



Borderless security update



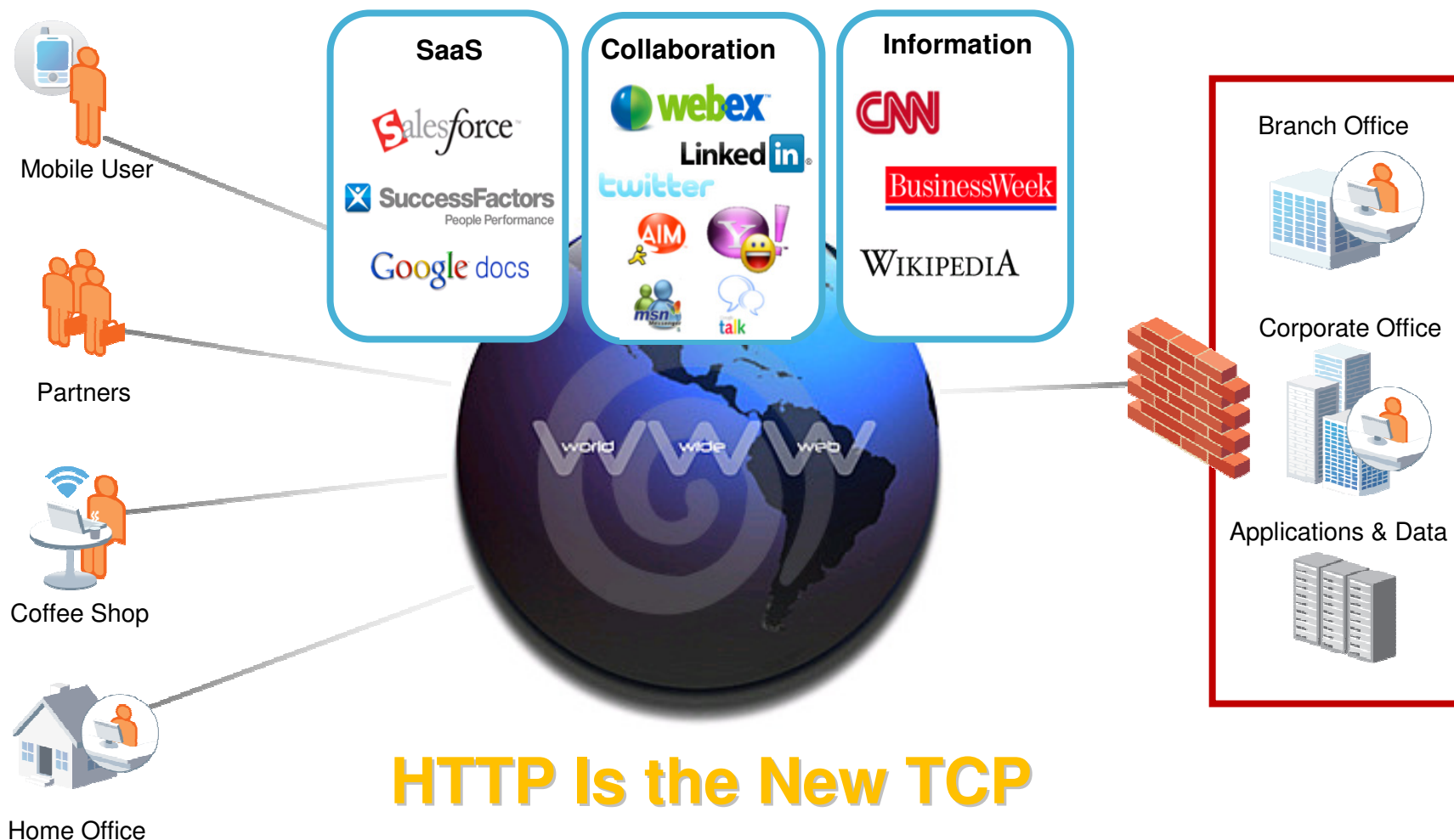
Tatjana Boskovic,
tboskovi@cisco.com

Finance event,
Belgrade, 21st January 2010

Fighting the Last War



Web: Enabling the Borderless Experience

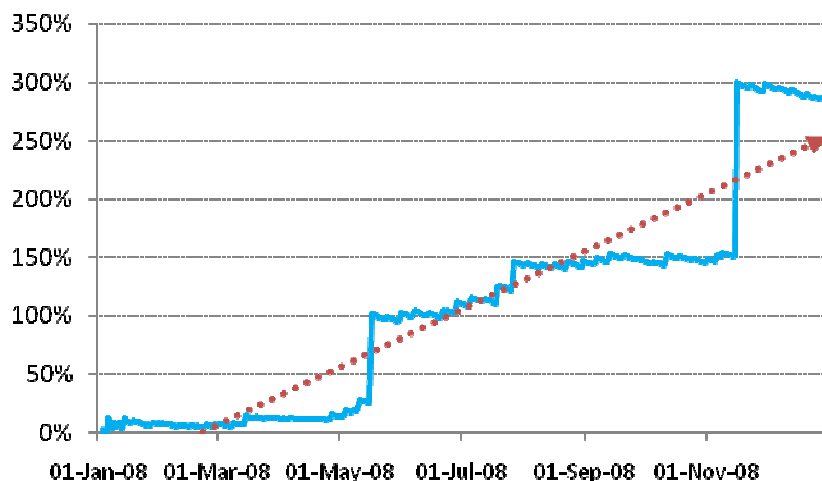


Web Business Challenges



Malware Threats & the Dark Web

2008 Volume Ratio Change
(Malware Blocks Relative to All Requests)



- 300% yearly volume increase in 2008
- Exploits and iframes up 1,731%
- 4,995% increase in data theft trojans in two years

Botnets on the Prowl

Zeus and Clampi: Botnets that steal online account credentials with a focus on bank accounts

- Zeus Trojan is estimated to have infected 3.6 million computers as of October 2009
- The newer Clampi Trojan is estimated to have infected hundreds of thousands of computers

The Dark Web

*80% of the web is uncategorized,
highly dynamic or unreachable by
web crawlers*

- Botnets
- Dynamic content
- Password protected sites
- User generated content
- Short life sites

The Known Web
20% covered by URL lists

Malware



Acceptable Use Violations

Acceptable Use Violations & the Dark Web

Legacy URL Filtering Effectiveness is Decreasing



- Legacy URL filtering primarily focuses on crawling and manual review/classification
- Databases add thousands of new URLs per day...while the web adds a Billion
- 95% of the web will be uncategorized by 2015

How Does the DCA Engine Work?

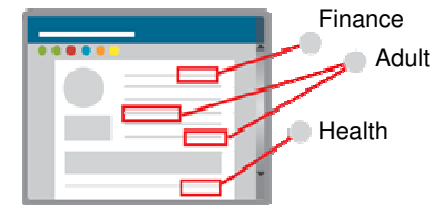
1. User requests unknown webpage.



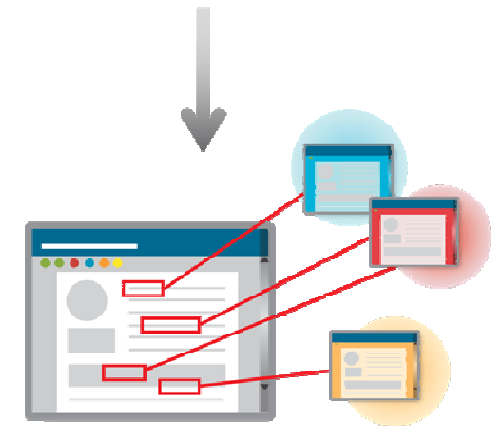
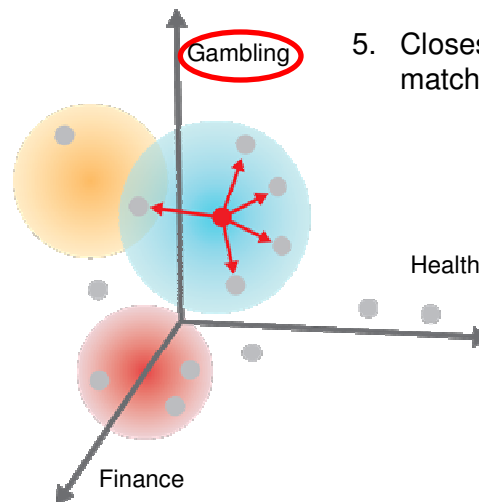
2. HTTP response received. Scan response to **identify relevant text**.



3. Calculate **content vector**. Each dimension is a score of the document's relevance to a particular category.



5. Closest category match is returned.



4. Calculate proximity of document's vector to the vectors of **model documents**.



6. Policy for category match is enforced: Block / Allow / Warn.

Data Loss Prevention

Data in the Network



salesforce.com
experience success.™

facebook®

Cisco
webex

Challenges

- Multiple enforcement points
- Accurate and consistent policies
 - Administrative overhead

Data at the End Point



Smart
Phones



Laptops

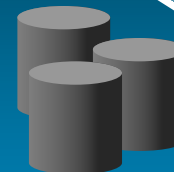


Kiosks

Fileservers



Disk Arrays

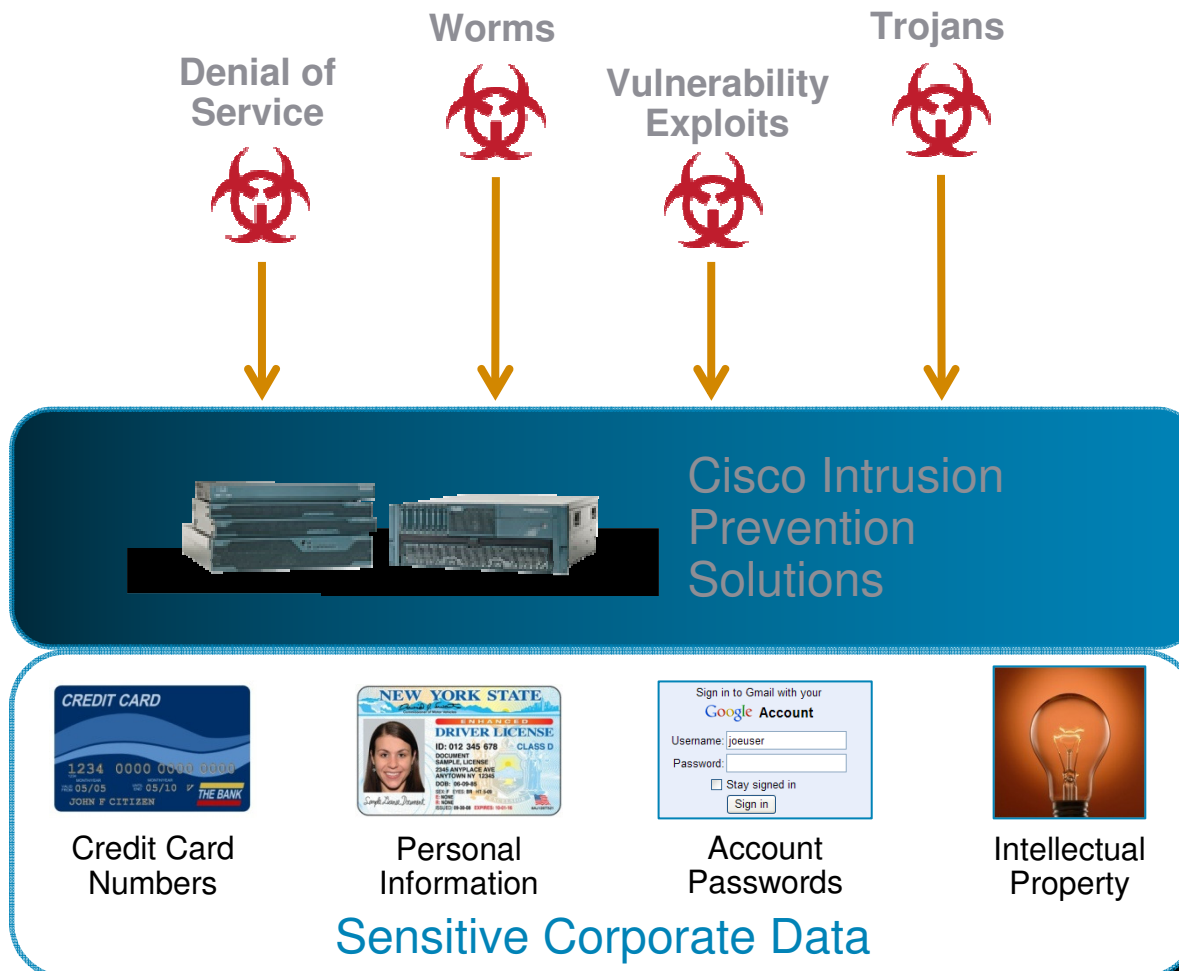


Databases

Data in the Datacenter

Protecting the Network: IPS

Stop Attackers from Accessing Your Network



- Stop attacks over any protocol
- Signature updates stop known attacks
- IP reputation filters and global correlation prevents unknown exploits
- Central to PCI architectures

How does the real world look like?

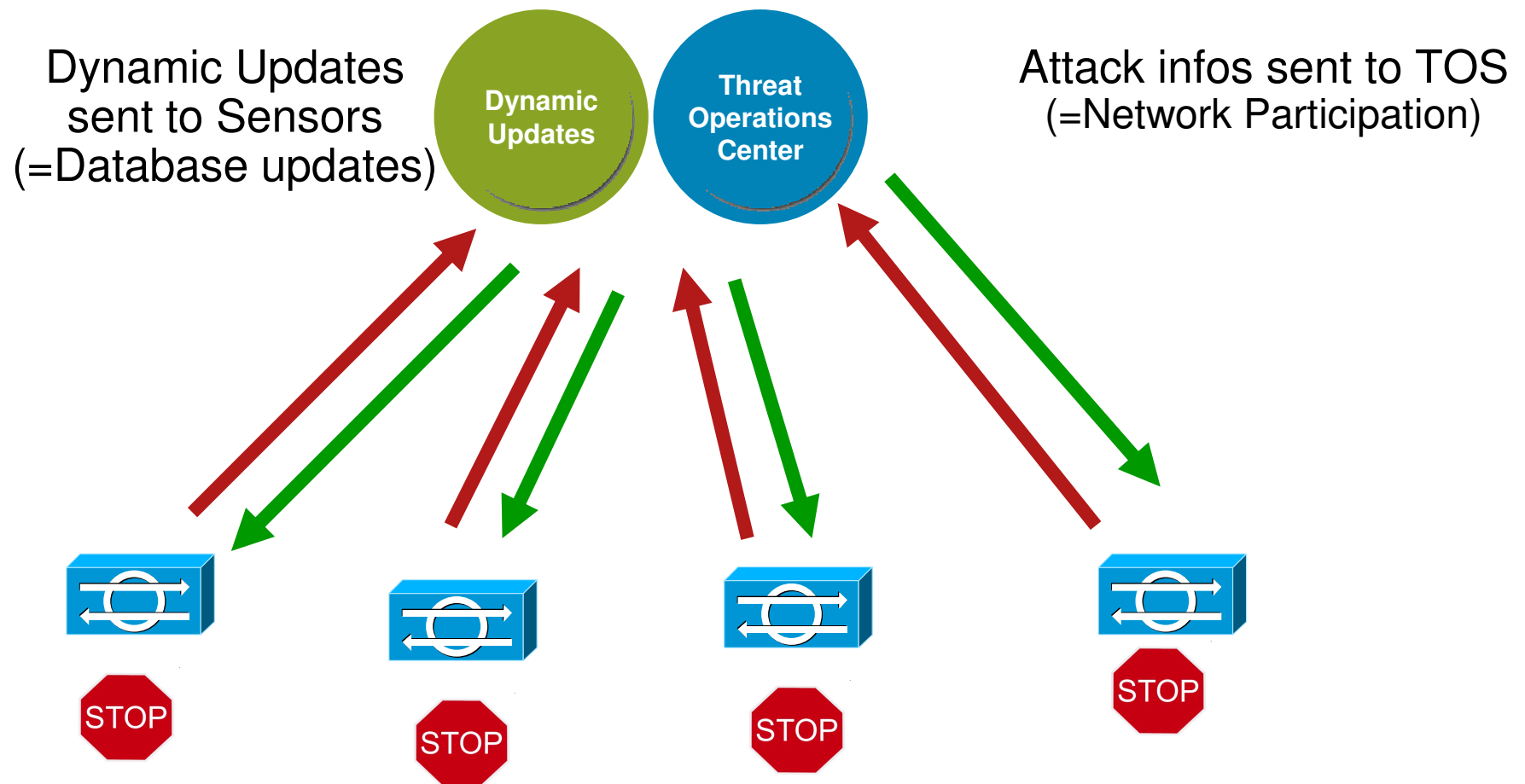
Lots of different and constantly mutating attacks

Single Sensor is only seeing part of the picture

Single Sensor can only try to react when something has already hit him...



Knowledge Sharing = Global Correlation!



Attacks stopped!

Global Correlation

Full Context Analysis: Seeing the Whole Picture

LARGEST FOOTPRINT | GREATEST BREADTH | **FULL CONTEXT ANALYSIS**

What?

Content

Who?

How?

Where?

Global Correlation

Full Context Analysis: Seeing the Whole Picture

LARGEST FOOTPRINT | GREATEST BREADTH | **FULL CONTEXT ANALYSIS**

What?

Content

Who?

Reputation of Counterparty

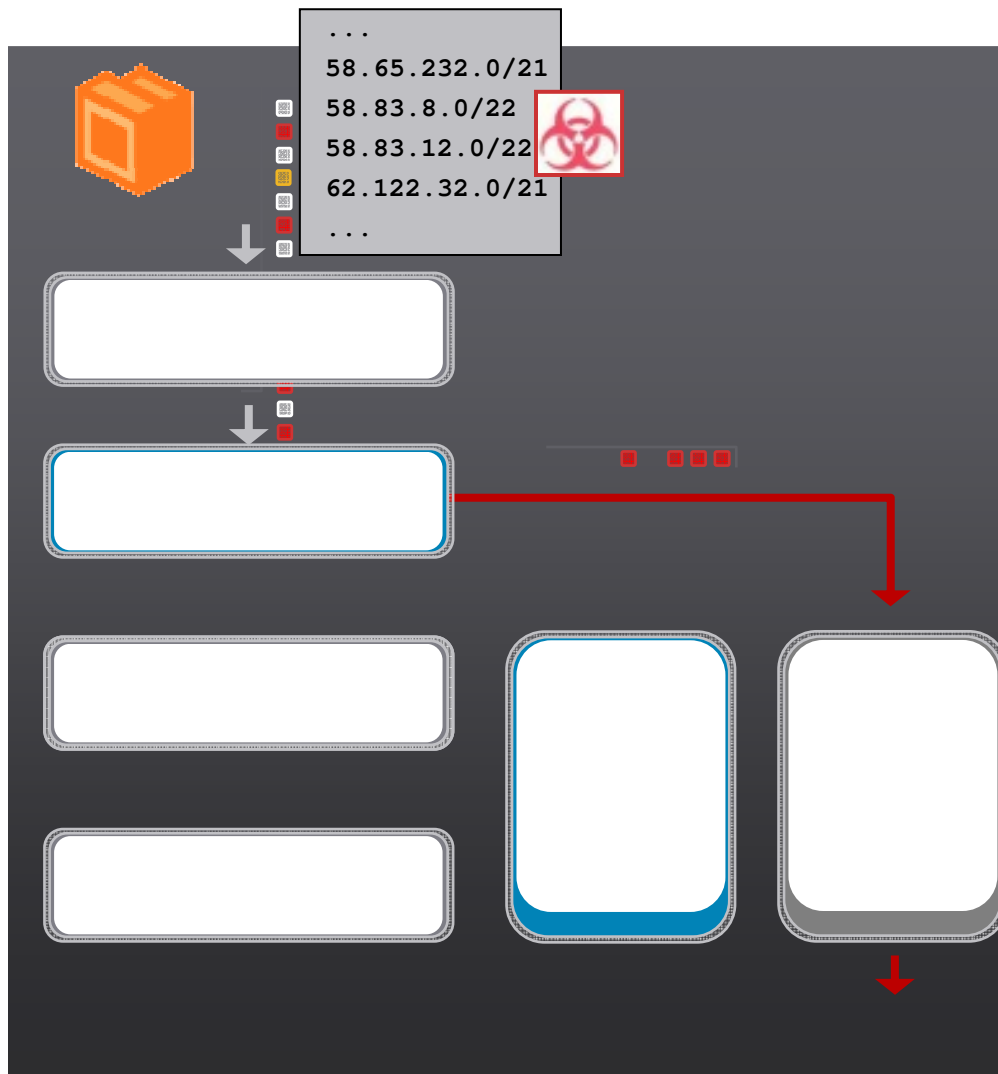
How?

Propagation & Mutation Methods

Where?

Geographic & Vertical Trends

IPS Reputation Filters: Blocking the worst bad apples



- Some networks on the Internet are owned wholly by malicious organizations or are hijacked 'zombie' networks
- Reputation Filters block access to these networks like an ACL
- Individual IP addresses do not go on this list because of things they do (An IP does not go from -1 to -9 to being put on this list)

Reputation Filters

Traditional IPS has to be Right on Every Attack

What SIGNATURES See

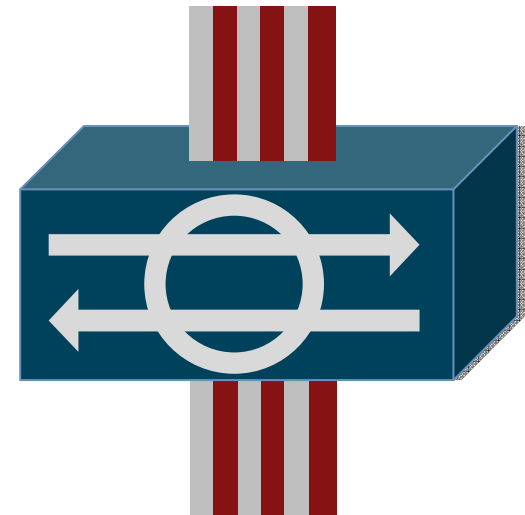
Verdict: **Has to be right every time**

What?

Potentially Hundreds of Different Attacks, C&C Traffic, etc

The Worst of the Worst on the Internet.

Instead of having to inspect and detect every attack they might send your way, IPS with Global Correlation allows you to Block that traffic with confidence.



Reputation Filters

Worst of the Worst are Blocked Outright

**What GLOBAL
CORRELATION Knows:**

Verdict: BLOCK

What?

Known Conficker Botnet sites

Who?

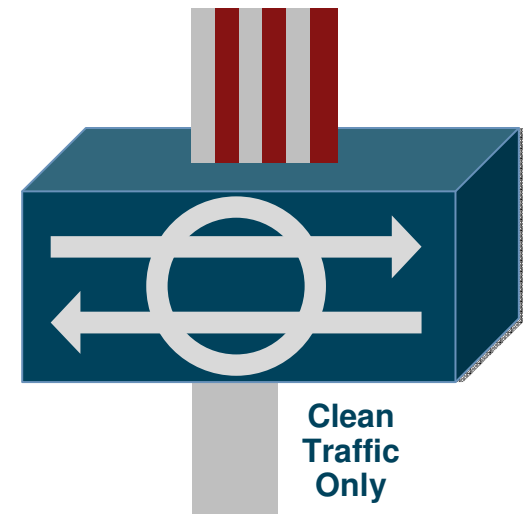
IP in Known Criminal Network

How?

All IP Traffic

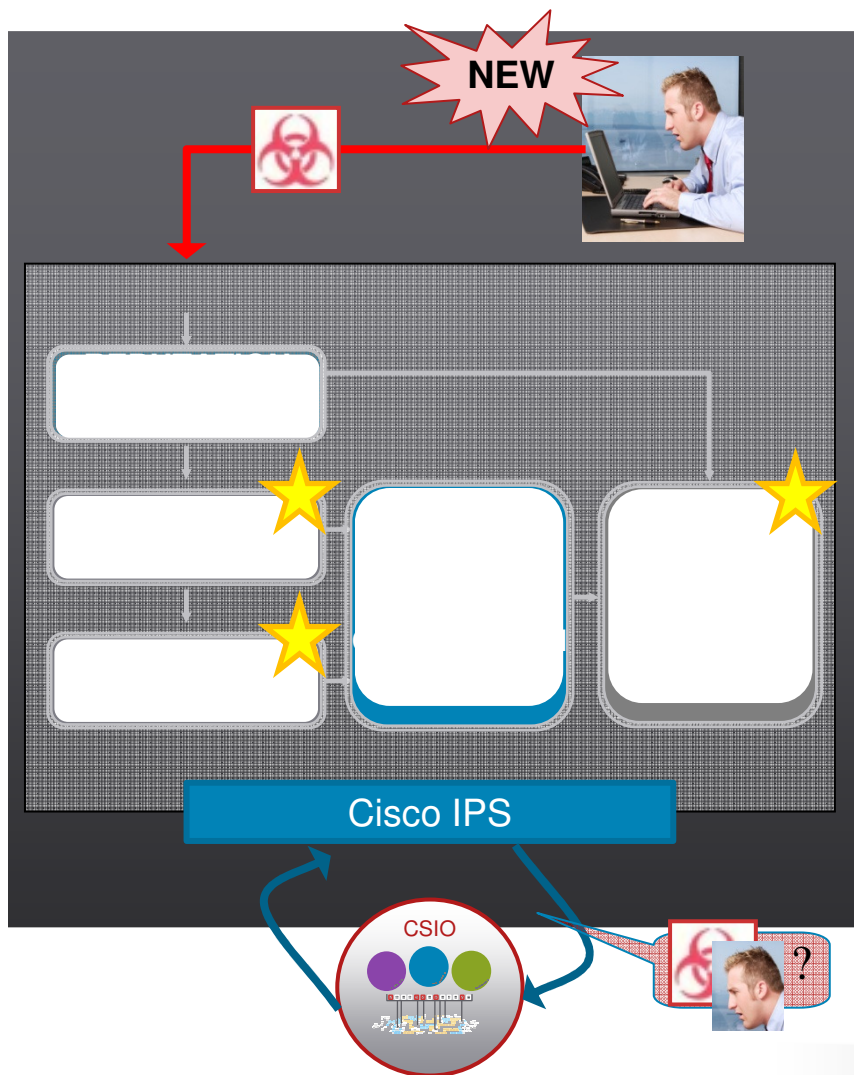
Where?

Anywhere in the World



Local Inspection will Always Matter

Example 1: Unknown Attacker



1. New Attacker hits the IPS
2. Attacker without a Reputation
3. Signatures or Anomaly Detection identify activity
4. The attack is handled according to the security policy implemented on the sensor (Deny if Risk Rating reaches threshold)
5. Information on the Attacker is sent back to CSIO to track his reputation (if configured)

Global Correlation Inspection

Example 2: Suspicious Attacker

Identified through Local Inspection, Denied due to Global Correlation



1. Suspicious Attacker attacks
2. Has medium Reputation
3. Signatures identify suspicious activity and give this a medium Risk Rating
4. Global Correlation adds context of Attacker Reputation to Risk Rating
5. Decision Engine blocks
6. Information on NEW Reputation is sent back to CSIO.

Global Correlation Network Participation: or “What is my sensor sending back to Cisco?”

Network Participation

Select the extent to which the sensor will contribute data to the SensorBase network.

- ☒ Off Do not contribute data to the SensorBase network.
- ☐ Partial Contribute data to the SensorBase network but withhold some potentially sensitive information.
- ☐ Full Contribute all alert data to the SensorBase network.

Network Participation Disclaimer

If you agree to participate in the SensorBase Network, Cisco will collect aggregated statistics about traffic sent to your IPS. This includes summary data on the Cisco IPS network traffic properties and how this traffic was handled by the Cisco appliances. We do not collect the data content of traffic or other confidential business or personal information. All data is aggregated and sent via secure HTTP to the Cisco SensorBase Network servers in periodic intervals. All data shared with Cisco will be anonymous and treated as strictly confidential.

The table below describes how the data will be used by Cisco.

Participation Level	Type of Data	Purpose
Partial	Protocol Attributes (e.g. TCP max, segment size and options string)	Track potential threats and understand threat exposure
	Attack Type (e.g. Signature Fired and Risk Rating)	Used to understand current attacks and attack severity
	Connecting IP Address and port	Identifies attack source
	Summary IPS performance (CPU utilization memory usage, inline vs. promiscuous, etc)	Tracks product efficacy
Full	Victim IP address and port	Detect threat behavioral patterns

Agree

Disagree

- Network Participation is entirely voluntary and on an Opt-In basis (off by default)
- No actual packet content data is ever sent back
- Partial participation sends back Attacker IP, port, Sig ID and Risk Rating, some protocol attributes and summary IPS performance data
- Full mode adds in Victim IP and port
- Private IP addresses are removed before sending

Defeating SQL Injection

The Challenge of Traditional Signature-Based IPS

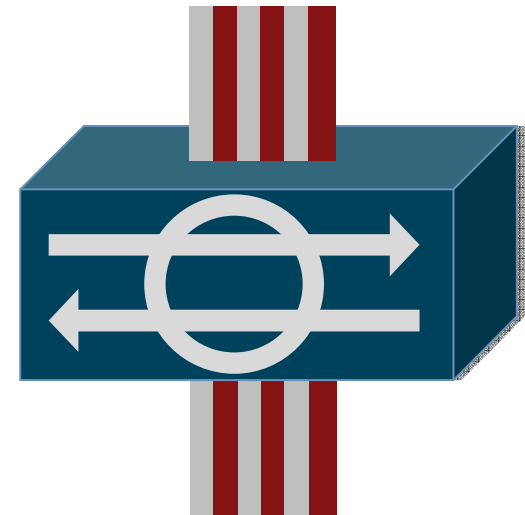
What SIGNATURES Find

Verdict: **UNKNOWN**

What?

SQL Command Fragments
in Web Traffic

This could be your billing system
talking to your customer database.
Or.....



Defeating SQL Injection

Collaborate with Confidence

**What GLOBAL
CORRELATION Knows:**

Verdict: BLOCK

What?

SQL Command Fragments
in Web Traffic from Untrusted Client

Who?

Dynamic IP Address
Dynamic DNS
History of Web Attacks

How?

4th Packet of HTTP Connection

Where?

Within Heavily Compromised
Network
History of Botnet Activity



Defeating SQL Injection

Collaborate with Confidence

Traditional Signature only IPS view without Reputation

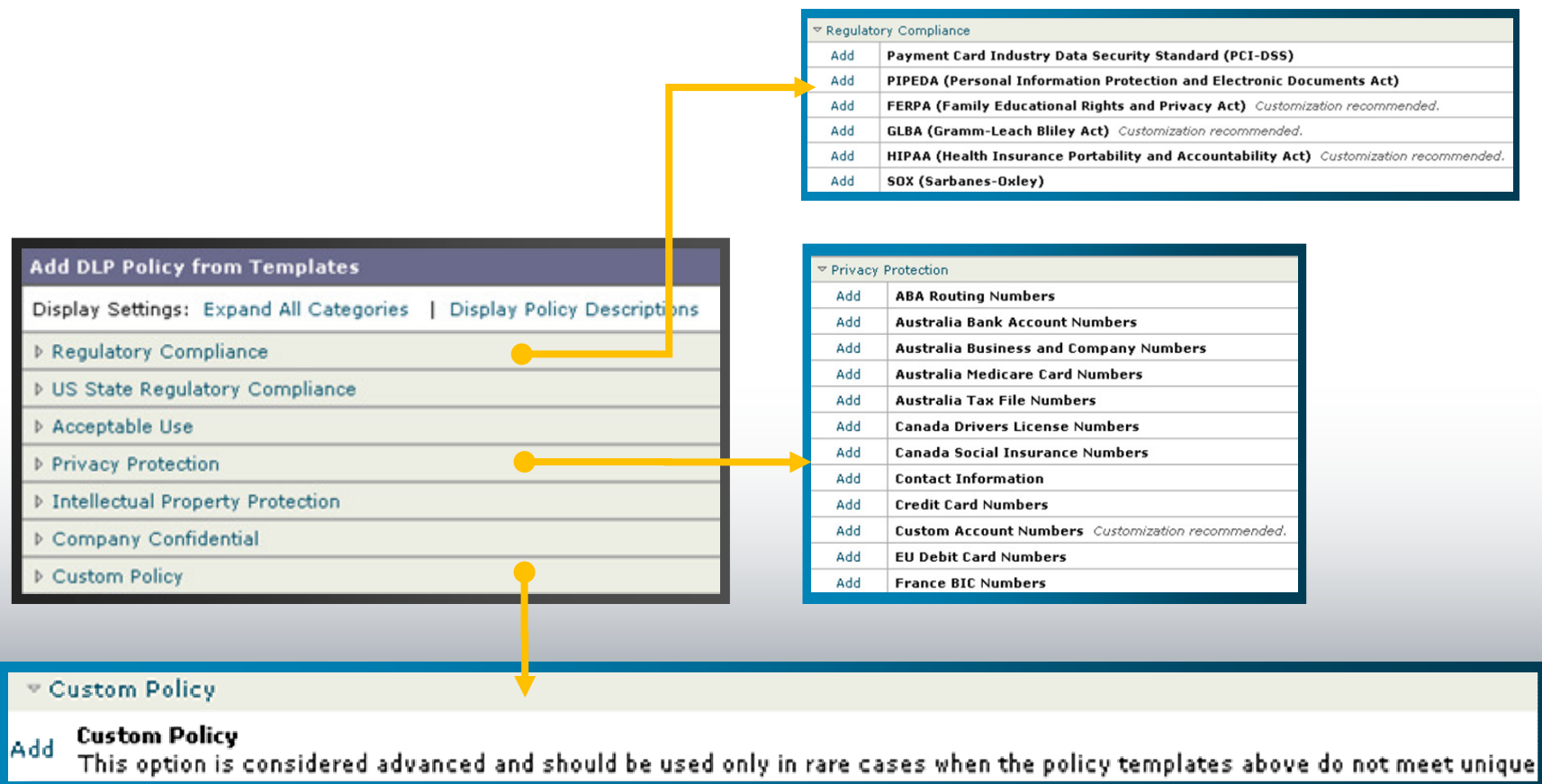


Risk Rating	Sig. Name	Actions Taken	Attacker IP
85	Generic SQL Injection		30.30.181.133
99	Generic SQL Injection	droppedPacket, deniedFlow, tcpOneWayResetSent	10.20.5.178

Global Correlation Enabled IPS allows Confident Deny Action

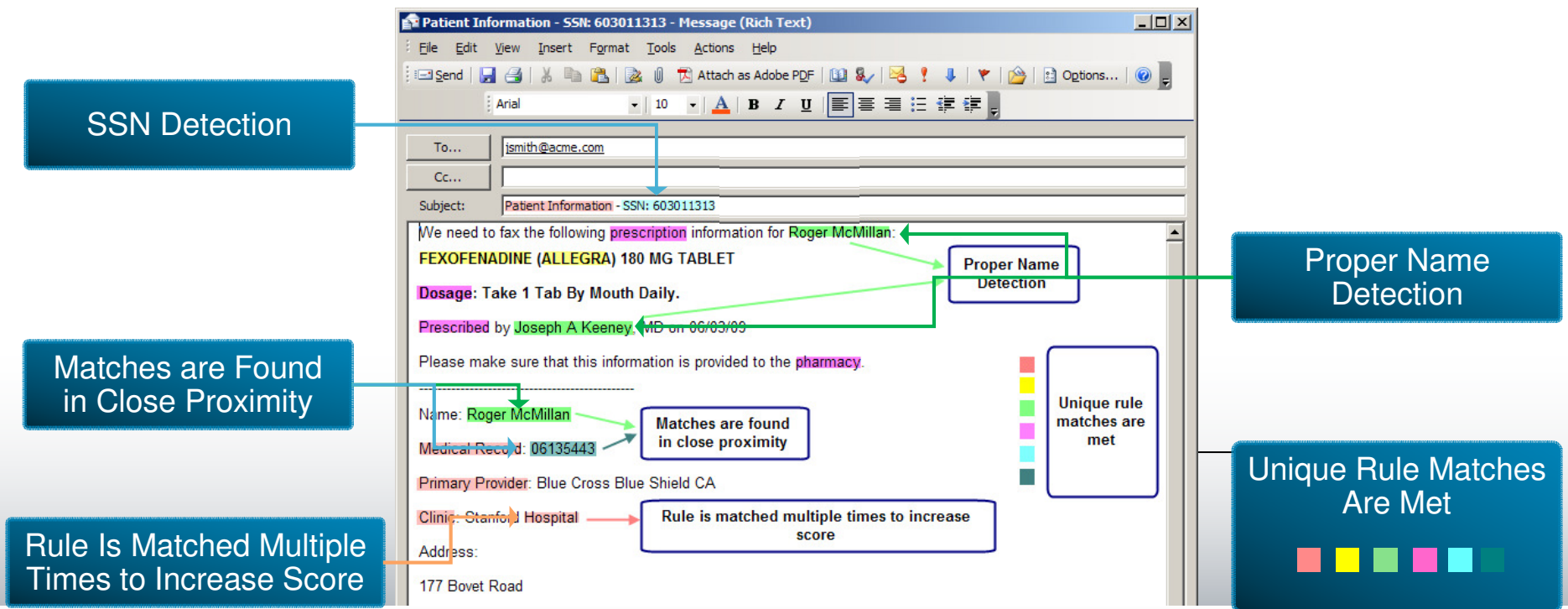
Protecting the Network: Email

100+ Predefined Policies for Comprehensive Coverage



Protecting the Network: Email

Accuracy through Proximity, Contextual Awareness, Proper Name Identification, Frequency and Other Methods



"RSA has strong described content capabilities enabled by a formal knowledge-engineering process"
- Gartner

Protecting the Network: Email

From: info@bankofchase.com
Subject: Customer Satisfaction Survey
Date: Fri, 23 Oct 2009 11:09:01 -0400

Customer Satisfaction Survey

At Chase Bank, we sincerely value your opinions. As part of our continuous improvement process, we're conducting a survey to benchmark the opinions of our customers. We will use the resulting information to better serve all of our customers.

We kindly ask you to take part in our quick and easy reward survey.

In return we will credit \$50.00 to your account.

[Click here to start the survey.](#)

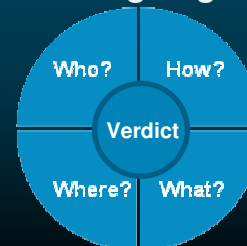
With the information collected we can decide changes to improve and expand our service.

Copyright © 1998-2009 JPMorgan Chase & Co. All Rights Reserved.

Fake survey to collect Name, Address, Social Security Number and Account Information

Cisco IronPort Anti-Phishing Solution

Context Adaptive Scanning Engine



SenderBase Reputation Filtering



Stop Phishing Attacks Before They Enter the Network

Cisco IronPort Anti-Malware Solution

Virus Outbreak Filters



"Western Union Malware"

**17 hr 16 min Lead Time
Over AV Vendor Signatures**

From: Western Union Support Team
Date: Tuesday, May 12, 2009 1:14 PM
To: [Redacted]
Subject: Western Union Transfer MTN: 4658925046
Attachment: Invoice_8773.zip (73.8 KB)

Dear Client!

The money transfer you have requested was not collected by the receiver. Due to the Western Union user credentials and allow are not collected in 30 business days. To collect cash you need to print the invoice attached to this email and visit the nearest Western Union agency.

**Western Union Malware:
Five variations of a trojan
in one week. Installed a
keylogger used to steal
user credentials and allow
remote system control
to sender.**

Detect and Stop Malware Before Any Other Technology

Protecting the Network: Email

Stop Attackers from Accessing Your Network

Quarantine ▼

☒ Enable Encryption

Encryption Profile: CRES Encryption ▼

Encrypted Message Subject: \$subject

☒ Apply TLS if message encryption fails.

Policy Quarantine: Policy ▼

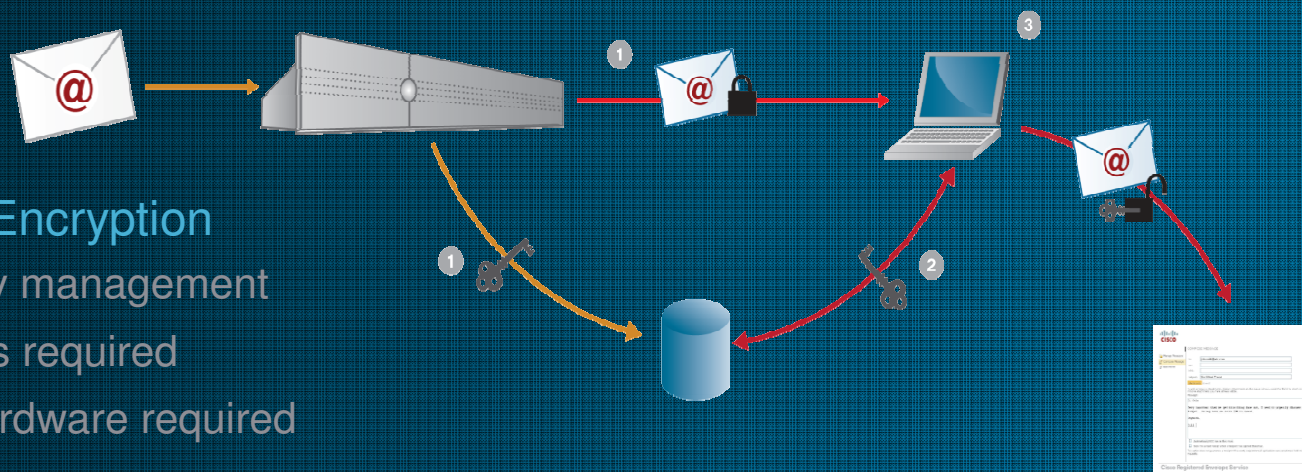
Message Modifications

Automated Remediation

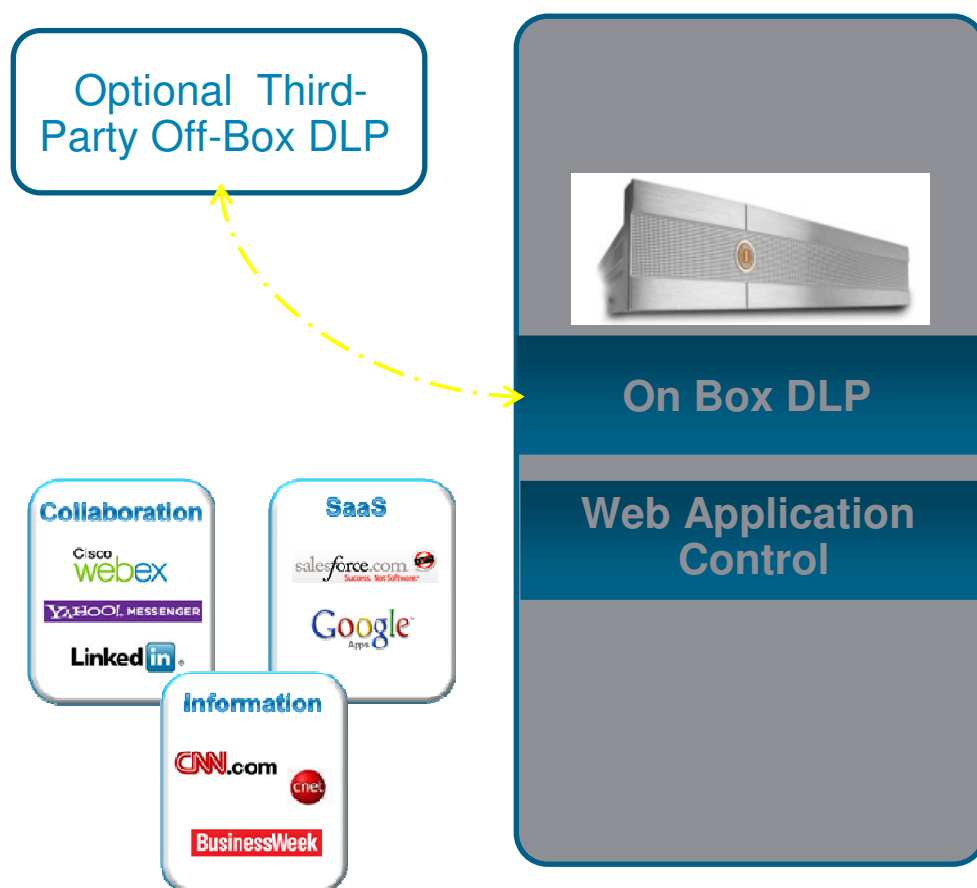
- Encrypt, quarantine, deliver, or drop
- Add disclaimer, modify subject
- Copy or notify
- Guaranteed secure delivery

Integrated Encryption

- Hosted key management
- No plug-ins required
- No new hardware required



Protecting the Network: Web



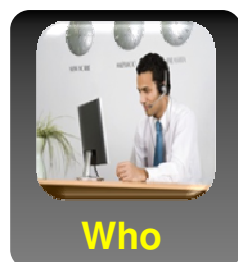
Deep Content Analysis

- Seamless off-box DLP with ICAP
- Best in class integrated RSA DLP
- Open DLP architecture
- Centralized Management

Complete Protocol Coverage

- Stops sensitive content from leaving via webmail, FTP, social networking sites and more
- Enforces policy while allowing security with Selective SSL Decryption

Protecting the Network: Web



Block Malware

- Three levels of malware protection provides ultimate defense-in-depth
- Preventive malware protection with web reputation filters
- Detailed reporting and forensics

Block Data Loss from Infected PCs

- Layer 4 Traffic Monitor stops infected PCs from sending sensitive content by preventing “phone home” activities
- Scans all 65,535 ports for malicious traffic

The Transformation New Borderless Enterprise

Right User
Anyone

Right Device
Anything



Customer Challenge in Building an Access Policy in a Borderless Network

Access Policy



Authorized Access

- Who is on my network?
- Can I manage the risk of using personal PCs?
- Common access rights when on-prem, at home, on the road?
- Endpoints are healthy?



Guest Access

- Can I allow guests Internet-only access?
- How do I manage guest access
- Can this work in wireless and wired?
- How do I monitor guest activities?



Non-User Devices

- How do I discover non-user devices?
- Can I determine what they are?
- Can I control their access
- Are they being spoofed?

ACS 5.0 Feature Highlights

Rule-based policy model

A rules-based, attribute-driven policy model, providing much greater flexibility in addressing policy needs

Light weight GUI

A completely redesigned web-based GUI that is lightweight, secure, intuitive and easy to use

Monitoring & Reports

Integrated monitoring, reporting and troubleshooting component in GUI that provides maximum level of control and visibility

Incremental Replication

Large-scale distributed deployment model with incremental configuration replication mechanism

Improved external integration

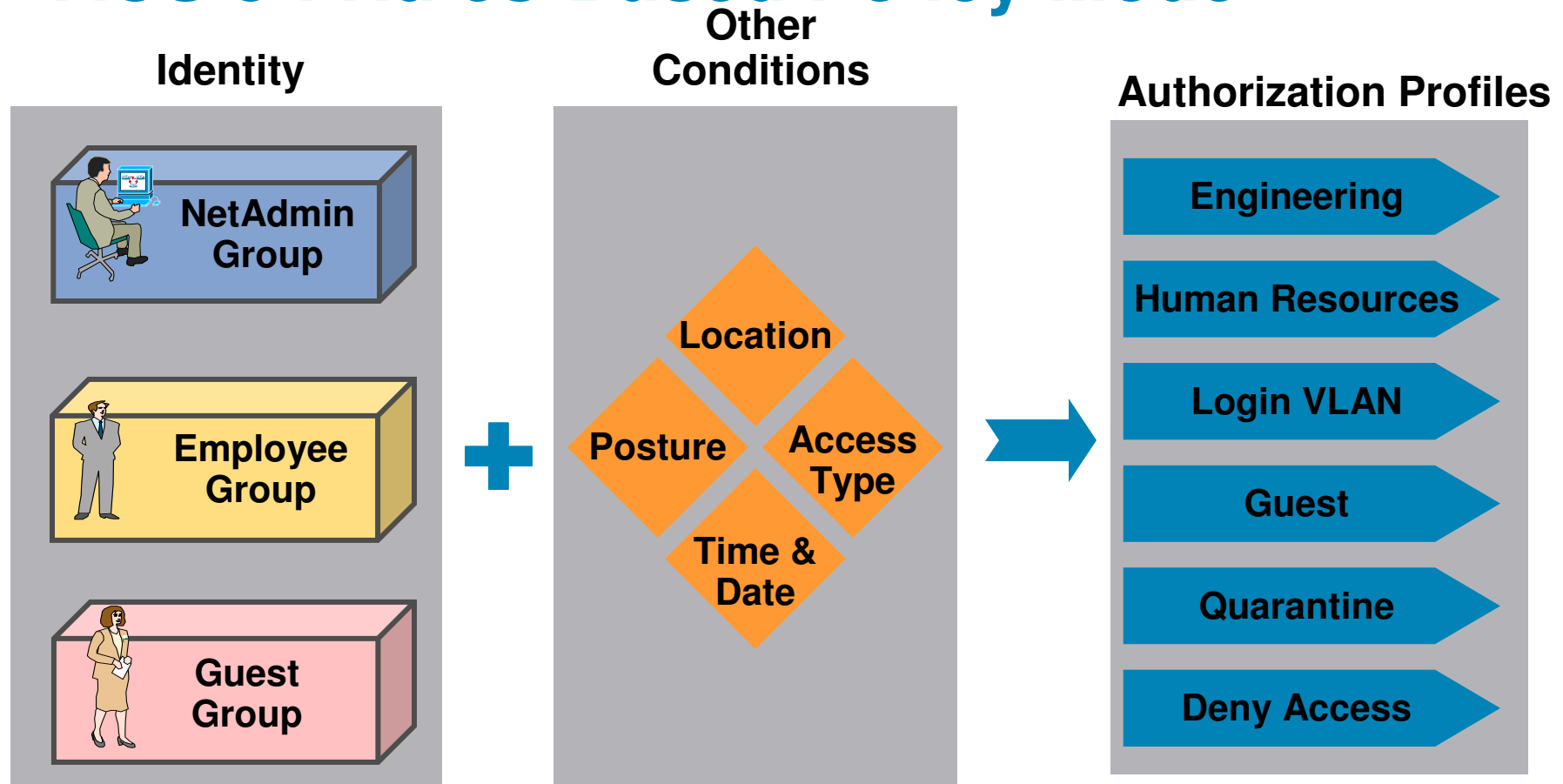
Improved integration with external identity and policy databases (AD, LDAP)

Platform

- 1 RU, security-hardened Linux appliance
- VMware virtual appliance

ACS 5.0 is the initial release of Cisco's next generation network identity and access solution

ACS 5 : Rules-Based Policy Model



Policy Rules *Policy Elements*

CONDITIONS		RESULT
ID GROUP	LOCATION	AZN PROFILE
ENG	SJ_CAMPUS	SJ_ENG
ENG	RTP_CAMPUS	RTP_ENG
ENG	EXTERNAL	EXT
IF NO MATCH		DENY ACCESS

Identity is decoupled from permissions
 Authorization based on identity and conditions specified as policy rules

- IF <condition(s)> THEN <permission>

ACS 5.1 Platform Options

1121 Hardware Appliance

One rack-unit (1RU)
security-hardened, Linux-
based appliance



VMware Appliance

Complete appliance image
for installation on VMware
ESX 3.5 or 4.0

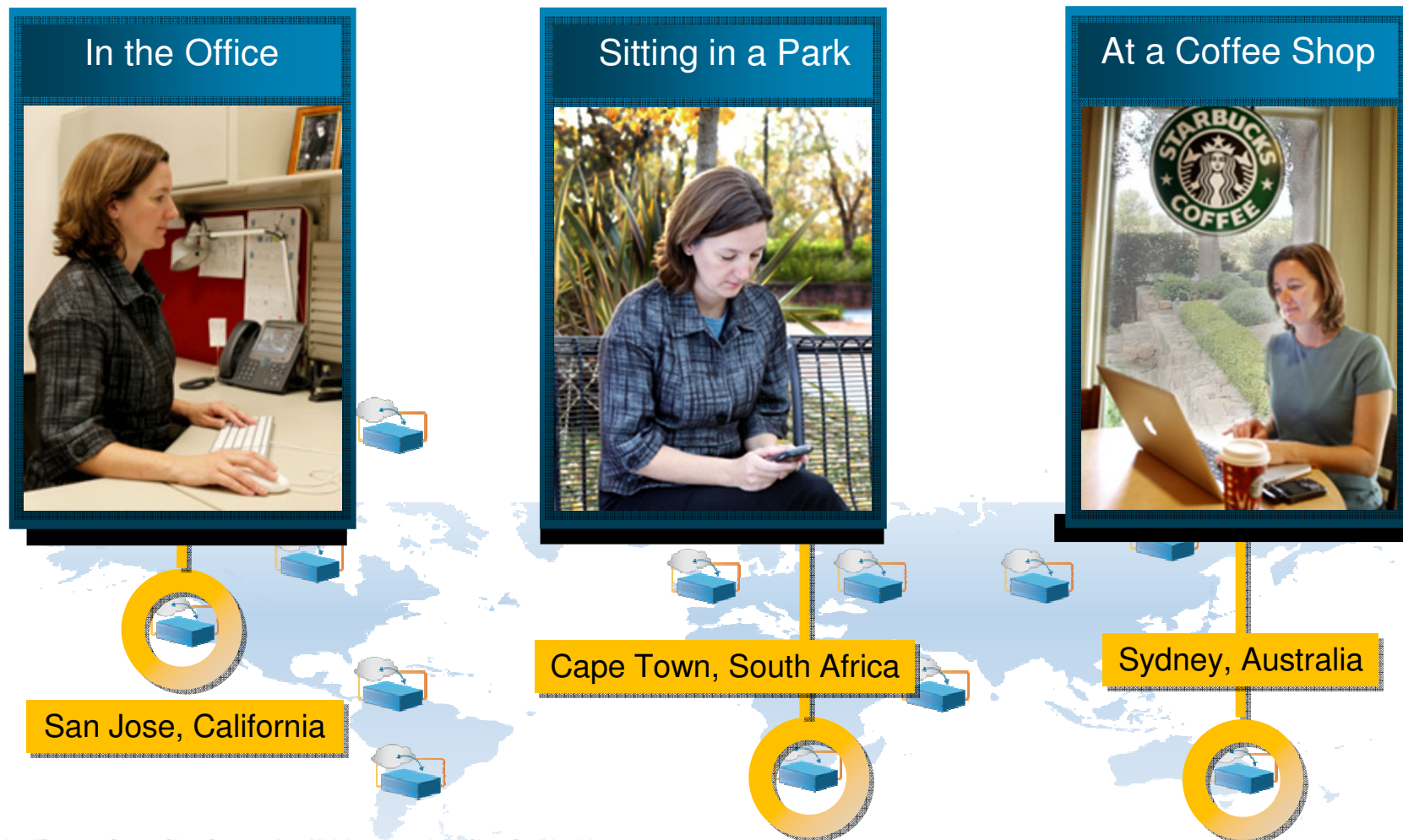
vmware

* Upgrade part numbers

Ordering Guide - http://cisco.com/en/US/prod/collateral/netmgtsw/ps5698/ps6767/ps9911/product_bulletin_c25-569135.html

Anytime, Anywhere, Any Device

Always On Security and Protection



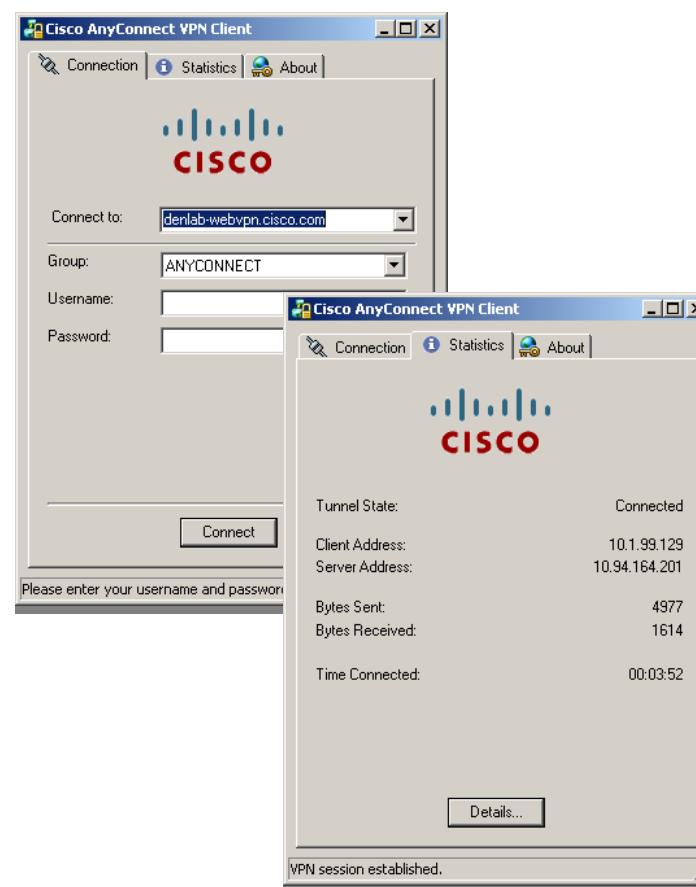
SSL VPN Introduction

Clientless	Thin-Client	Client-Based
<ul style="list-style-type: none">▪ Basic web access▪ E-mail access▪ CIFS (Common Internet File System) access▪ Customized user screen	<ul style="list-style-type: none">▪ Port redirection for only TCP applications▪ Smart tunnel	<ul style="list-style-type: none">▪ Full-SSL tunnel:<ul style="list-style-type: none">▪ AnyConnect▪ SVC (SSL VPN Client)

SSL VPN Tunneling: AnyConnect Client

Persistent “Thick”, “Full Tunneling”, or “Tunnel” Client

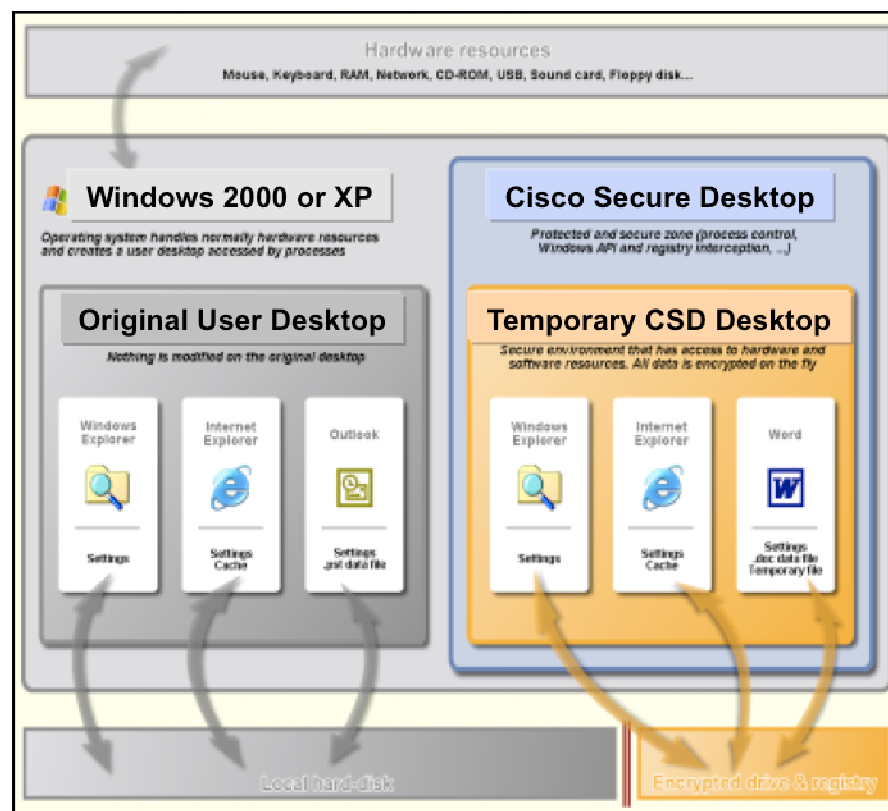
- Traditional-style client delivered via automatic download
- Requires administrative privileges for initial install only
- Stub installer has been replaced with an MSI out-of-band/pre-installation package
- Can use TLS or DTLS as transport
- Can be upgraded from a previous version upon connection



Cisco Secure Desktop

Works for Clientless and AnyConnect Sessions

- **Pre-connect assessment:**
 - Location assessment—managed or unmanaged desktop?
 - Gathers data about the end machine
- **Session protection:**
 - Data sandbox and encryption protects every aspect of session
- **Post-session clean-up:**
 - Encrypted partition overwrite (not just deletion)
 - Cache, history and cookie overwrite
 - File download and email attachment overwrite
 - Auto-complete password overwrite



Advanced Endpoint Assessment

Built-in Enforcement Capability

- Supported endpoint components
 - Anti-Virus
 - Personal Firewall
 - Anti-Spyware
- Licensed feature
- Regular updates provided
- No Dynamic Access Policies required

