment to prioritize testing investment
Hope you find vulnerabilities before attackers	Security assurance + testing to catch few escapes

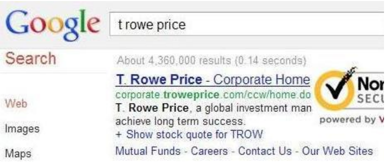
Addressing findings with Symantec Solutions

Self Signed Certificates

Security Risk Addressed/ Review Progress	Past Behavior	Fix
Support for third party certificates 🔴 ⇨ 🟢	Using **self-signed** certificates **hinders** customer **validation**, **exposing** customer and servers to **man-in-the-middle attacks**.	**Replaced self-signed certificates** and **provided** means for **validating** the **certificates** correctly



SSL Certificates and more



Google | t rowe price

Search

Web

Images

Maps

About 4,360,000 results (0.14 seconds)

T. Rowe Price - Corporate Home

corporate.troweprice.com/ccw/home.do

T. Rowe Price, a global investment man achieve long term success.

+ Show stock quote for TROW

Mutual Funds - Careers - Contact Us - Our Web Sites

Seal In Search

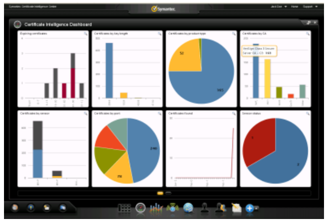
Norton Secured Seal

Extended Validation certificates

Always-On SSL

SGC Premium certificates

Anti-Malware Scanning

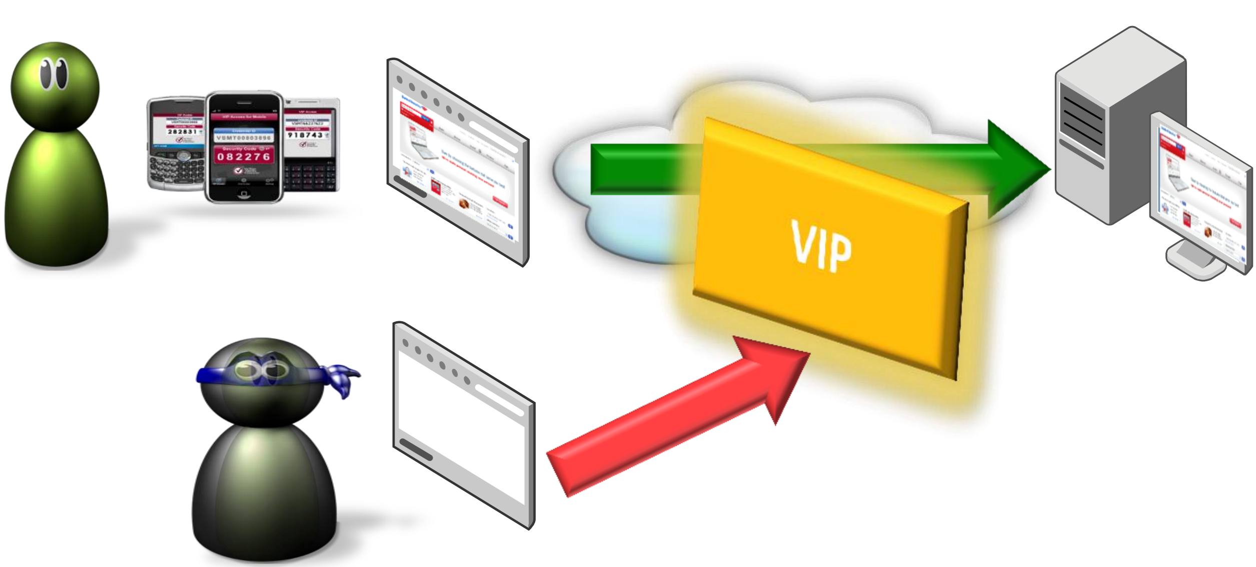


Certificate Intelligence Center

Vulnerability Assessment

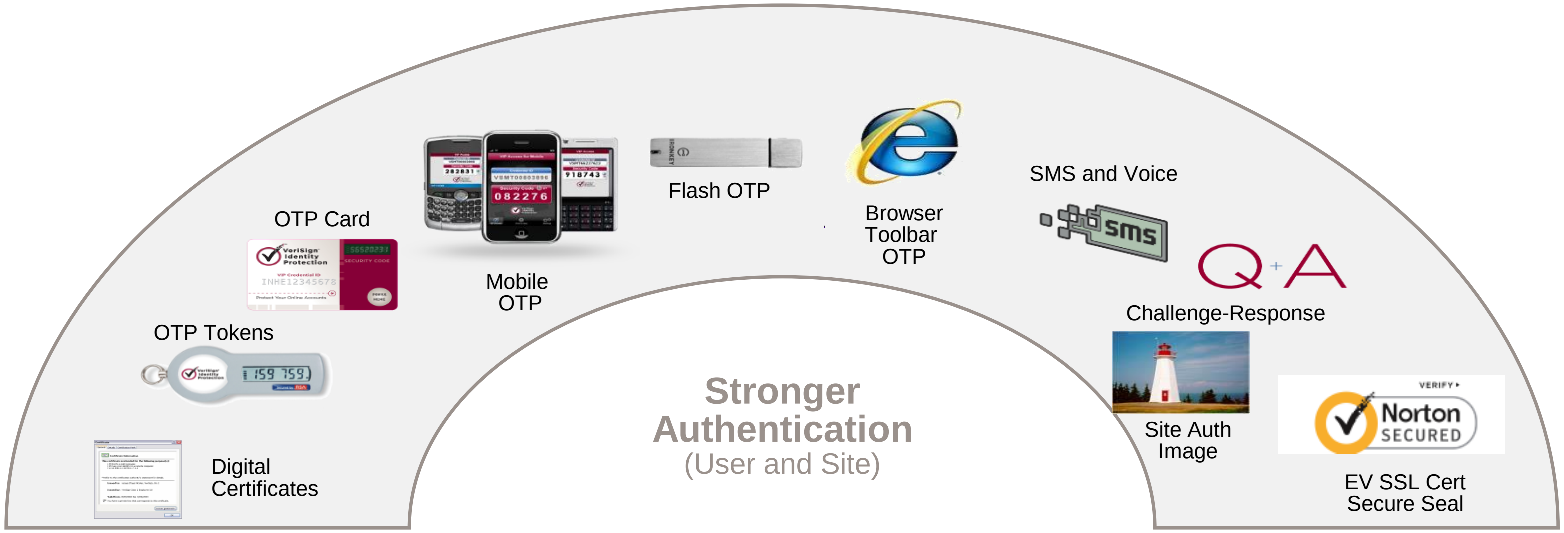
Risk based Authentication

Security Risk Addressed/ Review Progress	Past Behavior	Fix
Insufficient authentication strength 🟡 ⇨ 🟢	A username and password combination is a very **weak authentication** scheme, and **susceptible to** guessing **attacks and cascading breaches.** **Users may put sticky notes with passwords on their monitors or share passwords between systems**	**implement two-factor user authentication**



Norton SECURED powered by VeriSign

VIP: Complete Solution for Authentication



OTP Card

Mobile OTP

Flash OTP

Browser Toolbar OTP

SMS and Voice

Challenge-Response

OTP Tokens

Digital Certificates

Site Auth Image

EV SSL Cert Secure Seal

Stronger Authentication
(User and Site)

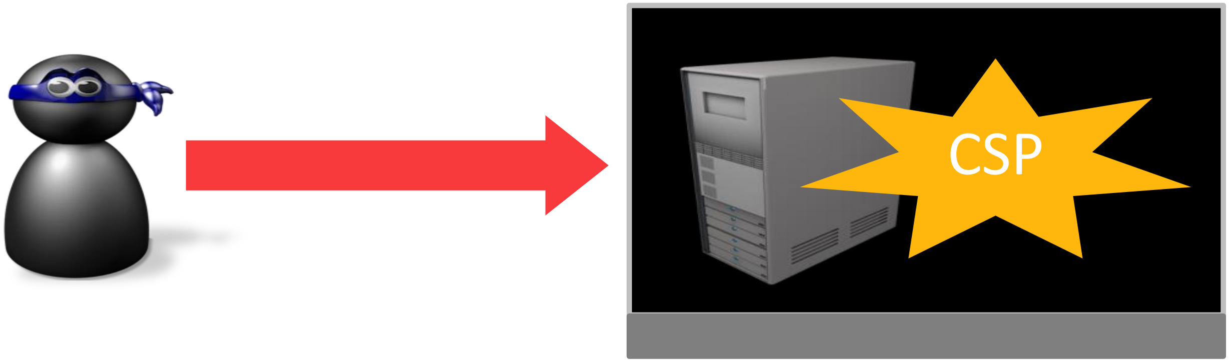
VIP Fraud Detection and Risk Analysis Service

Symantec Validation and ID Protection Service (VIP)
(fraud intelligence and shared authentication)

Lacking Least Privilege

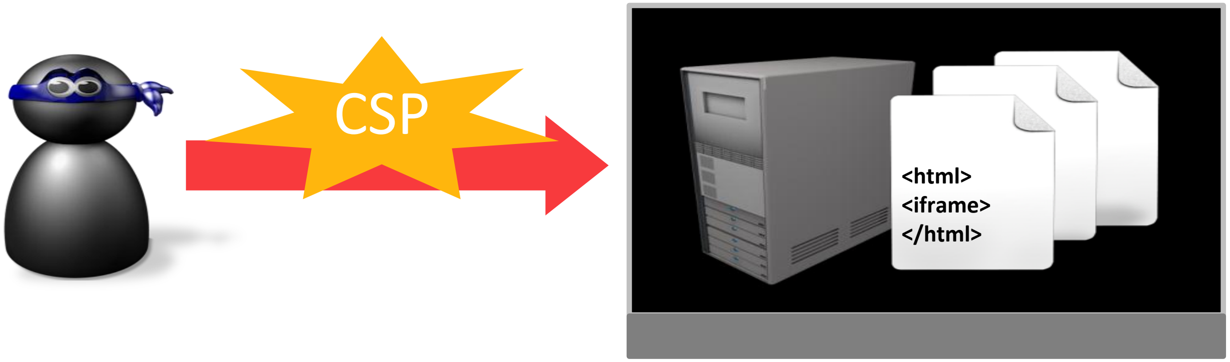
Restricting Root and other Accounts

Security Risk Addressed/ Review Progress	Past Behavior	Fix
Least privilege 🔴 ⇨ 🟢	All **process** daemons **running** as **root** gaining **full access** to the box and **defects** can **lead** to **unauthorized** code running as **root**	**Create restricted user account** and use it to **run** the process **daemons** **Deploy protection software** to limit the rights of user accounts.



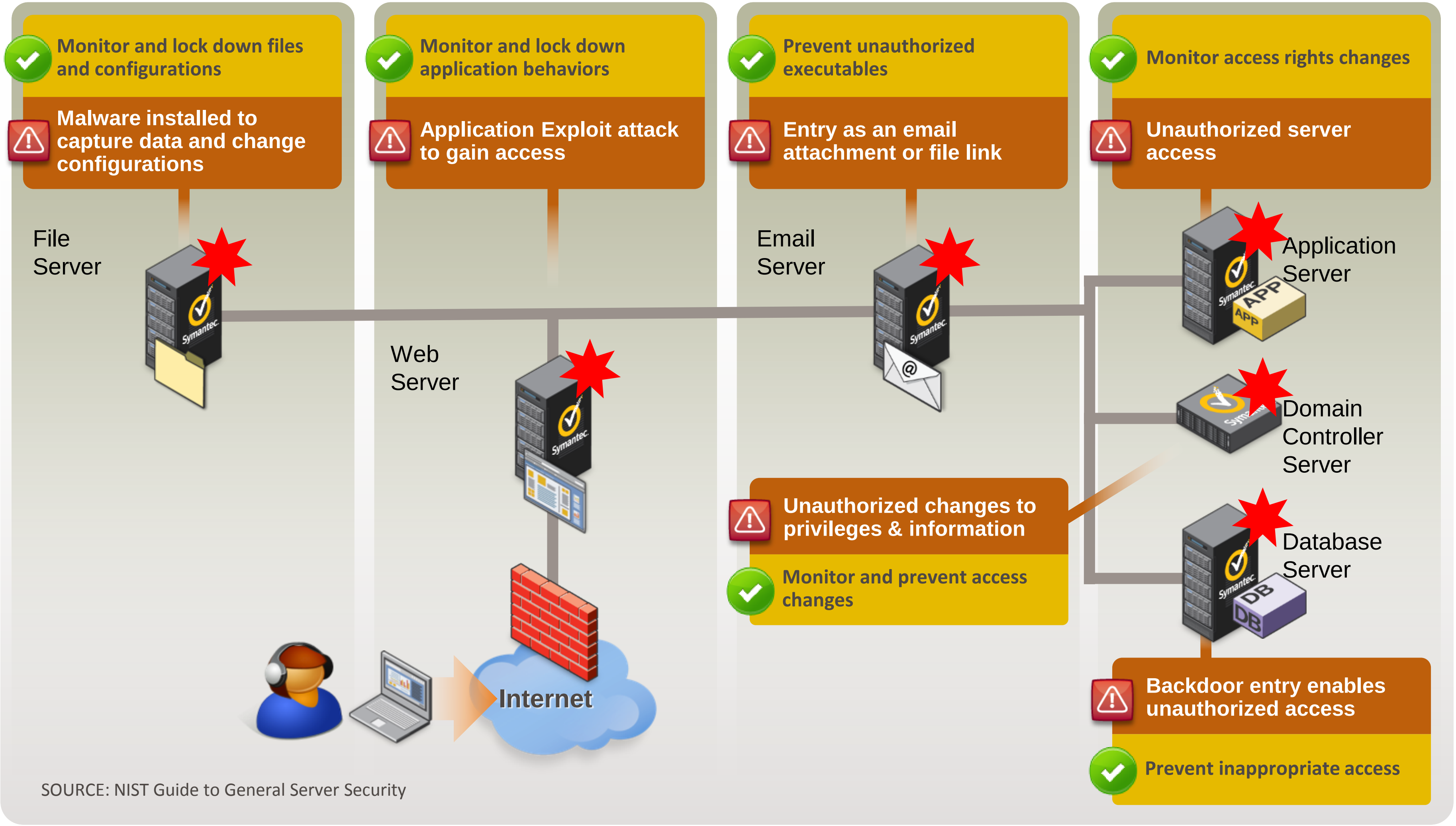
Critical File Monitoring and Protection

Security Risk Addressed/ Review Progress	Past Behavior	Fix
World-writable directory 🟡 ⇨ 🟢	Web application **configuration files** were **world –writable exposing** them to an external **attacker** to be able to **modify important application characteristics**	Included **file system checks** in build **scripts**. Protect and monitor critical system files with a **critical file monitoring solution**.



Critical System Protection

Stop Internal & External Attacks To Servers



✓ Monitor and lock down files and configurations

⚠ Malware installed to capture data and change configurations

✓ Monitor and lock down application behaviors

⚠ Application Exploit attack to gain access

✓ Prevent unauthorized executables

⚠ Entry as an email attachment or file link

✓ Monitor access rights changes

⚠ Unauthorized server access

⚠ Unauthorized changes to privileges & information

✓ Monitor and prevent access changes

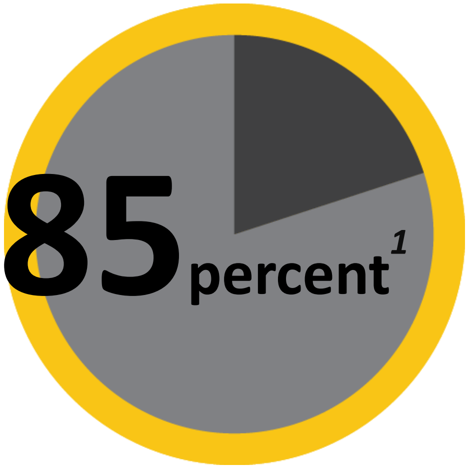
⚠ Backdoor entry enables unauthorized access

✓ Prevent inappropriate access

SOURCE: NIST Guide to General Server Security

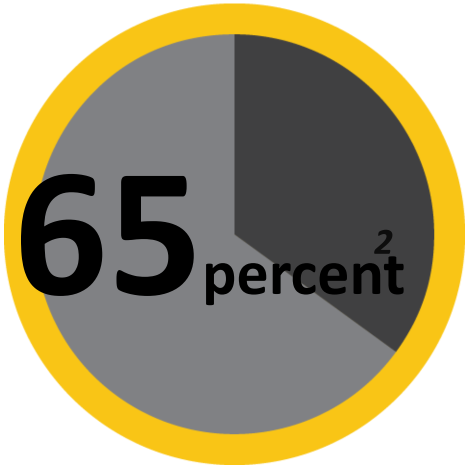
Data Security at the endpoint

Changes In Working Style moving to mobile



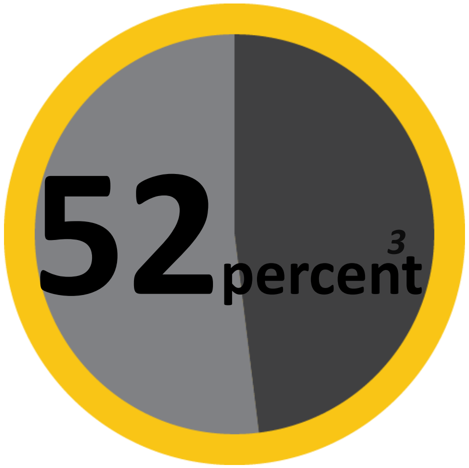
85 percent[1]

…of net new software built in 2013 will be built for cloud delivery.



65 percent[2]

…of enterprises allow mobile access to their network.

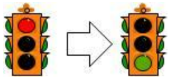


52 percent[3]

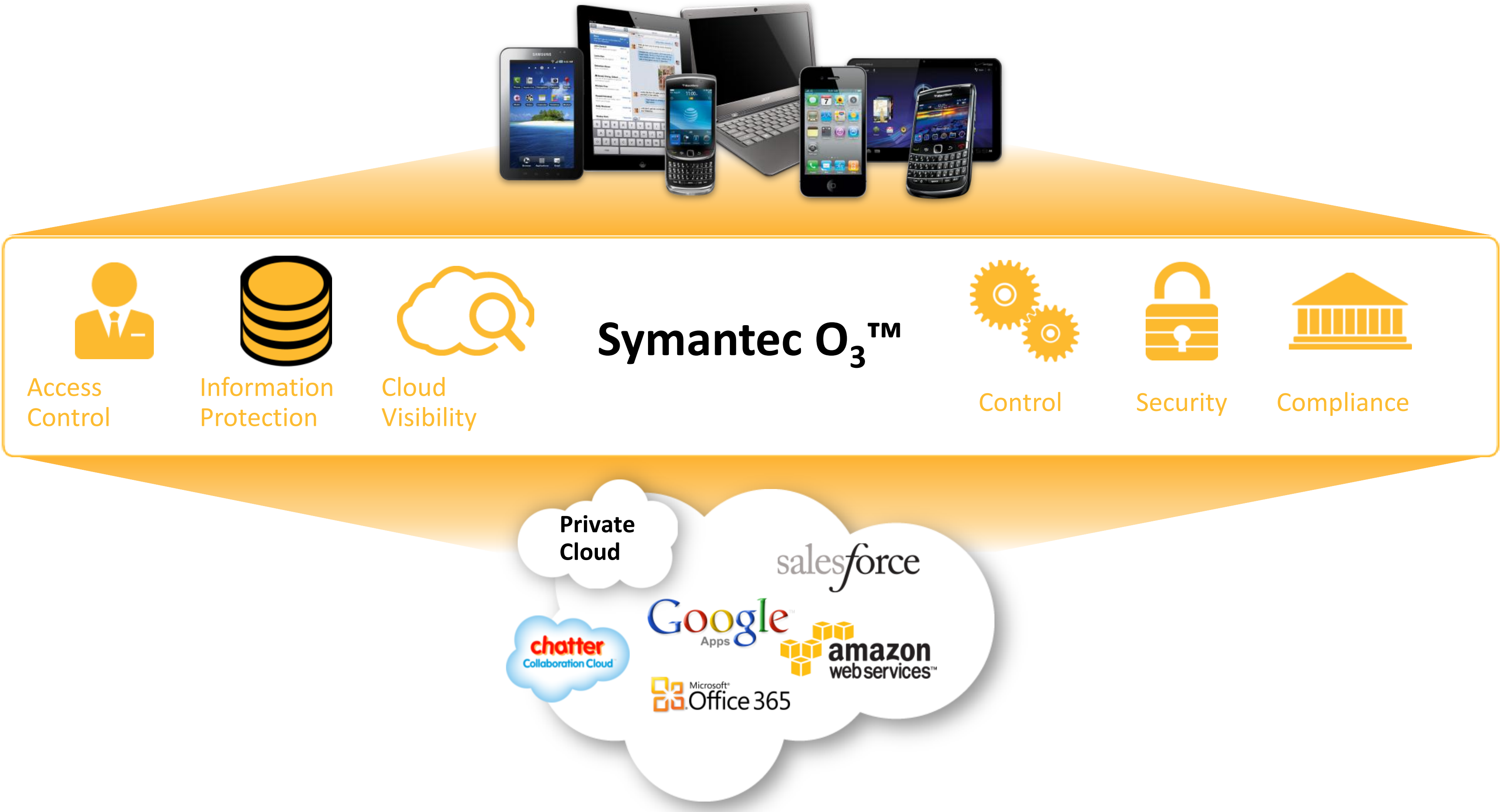
…of info workers use three or more devices for work.

1. IDC, "IDC Directions 2013 Presentation", Robert Mahowald, March 2013
2. The Impact of Mobile Devices on Information Security: A Survey of IT Professionals, Check Point, (January 2012), http://www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report.pdf
3. Info Workers Using Mobile And Personal Devices For Work Will Transform Personal Tech Markets, Frank E. Gillett, Forrester Research, Inc., 22 February, 2012

Addressing the endpoint

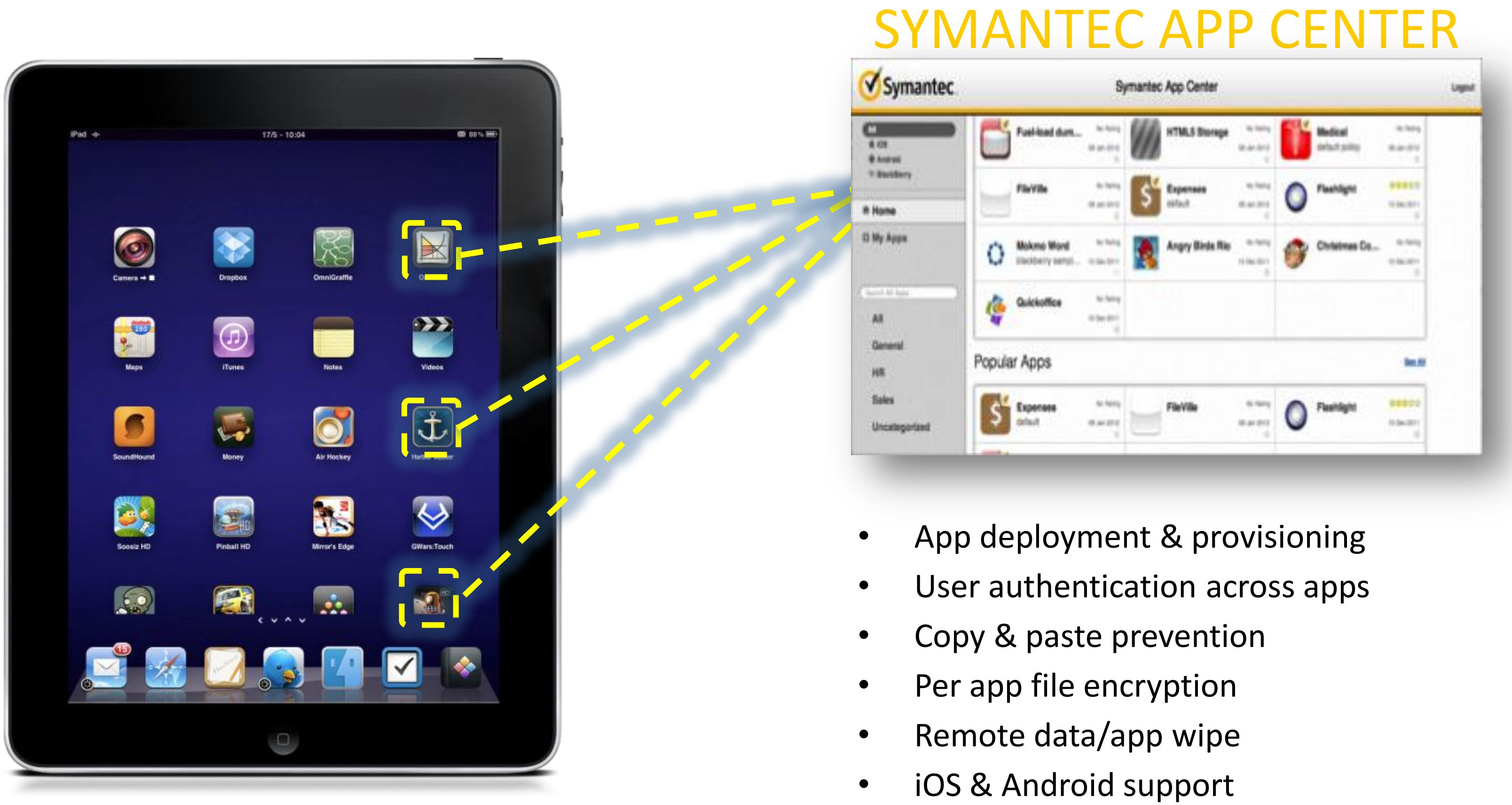
Security Risk Addressed/ Review Progress	Past Behavior	Fix
Allowing application access from BYOD 	Allowed access to web and mobile applications from non-corporate owned devices. **Data** is frequently **misused** and **stored insecurely violating state and federal regulations** as well as **possible theft or data loss**.	**Implement endpoint security**

Introducing Symantec O_3
A New Cloud Information Protection Platform



Symantec App Center

Mobile App & Data Protection for iOS, Android & HTML5



- App deployment & provisioning
- User authentication across apps
- Copy & paste prevention
- Per app file encryption
- Remote data/app wipe
- iOS & Android support

Symantec App Center Ready Program

- New Symantec mobility technology program
- Extends containerization to third-party public apps
- Delivery through vendor app stores
- **Apps delivered with Symantec security built-in**

Symantec
App
Center
Ready

Partners

Moxier Mail

Enterprise Email with direct push

Polaris Office

Mobile Office to edit MS Office docs

Good Reader

PDF reader with annotation features

iKonic Mail

Secure access to enterprise email

Xavy

Connects to MS Lync & Office Communicator

iAnnotate

Read, Annotate and Share PDF documents

Picsel SmartOffice

View and edit
MS Office files

Call to action

- Let HP and Symantec help you dramatically improve your application and data security
  - Symantec Contact: keith_mozena@symantec.com
  - HP Contact: allen.haws@hp.com.
- Require, Architect, and Design security in, such as with HP CATA (HP Comprehensive Applications Threat Analysis)
  - http://www.hp.com/go/CATA
  - Including IEEE Security & Privacy article reprint – Resilient Security Architecture
- Build security early and throughout SDLC
  - Requirements, architecture, design: e.g. HP CATA
  - Implementation: e.g. HP Fortify Static Code Analyzer (SCA)
  - Testing: e.g. HP Fortify WebInspect
  - Decide which multi-platform security solutions from Symantec address CATA findings

Q&A

**We can protect what matters.
Together.**