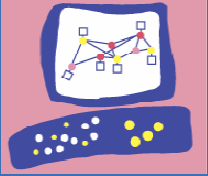


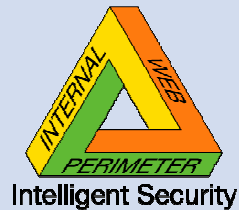
Check Point
SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

End-point security with Check Point Integrity

Patrick Hanel



1 June 2006



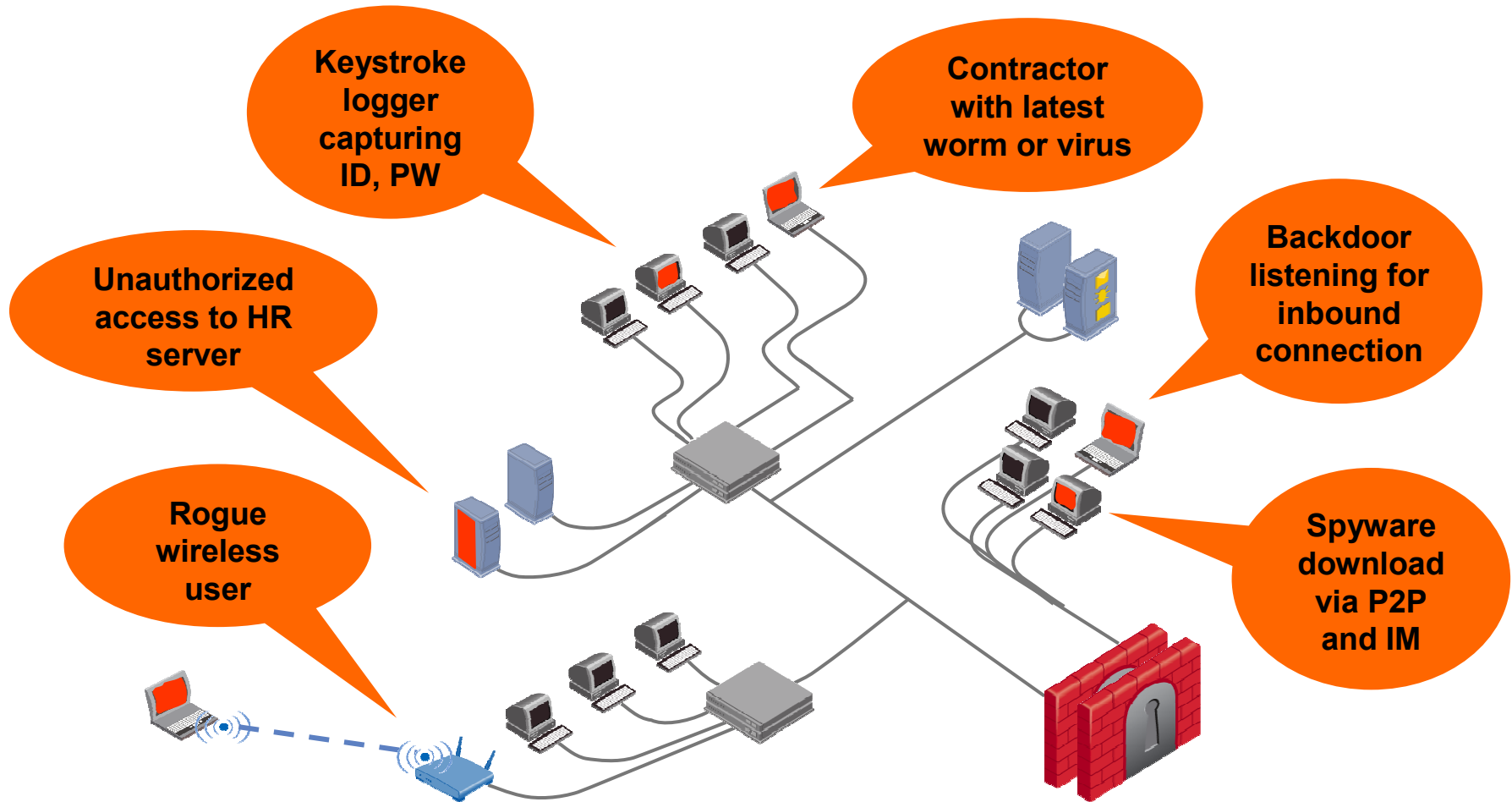
Agenda



- Risks to Endpoints
- Business Requirements to Secure Endpoints
 - Policy management
 - Access rights
 - Network protection
- Integrity Endpoint Security Solution
 - IPS
 - Program Controls
 - Anti-X
 - Compliance Enforcement
- Deployment Options
 - Scalability
 - Manageability



Many Endpoint Threats





Endpoint Security Value

Keep the network up and running

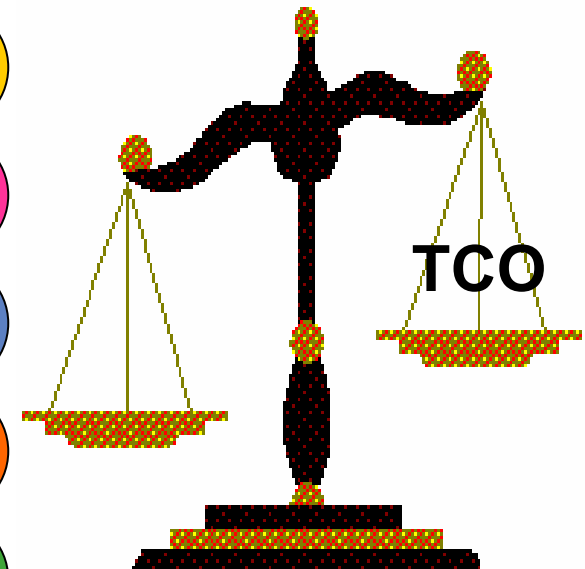
Avoid disruption of operations

Block exposure of sensitive data

Stop theft of proprietary information

Protect valuable reputation, brand

Maintain executive confidence





Business Requirements to Secure Endpoints



- Policy management
 - Reusable Policy Elements
 - Monitoring & Reporting
- Access rights
 - End User rights to networks and applications
 - Endpoint Compliance Validation
- Network Protection
 - Protect key elements of Infrastructure
 - Ensure Uptime and availability
 - Integrity with current networking components



Solution: Check Point Integrity™



- ➔ Blocks Worms, Spyware, and Other Hacker Attacks Preemptively
- ➔ Stops Day Zero Exploits That Evade Reactive Security Products
- ➔ Prevents Data Theft or Exposure
- ➔ Maintains Business Continuity
- ➔ Provide Mechanism for Endpoint Compliance

CHECK POINT
integrity™



Integrity Client Side Security



- Multi-Layered Approach
 - Classic Firewall Rules
 - Zone Rules
 - Program Controls
 - SmartDefense Program Advisor
 - Messaging Rules
 - IM Security
 - Email Controls
 - Anti-Spyware
 - Intrusion prevention capabilities:
 - Malicious Code Protection
 - Malware process termination
 - Cooperative Enforcement



Active	Programs ▲	Access		Server		Send Mail
		Trusted	Internet	Trusted	Internet	
	Adobe Reader 7.0	✓	✓	?	?	?
	AtMgr Module	✓	✓	?	?	?
	Check Point Eventi...	✓	✓	✓	✓	?
	Check Point Eventi...	✓	?	?	?	?
	Check Point SmartV...	✓	?	?	?	?
	Check Point SmartV...	✓	✓	✓	✓	?
	Citrix ICA Client Engi...	?	?	?	?	?
	Exodus Jabber Client	?	?	?	?	?
	File Transfer Program	✓	✓	?	?	?
	FwPolicy.exe	✓	✓	?	?	?
	Generic Host Proce...	✓	✓	✓	✓	?
	GoogleDesktopCra...	?	?	?	?	?
	GoogleDesktopInde...	✓	✓	?	?	?



Integrity Communication Rules



- **Classic Firewall Rules**
 - Allow/Block traffic based on protocol, source & destination
- **Zone Rules** (for Internet and Trusted Zones)
 - Allow/Block requests based on zone, direction, & protocol
- **Messaging Rules** (for pop3/imap4 and/or IM peer-to-peer)
 - Quarantine E-mail attachments based on file extension
 - Allow/Block traffic based on Instant Messaging protocol
- **Program Rules (for Application Control)**
 - Allow/Block traffic
 - Based on program, behavior, and zone



How to Manage Program Controls?



- Manage Troublesome Programs
 - Import checksums or observe programs in use, then
 - Block globally or restrict usage through enterprise policy
- Manage Reference Sources
 - Fingerprint “known good” programs then import checksums
 - Set policy “**Program Rules**” for “*Referenced Programs*”
- Manage Discovered Programs
 - Identify new programs, then
 - Fingerprint, block, or restrict.
- Manage Production Rollout
 - Create policy to block “*All Other Programs*” & “*Ask Server*”
 - Assign and test policy one department or group at a time



SmartDefense Program Advisor



- **Goals:**
 - Make security easier
 - Remove administrative time burden
 - Provide higher security at a lower cost
- **Advisory Services**
 - Known good - Application Authenticity Service
 - Known Bad - Malware Identification Service
 - Best Practices Policy
 - Based on expert analysis of millions of installations of Zone Alarm



Automated Defense Updates



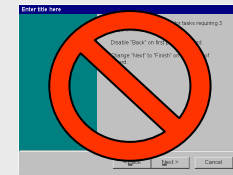
Unknown program
attempts network
access



Integrity connects
to Program
Advisor database



PA replies with
application
control rule



Integrity immediately
applies allow, block,
or terminate rule to
application

SmartDefense Program Advisor Service

- Rules for Over 100,000 Applications/Malware
- Handles Over 130 Million Queries per Week
- Allows Administrator Overrides
- ***Faster Malware Defense at Far Lower Cost***



Advisory Services Benefits



- **Facilitated Management**
 - Vastly reduce program management overhead
 - Focus on the unidentified programs
 - Make global permission changes
- **Proactive Security**
 - Proactive protection from threats never seen on your network
 - Process termination
- **Simplify End User Experience**
 - Reduce the number of alerts
 - Remove guess work
 - Reduce help desk calls



Integrity 6.5 – Anti-Spyware

- Anti-Spyware Tool
 - Central Management
 - Scheduled scans
 - Easy-to-manage categories
 - Exception lists
 - Comprehensive Reporting
 - Integrity Client module with:
 - Spyware detection
 - Disablement
 - Quarantining
 - Removal



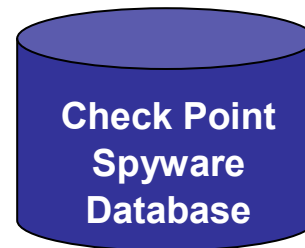


Integrated Anti-Spyware

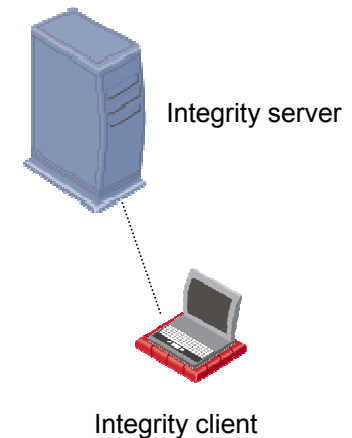
Millions of ZoneAlarm
Users Automatically
Report Details of Newly
Detected Spyware



Check Point Security
Services Develops
Timely Detection &
Removal Techniques



Updates
Automatically Sent
to Integrity Users



No Additional Management or Client Software Required



Host IPS Functionality

Check Point
SOFTWARE TECHNOLOGIES LTD.

integrity

Home
System Configuration
Client Configuration
Entities
Global Policy Settings
Policies
Policy Objects
Reports

Administrator
masteradmin
Role
Master Administrator
© Check Point Technologies Ltd

About | Help | Change Password | Log Out

Edit Policy Cancel Save

Name & Notes | Firewall Settings | Zone Rules | Access Zones | Program Rules | Anti-Spyware | **SmartDefense** | Messaging Settings | Enforcement Settings | Client Settings

Malicious Code Protection for "Default Policy"

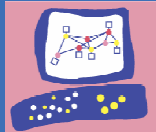
Turn malicious code protection ON for this policy

Observe malicious code activity
 Act on malicious code activity

Setting applies to:

Protocol	Inbound	Outbound
FTP	<input type="checkbox"/>	<input type="checkbox"/>
HTTP	<input checked="" type="checkbox"/>	<input type="checkbox"/>
IMAP4	<input checked="" type="checkbox"/>	<input type="checkbox"/>
NNTP	<input type="checkbox"/>	<input type="checkbox"/>
POP3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
SMTP	<input type="checkbox"/>	<input checked="" type="checkbox"/>

- Zero day detection and prevention of malicious code
- Early detection on the network
- Supports a variety of protocols
 - Scans potentially compromised parts of the protocol
 - Works on HTTP, FTP, IMAP4, SMTP, POP3, NNTP



Integrity 6.5 – Auto-Remediation

- Auto-Remediation
 - Specify enforcement rules in policy
 - When end users are out of compliance:
 - Securely pull the package from sandbox
 - Run installation on end point automatically
 - Process can be completely silent
 - No end user confusion
 - No uncertainty about updates
 - Reporting enhancements



KS6879
"www.web.concepts" Disc
© Comstock IMAGES

Royalty-Free Division
www.comstock.com



Client Enforcement Rules



Enforcement Rule Options

- ▶ Fail-open or restrict session when out-of-compliance.
- ▶ Specify client heartbeats until restriction & disconnection.
- ▶ Enter dialog text to display to out-of-compliance user.

Anti-Virus Rules

- ▶ Specify one or more Anti-Virus Packages (“OR” logic).
- ▶ Check for running process, DAT and software versions.

Manual Rules (Extensible Custom Rules with “AND” logic).

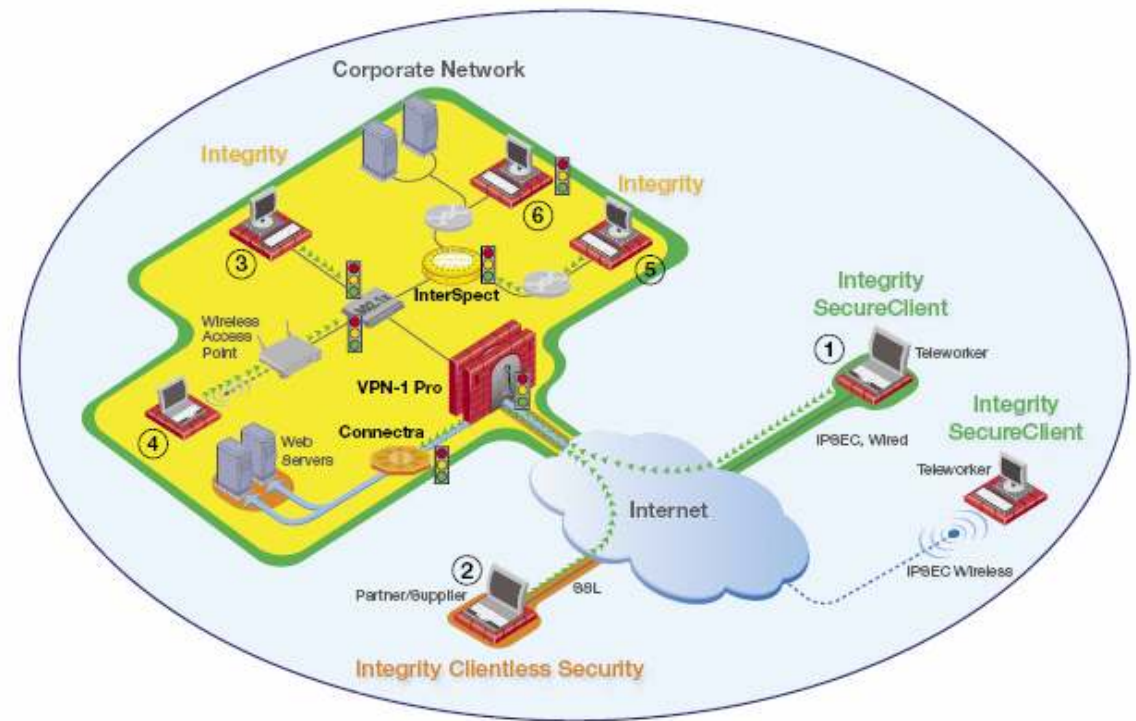
- ▶ Require or prohibit file existence (exact path, not disc scan).
- ▶ Require a file with particular version or date “no older than.”
- ▶ Require or prohibit specific registry key with particular value.



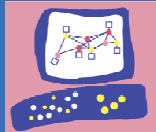
Integrity Policy Enforcement



1. IPSec VPN
2. SSL VPN
3. 802.1x Switches
4. 802.1x Access Points
5. InterSpect
6. LAN Quarantine

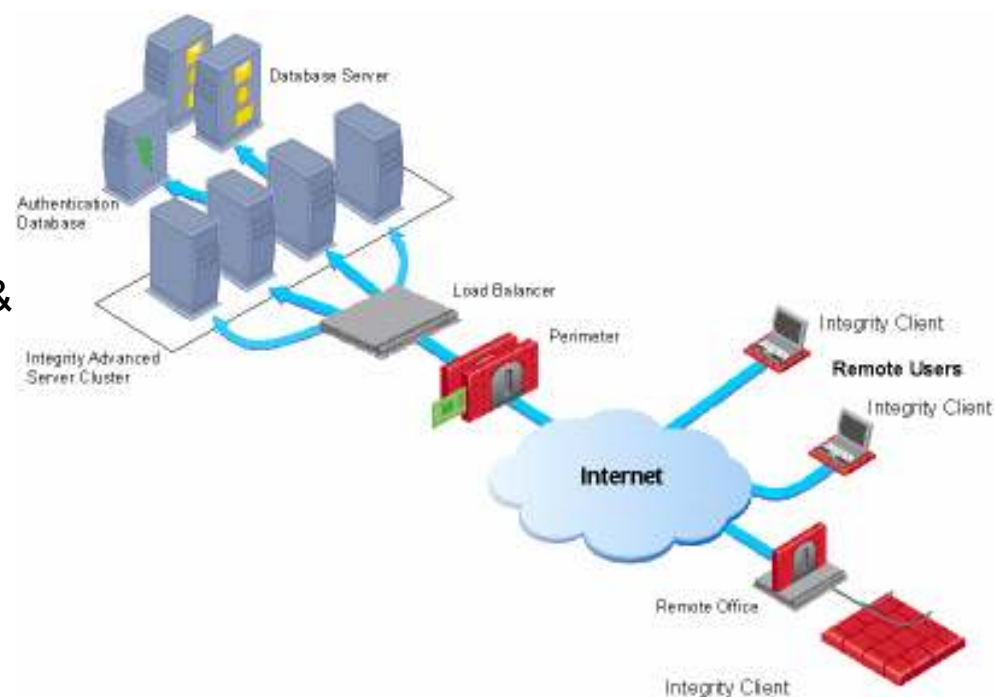


Mature, proven access control inside and outside the perimeter



Integrity Server Architecture

- Distributed architecture for extreme scalability with clustered, load-balanceable server
- Tiered administration and role-based security
- Server platform certification
 - Red Hat Linux ES 3.0 , Windows & SecurePlatform
 - External Database: Oracle, Microsoft SQL and IBM DB2
- Single and multi-domain support.
- MSI improvements to allow SMS and GPO silent deployment with heightened privileges.





Integrity Management



- Disconnected policy management
- Enforcement rule enhancements
- Support for automatic client upgrades
- Policy templates, versioning, rollback and auditing
- Notifications in SNMP, Syslog, SMTP, JDBC and text formats.
- Reporting Overhaul
- Sandbox & support enhancements



Integrity NGX



- Check Point SMART integration
 - Data Management
 - Send all relevant client logs to SmartCenter
 - Special log views in SmartView Tracker
 - Integrity Monitoring using SmartView Monitor
 - Integrity Reporting with Eventia Reporter
 - Shared Objects
 - Integrity objects in SmartDashboard
 - Shared administrators across all Check Point products
 - Allow Integrity to be launched from other SmartCenter applications



Integrity NGX



- **Check Point SMART integration**
 - Server-side License Management
 - All Integrity licenses will be server-side
 - All license management via User Center
 - No more inconvenient client-side licenses
 - Provider-1 integration
 - SecurePlatform support
 - Co-installation with Check Point products
 - Integrity added to VPN1/SmartCenter installer
 - Allow local and remote installation of Integrity
 - Start/stop of Integrity with other Check Point apps



Integrity integration

- Integrity server software is part of Check Point's installation CD and can be installed via the wrapper.
 - On SmartCenter's machine
 - Or on a separate machine establishing SIC communication

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

NGX

More Security Solutions
Contact Information

Gateway

- VPN-1 Pro

Management

- SmartCenter
- Eventia Reporter
- SmartConsole
- Integrity

NGX: The Only Unified Security Platform

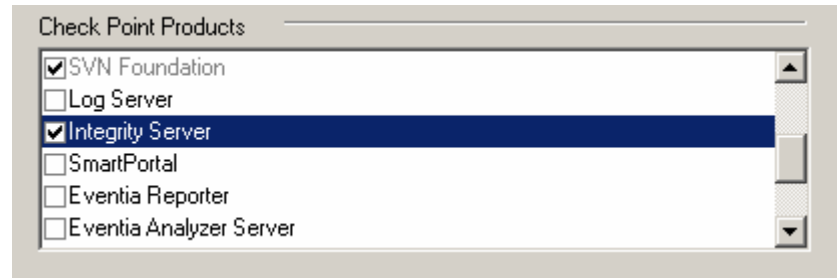
NGX is the latest Check Point security software platform that delivers a unified security architecture for internal, perimeter and Web security. This unified security architecture enables enterprises of all sizes to reduce the cost and complexity of security management and ensure that their security systems can be easily extended to adapt to new and evolving threats.



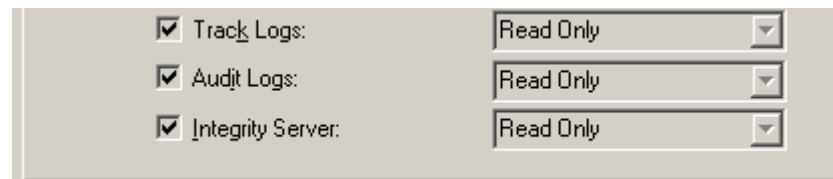
Integrity integration (cont)



- Integrity server object is defined in SmartDashboard by checking the Integrity server product.



- An administrator defined via SmartDashboard can be assigned with permission to access integrity server.

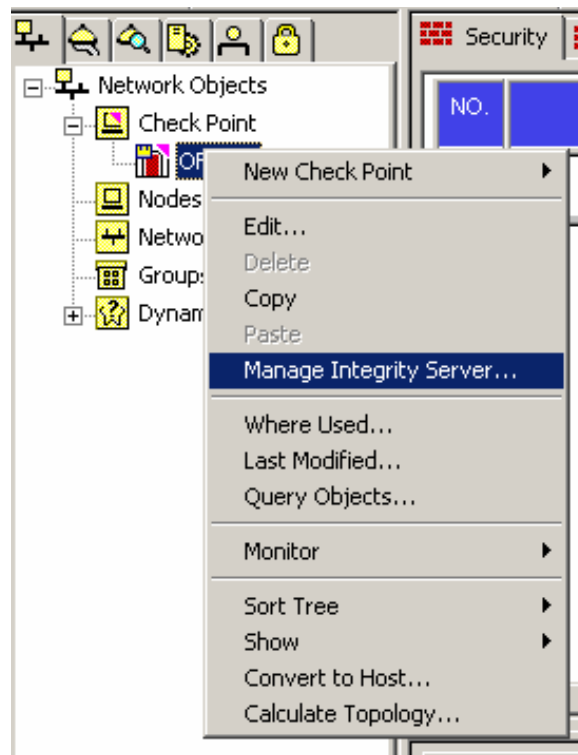




Integrity integration (cont)



- Such administrator can login directly to Integrity server, or launch it by a right click on Integrity object

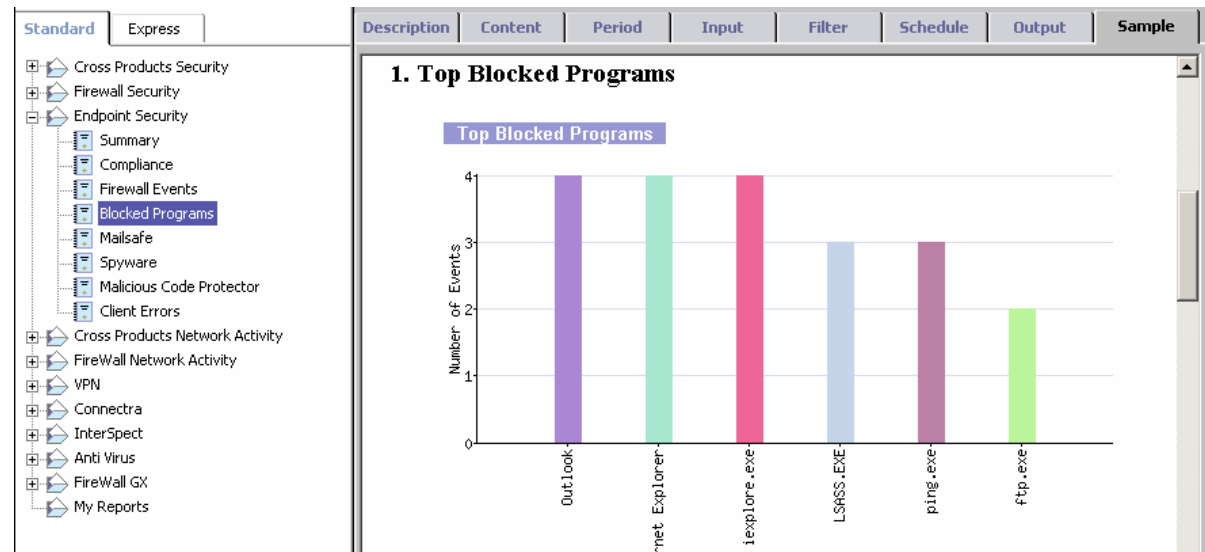




New Reporting Capabilities

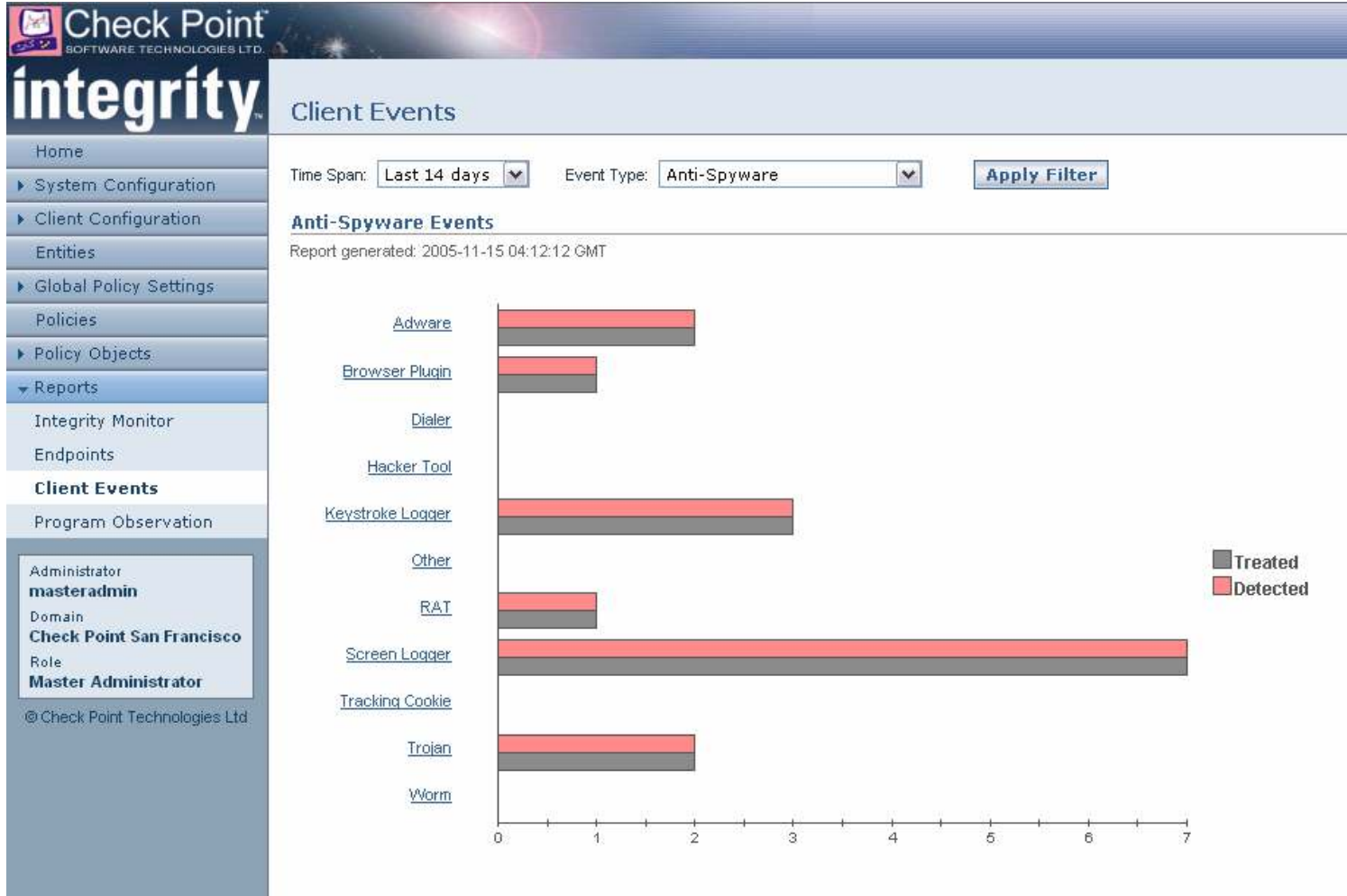


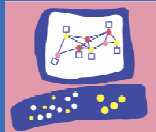
- Reporting now includes:
 - Eventia Suite Integration
 - Integrity Monitor
 - Improved logging
 - More filtering & drill-down options
 - More charting
 - More information





Spyware Reporting





Spyware Details Report



Event Details Report

Print

- Home
 - ▶ System Configuration
 - ▶ Client Configuration
 - Entities
 - ▶ Global Policy Settings
 - Policies
 - ▶ Policy Objects
 - ▼ Reports
 - Integrity Monitor
 - Endpoints
 - Client Events**
 - Program Observation
- Administrator
masteradmin
Domain
Check Point San Francisco
Role
Master Administrator

© Check Point Technologies Ltd

Time Span: **Last 14 days** Event Type: **Anti-Spyware** Keystroke Logger

Results

Report generated: 2005-11-15 04:14:12 GMT

User	Group	Catalog	Event Description	Timestamp
172.18.22.71	n/a	UniversallP	Keystroke Logger type spyware AB System Spy detected. Treatment Delete was successful.	2005-11-15 00:36:28 GMT
172.18.22.71	n/a	UniversallP	Keystroke Logger type spyware AceSpy 2.1 detected. Treatment Delete was successful.	2005-11-15 00:36:28 GMT
172.18.22.71	n/a	UniversallP	Keystroke Logger type spyware 007 Spy detected. Treatment Delete was successful.	2005-11-15 00:36:26 GMT

◀ Rows 1-3 ▶ 100 Rows ▼



User Report

Check Point
SOFTWARE TECHNOLOGIES LTD.
2006 | Back | Refresh | Logout

integrity

- Home
- System Configuration
- Client Configuration
- Entities
- Global Policy Settings
- Policies
- Policy Objects
- Reports
- Integrity Monitor
- Endpoints**
- Client Events
- Program Observations
- Administrators
- Master Admins
- Role
- Monitor Administrator

© Check Point Technologies Ltd.

Endpoint Details

Back Print

General Information

Report generated: 2006-11-16 09:27:49 GMT

General Information					
User	172.18.22.138	Group	n/a	Catalog	Intune:IP138
Computer Name	lap-xp138	IP Address	172.18.22.138	MAC Address	8011P45804F4L
Client	Integrity Files	Client Version	6.5.655.999	Operating System	WinXP 5.L2666-Service Pack 3-SP
Current Policy	IntunePol	Last Contact	2006-11-16 09:27:33 GMT	Compliance State	■ Compliant

Enforcement Rule Compliance

The user is compliant but the Cooperative Enforcement Rules listed below have been dispersed or have caused warning alerts.

Item	Action	Provider	Reason
No Data in List			

Provider Details

The user has the following security providers installed:

Provider	Last Scan	Last Update	Engine	Plugin	DAT	DAT Date
Symantec Norton AntiVirus	169	n/a	4.20.7	n/a	71110	2006-11-09 16:00:00 GMT

Event Statistics by Type

Client Event Type	Last 24 Hours	24 Hours to 7 Days	More than 7 Days	Event Total
Firewall (Inbound)	30	0	0	30
Firewall (Outbound)	20	0	0	20
MalWare (Inbound)	0	0	0	0
MalWare (Outbound)	0	0	0	0
Application	0	0	0	0
Client Errors	0	0	0	0
Malicious Code (Inbound)	0	0	0	0
Malicious Code (Outbound)	0	0	0	0
IP Security (By Event Type)	0	0	0	0
Anti-Spyware	0	0	0	0
Totals	50	0	0	50



Integrity Monitor



integrity

Integrity Monitor

Print

- Home
- System Configuration
- Client Configuration
- Entities
- Global Policy Settings
- Policies
- Policy Objects
- Reports

Integrity Monitor

- Endpoints
- Client Events
- Program Observation

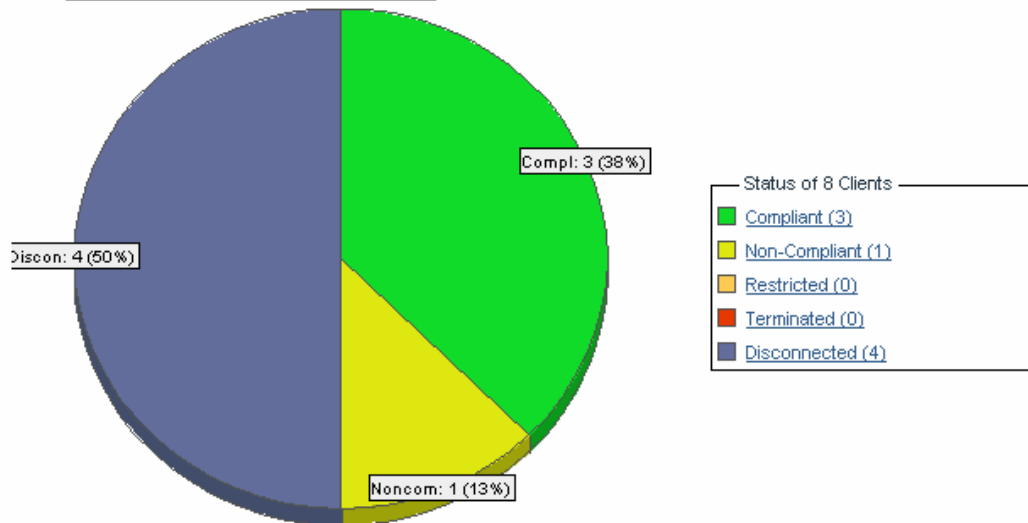
Administrator
masteradmin
Role
Master Administrator

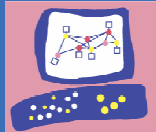
© Check Point Technologies Ltd

Chart:

Chart
Report

- Current Client Compliance Status
- Client Connectivity
- Client Version
- Policy Assignment
- Client Compliance by Rule
- Client Compliance by Policy
- Spyware Scanned Date





Summary Report



integrity™

Client Events

Print

Home

System Configuration

Client Configuration

Entities

Global Policy Settings

Policies

Policy Objects

Reports

Integrity Monitor

Endpoints

Client Events

Program Observation

Administrator

masteradmin

Role

Master Administrator

© Check Point Technologies Ltd

Time Span:

Event Type:

Apply Filter

Events Summary

Report generated: 2005-11-15 02:53:33 GMT

Event Type	Total Events	Total Users	Description
Firewall (Inbound)	360	5	Inbound firewall events totaled by user and event counts.
Firewall (Outbound)	370712	6	Outbound firewall events totaled by user and event counts.
Compliance Status	0	3	Summary of users that have been terminated, restricted or out of compliance.
Client Errors	0	0	Client errors totaled by user and event counts.
Anti-Spyware	7	3	Spyware events summary.
Mailsafe (Inbound)	40	1	Inbound mailsafe events totaled by user and event counts.
Mailsafe (Outbound)	0	0	Outbound mailsafe events totaled by user and event counts.
Malicious Code (Inbound)	23	1	Inbound malicious code events totaled by user and event counts.
Malicious Code (Outbound)	60	1	Outbound malicious code events totaled by user and event counts.
IM Security (by IM Protocol)	0	0	IM Security events by protocol totaled by user and event counts.
IM Security (by Event Type)	0	0	IM Security events by type totaled by user and event counts.
Application	113	4	Application block events totaled by user and event counts.



Summary

Broader protection for:

- Communication
- Data on the wire
- Applications
- System Core

**Total
End Point
Lockdown**