



Innovation
that Matters

Secure:
**How Prepared are You for
Data Loss Risks in the
Mobile Environment?**

Cecil Siu

**Security Solution Manager, Global Technology Services
IBM Hong Kong**

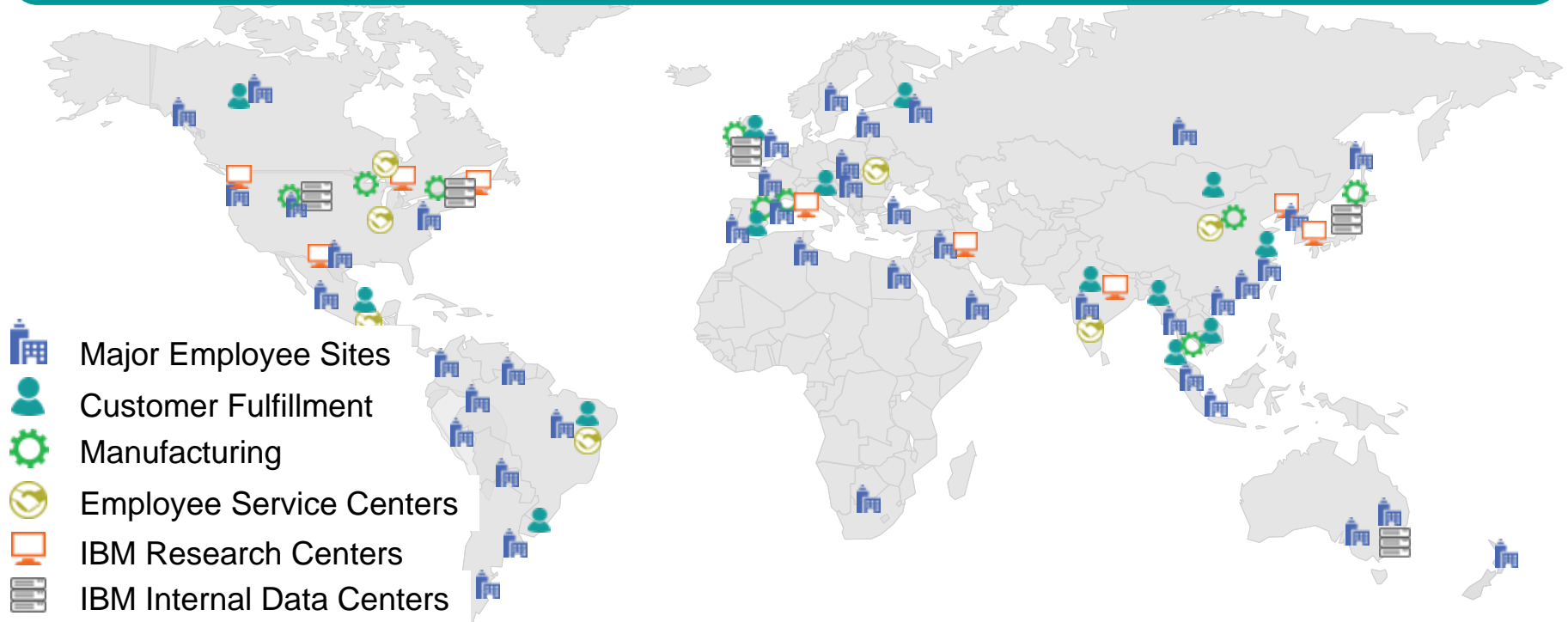


The Enterprise Today

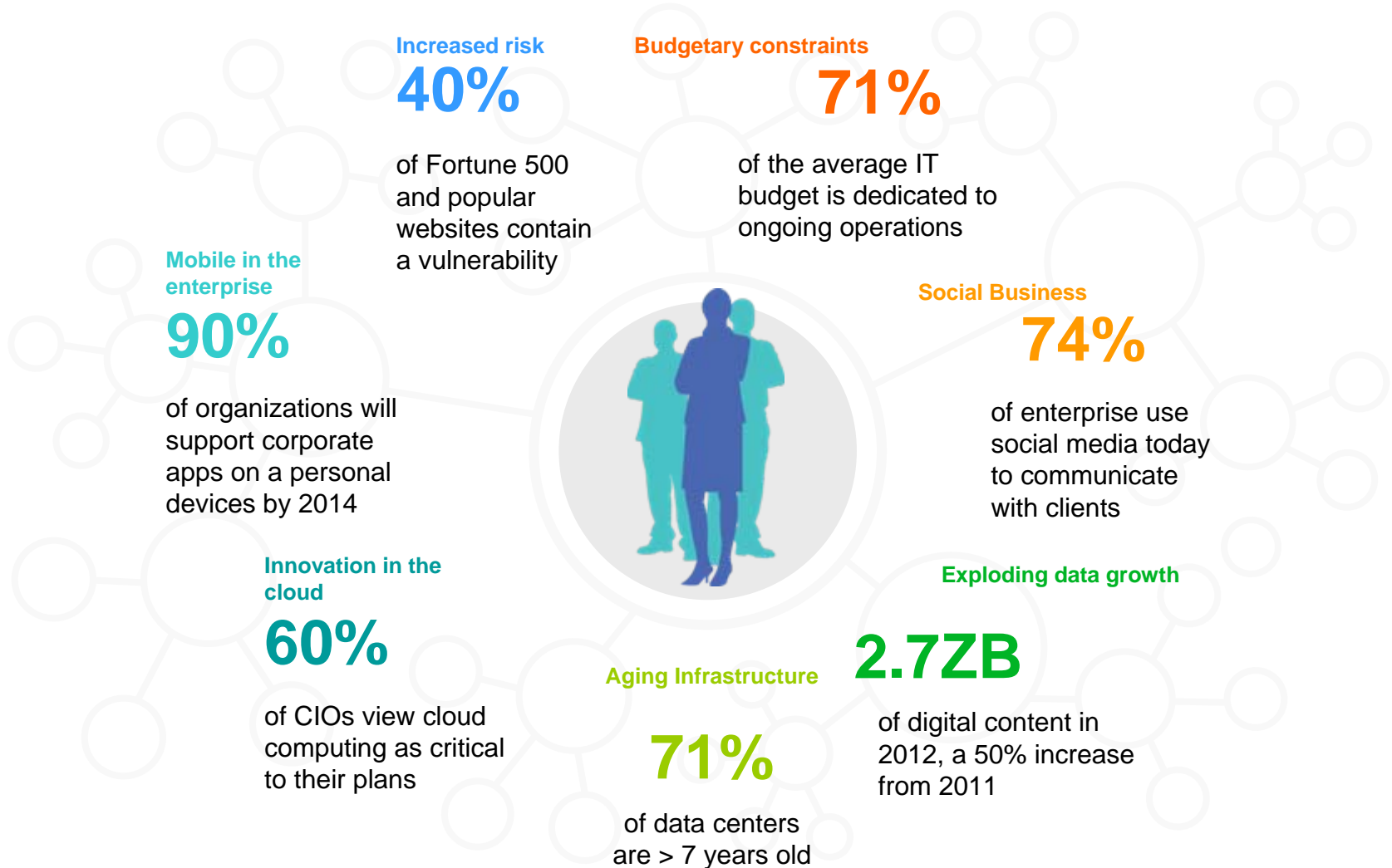
IBM is well qualified to secure the enterprise

One of the largest and most complex internal IT infrastructures in the world

- 2,000+ major sites
- 400,000+ employees
- 800k+ traditional endpoints
- 170+ countries
- Approx. 200,000+ contractors
- ~50% of employees are mobile



CxOs are under increasing pressure to deliver transformative business value— with limited resources available



In IBM's recent 2012 CISO study, security leaders shared their views on how the landscape is changing



Nearly two-thirds say **senior executives** are paying **more attention** to security issues.



2/3s expect to **spend more** on security over the next two years.



External threats are rated as a **bigger challenge** than internal threats, new technology or compliance.



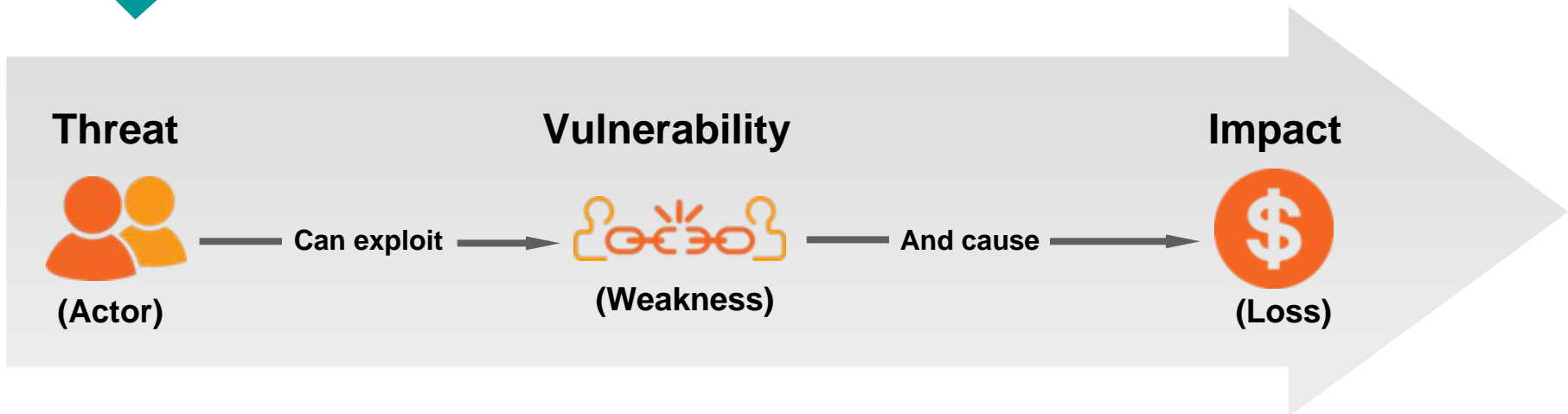
More than one-half say **mobile security** is their greatest near-term **technology concern**.



The changing dynamics of securing the enterprise

Think like a security expert

Security Risk exists when....



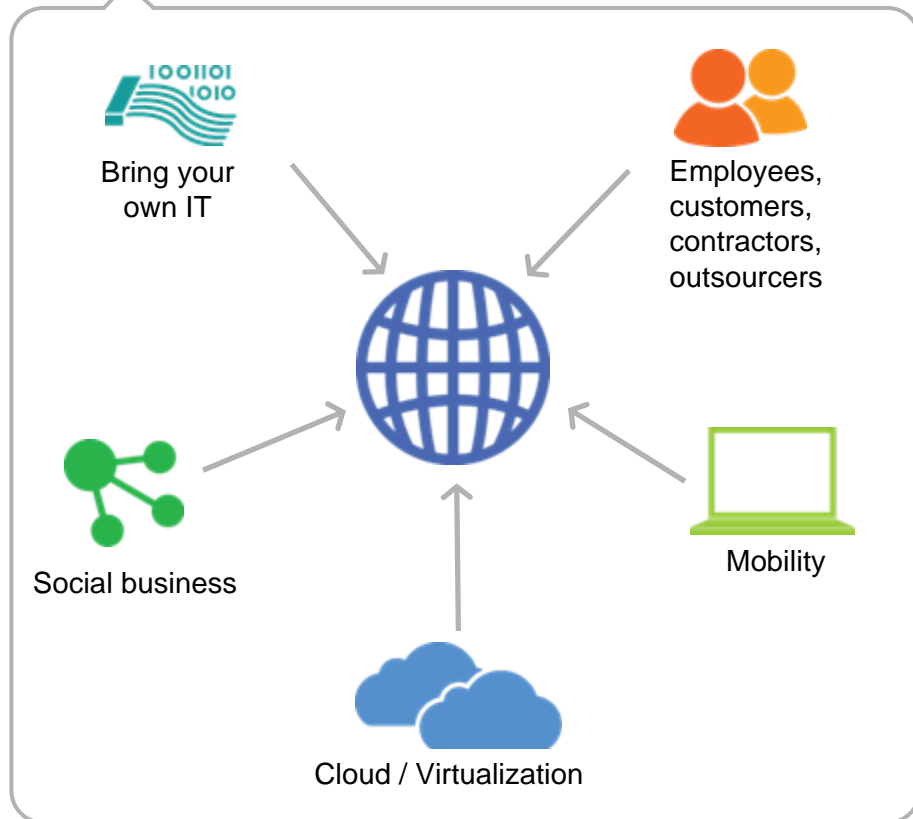
Security Risk Management is the application of **control** to detect and block the threat, to detect and fix a vulnerability, or to respond to incidents (impacts) when all else fails.

Threats (Actors) are More Sophisticated

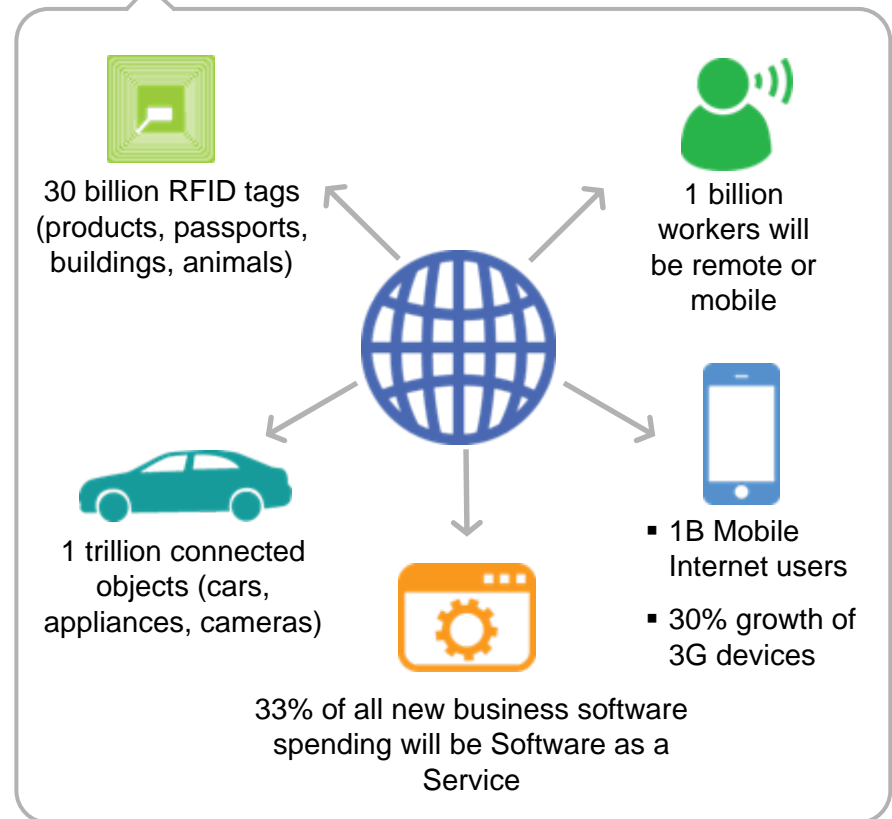
Threat Name	Inadvertent Actor	Opportunist	Hacktivist	Advanced, Persistent Threat/Mercenary
Types	<ul style="list-style-type: none"> Insiders - Employees, Contractors, Outsourcers 	<ul style="list-style-type: none"> Worm and Virus Writers Script Kiddies 	<ul style="list-style-type: none"> White Hat and Black Hat Hackers “Protectors of Internet freedoms” 	<ul style="list-style-type: none"> National Governments Organized Crime Industrial Spies Terrorist Cells
% of Incidents attributable	60%	20%	=<10%	=<10%
Threat Profile	<ul style="list-style-type: none"> Inexperienced No funding Causes harm inadvertently by unwittingly carrying viruses, or posting, sending or losing sensitive data Increasing in prevalence with new forms of mobile access and social business 	<ul style="list-style-type: none"> Inexperienced Limited funding Opportunistic Behavior Target known vulnerabilities Use viruses, worms, rudimentary trojans, bots Acting for thrills, bragging rights Easily detected 	<ul style="list-style-type: none"> Inexperienced to higher-order skills Target known vulnerabilities Prefer Denial of Service Attacks BUT use malware as means to introduce more sophisticated tools Detectable, but hard to attribute Increasing in prevalence 	<ul style="list-style-type: none"> Sophisticated tradecraft Foreign intelligence agencies, organized crime groups Well financed Target technology as well as information Often acting for profit Target and exploit valuable data Establish covert presence on sensitive networks Difficult to detect Increasing in prevalence

Number of vulnerabilities increase radically with emergence of new business models and technologies

Adopting new business models, and embracing new technologies



Exploding and Interconnected digital universe





Security essentials for CIOs

IBM developed 10 essential practices required to achieve security intelligence


Essential Practices



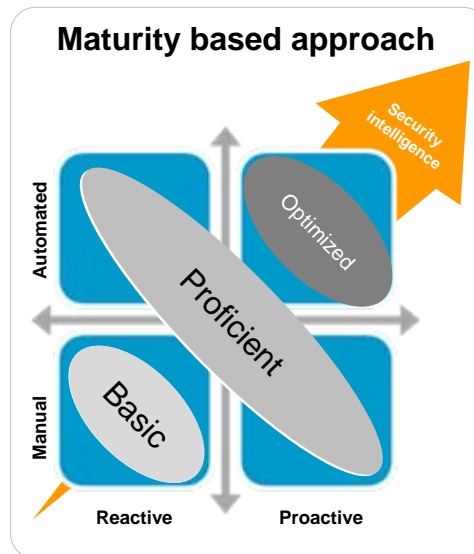
1. Build a risk aware culture and management system

6. Control network access and assure resilience







2. Manage security incidents with intelligence




7. Address new complexity of cloud and virtualization






3. Defend the mobile and social workplace


8. Manage third party security compliance






4. Secure services, by design


9. Secure data and protect privacy





5. Automate security "hygiene"

10. Manage the identity lifecycle



IBM Services to help you manage your security challenges



9. Secure data and protect privacy

- Data Security & Privacy Strategy & Assessment
- Data Loss Prevention
- Data Encryption
- Database Security Assessment & Architecture
- Big Data Security Architecture
- Database Auditing & Monitoring
- Data Masking

IBM is helping to solve essential security challenges – world wide

Secure data and protect privacy

A large Canadian pharmaceutical company improves its ability to protect against internal and external threats with an IBM Information Security Assessment

Control network access & assure resilience

A Danish dairy company protects users and its infrastructure from malicious content and limits administration

Defend mobile and social workplace

A leading manufacturer in India identifies potential security threats, strengthens its security levels and improves customer confidence

Manage 3rd party security compliance

A US Retailer identifies gaps to achieve Payment Card Industry (PCI) compliance

Address new complexity of cloud & virtualization

An urban services organization in Portugal, improves employee productivity through e-mail filtering and cloud/managed security services

Secure services by design

A bank in Kuwait gains a better view of its security posture and network vulnerabilities by conducting real-world security testing

Build a risk aware culture

An Austrian bank conglomerate establishes a consistent security policy with IBM Security Services



Websense - An IBM Partner in Data Loss Prevention



- Websense Technical Manager for Asia Pacific
- Join Websense in 2003
 - Previously served at Sun, IBM and Lucent
- Technology Advisory Role in
 - Business Processing Outsourcing
 - People Support (Philippines)
 - Casino, Resort, Entertainment and Retail
 - KFC (Philippines)
 - Melco Crown (Macau)
 - MGM Grand (Macau)
 - Galaxy Entertainment (Macau)
 - High Tech Manufacturing
 - HTC (Taiwan)
 - ZTE (China)
 - Oil & Gas
 - PETRONAS (Malaysia)
 - TV Cable Operator
 - Astro (Malaysia)
- Government
 - Hong Kong Sport Institute (Hong Kong)
 - National Security Bureau (Taiwan)
- Financial Services Industry
 - AIA (Asia Pacific)
 - Bank Of China (Hong Kong)
 - China Merchant Bank (China)
 - China Construction Bank Asia (Hong Kong)
 - China Taiping Insurance (HK and China)
 - Citi Bank International (HK and China)
 - Octopus (Hong Kong)
 - PingAn Insurance (China)
 - Shanghai Commercial Bank (HK /TW)
 - TouchNGo (Malaysia)

Websense : An IBM Partner



websense

- ✓ Over 1400 Employee from 26 offices in 35 Countries and 4 Support Centers Worldwide
- ✓ HQ in San Diego and Development Centers in US, UK, China and Israel
- ✓ Over 50 thousand customers and 42 million subscription seats world wide
- ✓ Global ThreatSeeker Network and SaaS Infrastructure with 15 x ISO 27001 Certified Data Centers
- ✓ 47 patents granted worldwide, 106 patents pending and 30 in submission

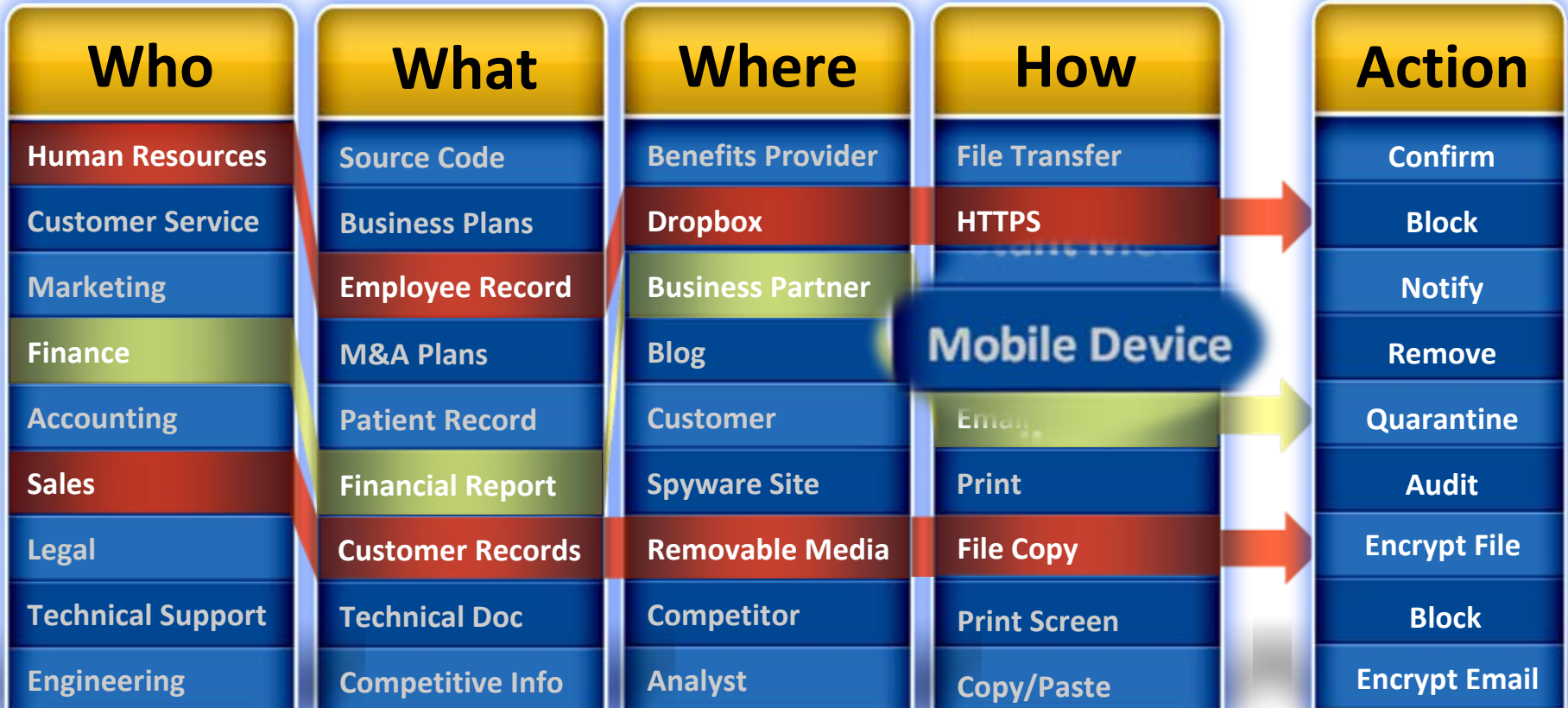
Websense : An IBM Partner



websense

- ✓ Gartner Data Loss Prevention MQ: Leaders Quadrant - 2008, 2009, 2010 and 2011
- ✓ Gartner Secure Web Gateway MQ: Leaders Quadrant - 2010, 2011 and 2012
- ✓ Gartner Secure Web Gateway Worldwide Market Share Leader, 2010, 2011
- ✓ Forrester Wave™: Email Content Security: Leader Wave - Q4 2012
- ✓ IDC Web Security – Overall, Appliance and Software Market Share Leader – 2011

The "4-W" in Websense Data Loss Prevention Strategy



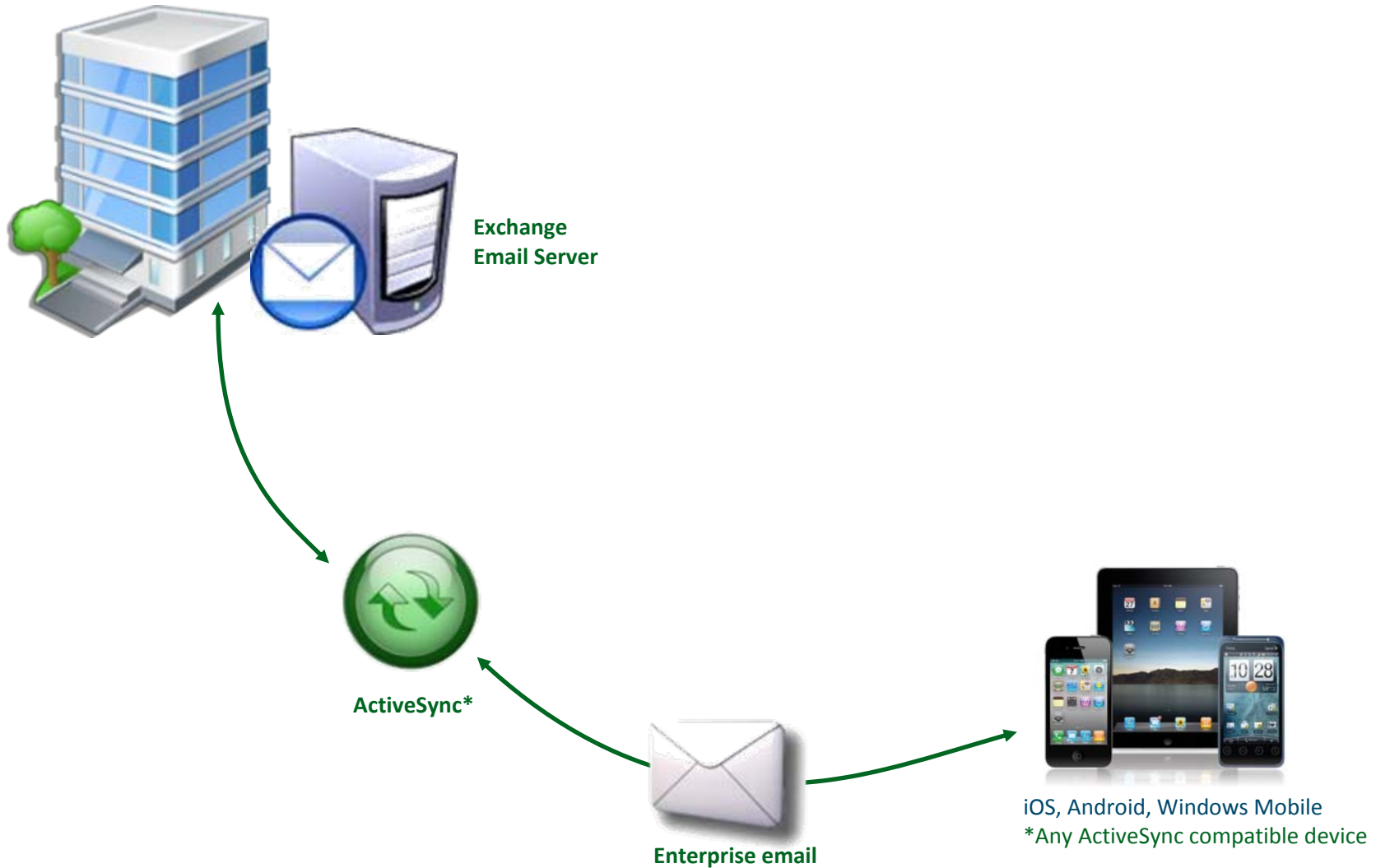
Mobile become the weakest link

- User owned device (BYOD)
- Mobile device lack the horse power for real content analysis
- Container only secure data at rest
- Lack of consistence DLP policy for mobile device
- How you track if sensitive data are getting onto the device ?

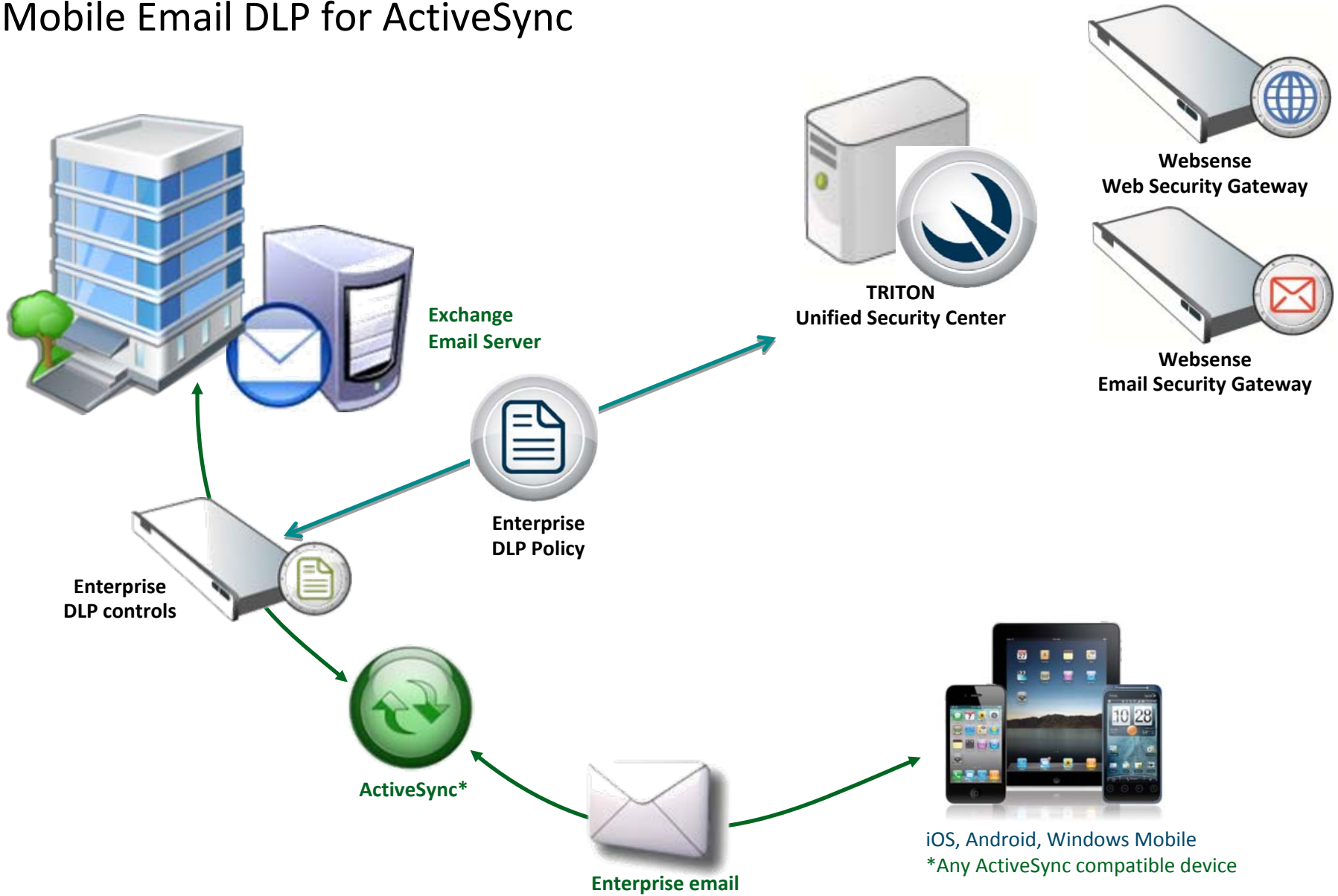


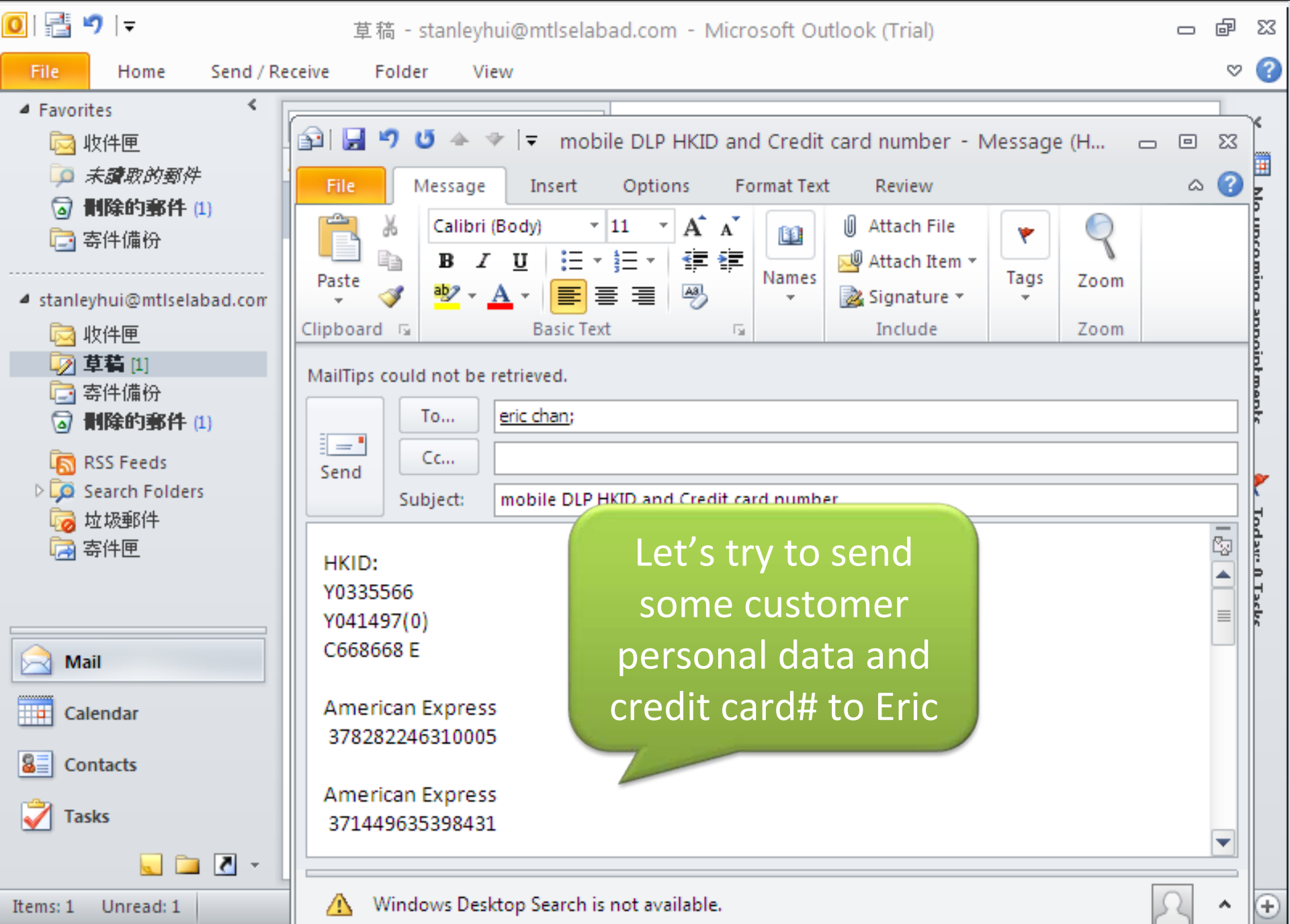
Microsoft ActiveSync

– the most common channel for accessing sensitive data from mobile device



Mobile Email DLP for ActiveSync





- Favorites
 - 收件匣
 - 未讀取的郵件
 - 刪除的郵件 (1)
 - 寄件備份
- stanleyhui@mtltselabad.com
 - 收件匣
 - 草稿 [1]
 - 寄件備份
 - 刪除的郵件 (1)
 - RSS Feeds
 - Search Folders
 - 垃圾郵件
 - 寄件匣

File Message Insert Options Format Text Review

Paste Clipboard Basic Text Names Include Tags Zoom

Calibri (Body) 11

B *I* U [List Icons]

Attach File Attach Item Signature

MailTips could not be retrieved.

To... eric chan;

Cc...

Subject: mobile DLP HKID and Credit card number

Let's try to send some customer personal data and credit card# to Eric

HKID:
Y0335566
Y041497(0)
C668668 E

American Express
378282246310005

American Express
371449635398431

- Favorites
 - 收件匣 (1)
 - 未讀取的郵件
 - 寄件備份
 - 刪除的郵件 (17)
- ericchan@mtiselabad.com
 - 收件匣 (1)
 - 草稿
 - 寄件備份
 - 刪除的郵件 (17)
 - RSS Feeds
 - Search Folders
 - 垃圾郵件
 - 寄件匣

- Search 收件匣 (Ctrl+E)
- Arrange By: Date Newest on top
- Today
 - stanley hui 10:09 AM mobile DLP HKID an...
 - stanley hui 9:55 AM mobile DLP solution...
 - Last Week
 - administrator Thu 1... [i] Message blocked:...
 - stanley hui Thu 11/15 DB info
 - administrator Thu 1... [i] Message blocked:...
 - stanley hui Thu 11/15 mobile DLP
 - administrator Thu 1... [i] Message blocked:...
 - stanley hui Thu 11/15 email cotains HKID
 - stanley hui Thu 11/15 normal email start
 - eric chan Thu 11/15 test

mobile DLP HKID and Credit card number

stanley hui

Sent: Fri 11/23/2012 10:09 AM
To: eric chan

HKID:
Y0335566
Y041497(0)
C668668 E

American Express
378282246310005

American Express
371449635398431

American Express Corporate
378734493671000

Australian BankCard
5610591081018250

Diners Club

Windows Desktop Search is not ava...

Eric can receive the email from Outlook Mail Client on his desktop

Inbox (1)

2 of 2



Mailboxes **Inbox (1)** Edit

Details

Search Inbox

administrator 10:09 AM

[!] Message blocked: mobile DLP HKI...
You received an email message from stanley hui on 23 Nov. 2012. The message contain...

stanley hui 9:54 AM

mobile DLP solution start
mobile DLP solution start

But Eric can not download the same email to his iPad

Inbox



2 of 2



From: administrator

Details

[!] Message blocked: mobile DLP HKID and Credit card number

November 23, 2012 10:09 AM

You received an email message from stanley hui [on 23 Nov. 2012](#).
The message contains data that cannot be downloaded to mobile devices based on corporate policy.

Please use your laptop or desktop to view the original message.

Original subject: mobile DLP HKID and Credit card number

Attachments:

From: stanley hui

Sent: [23 Nov. 2012](#)

Message type: Email

The warning message explain why it was blocked

- File Home
- Favorites
 - 收件匣
 - 未讀取的郵件
 - 寄件備份
 - 刪除的郵件
- ericchan@mtlsla
 - 收件匣
 - 草稿
 - 寄件備份
 - 刪除的郵件
 - RSS Feeds
 - Search Fold
 - 垃圾郵件
 - 寄件匣
- Mail
- Calendar
- Contacts
- Tasks

mobile DLP sensitive data - Message (HTML)

File Message

Delete Respond Quick Steps Move Tags Editing Zoom

From: stanley hui Sent: Fri 11/23/2012 10:20 AM
To: eric chan
Cc:
Subject: mobile DLP sensitive data

Message Data Security Deployment and Installation Guide v7.5_634172342439726475.pdf (3 MB)

The *Data Security Management Server* is the core of the system, providing complete data loss prevention analysis to the network. In addition, the Management Server gathers and stores all management data for reporting purposes, analysis can be shared among a number of users. The protector can provide added blocking capabilities. The protector works in tandem with the Data Security Management Server performs discovery and blocking capabilities, while the protector sits on the network to monitor or block the traffic, as needed. The protector also monitors HTTP, FTP, Generic Text and IM traffic (chat and instant messaging). The protector is also an integration point for third-party solutions that support ICAP. The protector fits into your existing network with minimum configuration and

Windows Desktop Search is not available.

Now I send a few paragraphs extracted from a sensitive document

Inbox (1)

2 of 3



Mailboxes

Inbox (1)

Edit

Search Inbox

administrator

10:20 AM

[!] Message blocked: mobile DLP sensi...
You received an email message from stanley hui on 23 Nov. 2012. The message contain...

administrator

10:09

[!] Message blocked: mobile DLP HKI...
You received an email message from stanley hui on 23 Nov. 2012. The message contain...

stanley hui

9:54

mobile DLP solution start
mobile DLP solution start

Credit card numbery hui [on 23 Nov. 2012.](#)

downloaded to mobile devices based on corporate

Details

The email was also
blocked from
downloading to the
iPad

Inbox

1 of 3



From: administrator

[Details](#)**[!] Message blocked: mobile DLP sensitive data**

November 23, 2012 10:20 AM

You received an email message from stanley hui [on 23 Nov. 2012](#).

The message contains data that cannot be downloaded to mobile devices based on corporate policy.

Please use your laptop or desktop to view the original message.

Original subject: mobile DLP sensitive data

Attachments:

From: stanley hui

Sent: [23 Nov. 2012](#)

Message type: Email

Not just structure
data but also
unstructured text
can be identified

Web Security

Data Security

Email Security

Mobile Security

Main

Settings

Now let's take a look at the incident from the TRITON Unified Security Center

- Reporting
 - Data Loss Prevention
 - Mobile Devices
 - Discovery
- Policy Management
 - DLP Policies
 - Discovery Policies
 - Content Classifiers
 - Resources
- Status
 - System Health
 - Endpoint Status
 - Mobile Status
 - Traffic Log
 - System Log
 - Audit Log

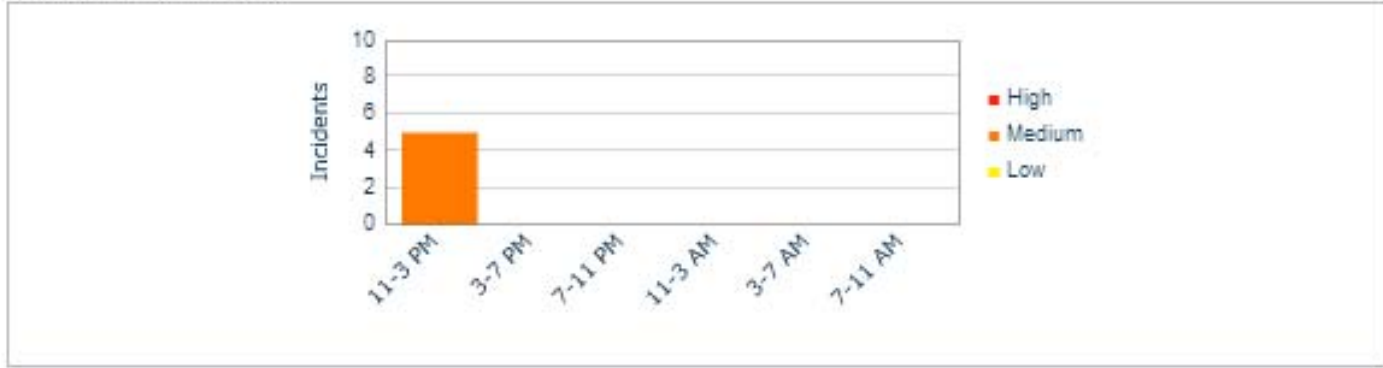
Today

Health Alert Summary

- [Your subscription is valid](#)
- [8 data loss prevention and mobile policies are configured](#)
- [No discovery policies are configured](#)
- [3 missing essential configurations](#)

Data Loss Prevention Incidents - Data collected over the last 24 hours

Incidents by Severity



Last data loss prevention incident received at: **22 Nov. 2012, 11:56:09 AM**

Web Security

Data Security

Email Security

Mobile Security

Main

Settings

- Reporting
 - Data Loss Prevention
 - Mobile Devices**
 - Discovery
- Policy Management
 - DLP Policies
 - Discovery Policies
 - Content Classifiers
 - Resources
- Status
 - Today
 - System Health
 - Endpoint Status
 - Mobile Status
 - Traffic Log
 - System Log
 - Audit Log

Mobile Incidents (last 3 days)

Workflow Remediate Escalate

Report: Mobile Incidents (last 3 days)

Showing 2 incident(s)

<input type="checkbox"/>	ID	Incident Time	Source	Policies	Severity	Action
<input type="checkbox"/>	262609	23 Nov. 2012, 10:20:26 AM	stanley hui	sensitive DLP	Medium	Quarantined
<input type="checkbox"/>	263046	23 Nov. 2012, 10:09:38 AM	stanley hui	PCI; Hong Kong PII	High	Quarantined

Incident: **262609** Severity: Medium Action: **Quarantined** Synched by: user

Display: Violation triggers

- Rule: sensitive DLP**
- private (Key Phrase) 1
 - file server fingerprint (PreciseID Fingerprinting - F... 2

Forensics Properties History

From: stanley.hui
 To: "eric chan" <ericchan@mtlslab.com>
 Subject: **mobile DLP sensitive data**
 Attachments: Data Security Deployment a...
 Message Body

The Data Security Management Server performs data loss prevention analysis to the network. The Data Security Management Server gathers and stores data for analysis. For security purposes, analysis can be shared among...

Web Security

Data Security

Email Security

Mobile Security

Main

Settings

Mobile Incidents (last 3 days)

Workflow Remediate Escalate

Report: Mobile Incidents (last 3 days)

I can see both incidents being captured

Report: Mobile Incidents (last 3 days)

Date Range: Last 3 Days

Showing 2 incident(s)

ID	Incident Time	Source	Policies	Severity	Action	Synced by	Maximum Matches	Transaction Size	Status
262609	23 Nov. 2012, 10:20:26 AM	stanley hui	sensitive DLP	Medium	Quarantined	1 user(s)	2	4.71 MB	New
263046	23 Nov. 2012, 10:09:38 AM	stanley hui	PCI; Hong Kong PII	High	Quarantined	1 user(s)	14	2.48 KB	New

Incident: 262609 Severity: Medium Action: Quarantined Synced by: 1 user Tune Policy

Display: Violation triggers

Rule: sensitive DLP

- private (Key Phrase) 1
- private
- file server fingerprint (PreciseID Fingerprinting - F... 2
- \\172.20.13.203\c\$\Users\administrator.MTLSELABAD\

Forensics Properties History

From: stanley hui Sent: 23 Nov. 2012, 10:19:38 AM
 To: "eric chan" <ericchan@mtlselabad.com>
 Subject: mobile DLP sensitive data
 Attachments: Data Security Deployment and Installa...e v7.5 634172342439726475.pdf(4.7 MB)

Message Body Show as: Marked HTML

I can see what triggered the blocking and which policy was violated

I can see the forensics including a copy of the email message and attachment too

The Data Security Management Server is the core of the system, providing complete data loss prevention analysis to the network. In addition, the Data Security Management Server gathers and stores all management statistics. For load balancing purposes, analysis can be shared among a number of Data Security servers.

- Reporting
- Data Loss Prevention
- Mobile Devices
- Discovery

Mobile Incidents (last 3 days)

Workflow Remediate Escalate

Report: Mobile Incidents (last 3 days)

Showing 2 incident(s)

It also show me the status of the incident, the action taken and the all the related details

Incident: 262609 Severity: Medium Action: Quarantined Synched by:

Display: Violation triggers

- Rule: sensitive DLP
 - private (Key Phrase) private 1
 - file server fingerprint (PreciseID Fingerprinting - F... \\172.20.13.203\c\$\Users\administrator.MTLSELABAD\D... 2

Forensics Properties History

Incident Details	
Transaction type:	Email
Total synchronizations:	1
Severity:	Medium
Status:	New
Action:	Quarantined
Released incident:	No
Channel:	Mobile Airsync
Analyzed by:	Policy Engine protector-7788
Detected by:	Mobile Airsync Agent on protector-7788
Event time :	23 Nov. 2012. 10:19:38 AM

- System Health
- Endpoint Status
- Mobile Status
- Traffic Log
- System Log
- Audit Log

- file server fingerprint (PreciseID Fingerprinting - F... \\172.20.13.203\c\$\Users\administrator.MTLSELABAD\D...

Severity:	
Status:	
Action:	
Released incident:	
Channel:	
Analyzed by:	
Detected by:	
Event time :	

It also show me what has been done to this incident, e.g. who was notified, who has release the incident, etc.

- Reporting
- Data Loss Prevention
- Mobile Devices
- Discovery

Mobile Incidents (last 3 days)

Workflow Remediate Escalate

Report: Mobile Incidents (last 3 days)

Showing 2 incident(s)

Incident: 262609 Severity: Medium Action: Quarantined Synched by: 1 user

Display: Violation triggers

- Rule: sensitive DLP
 - private (Key Phrase) private 1
 - file server fingerprint (PreciseID Fingerprinting - F... \\172.20.13.203\c\$\Users\administrator.MTLSELABAD\D... 2

Forensics Properties History

Find: [search box]

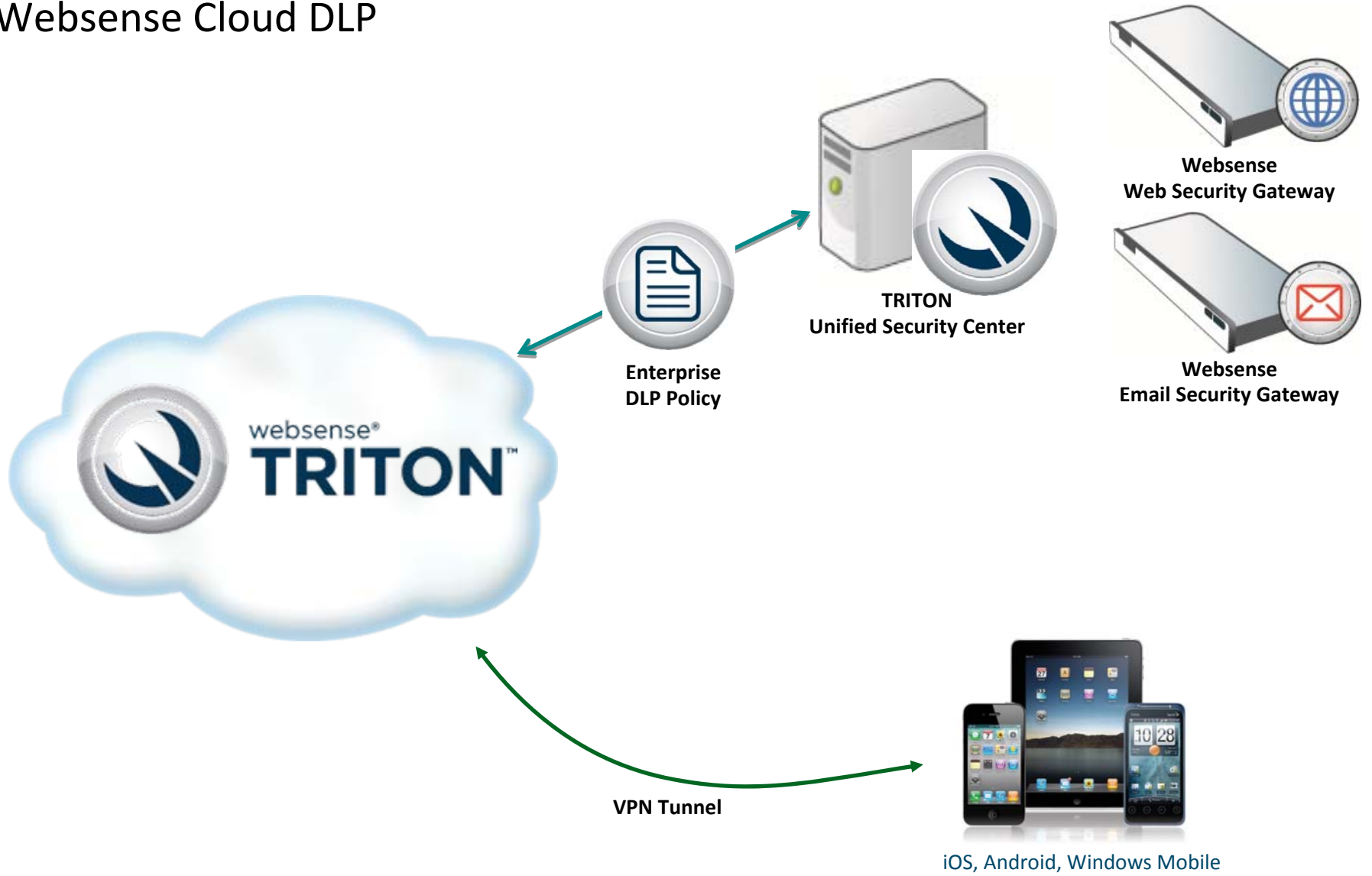
- 23 Nov. 2012, 10:20:5... system Notification with incident details was mailed
- Notification with incident details was mailed
- Comments: Notification was mailed to Administrator@mtlselabad.com
- 23 Nov. 2012, 10:20:2... system Detected and recorded incident
- Detected and recorded incident

- System Health
- Endpoint Status
- Mobile Status
- Traffic Log
- System Log
- Audit Log

- private
- file server fingerprint (PreciseID Fingerprinting - F... \\172.20.13.203\c\$\Users\administrator.MTLSELABAD\D...

- 23 Nov. 2012, 10:20:5... system Notification with incident details was mailed
- Comments: Notification was mailed to A
- 23 Nov. 2012, 10:20:2... system Detected and recorded incident

Websense Cloud DLP



Summary

- Mobile can be part of your Enterprise DLP Strategy

