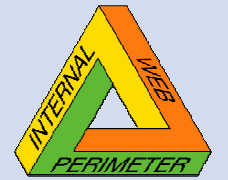
Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

End-point security with Check Point Integrity

Patrick Hanel



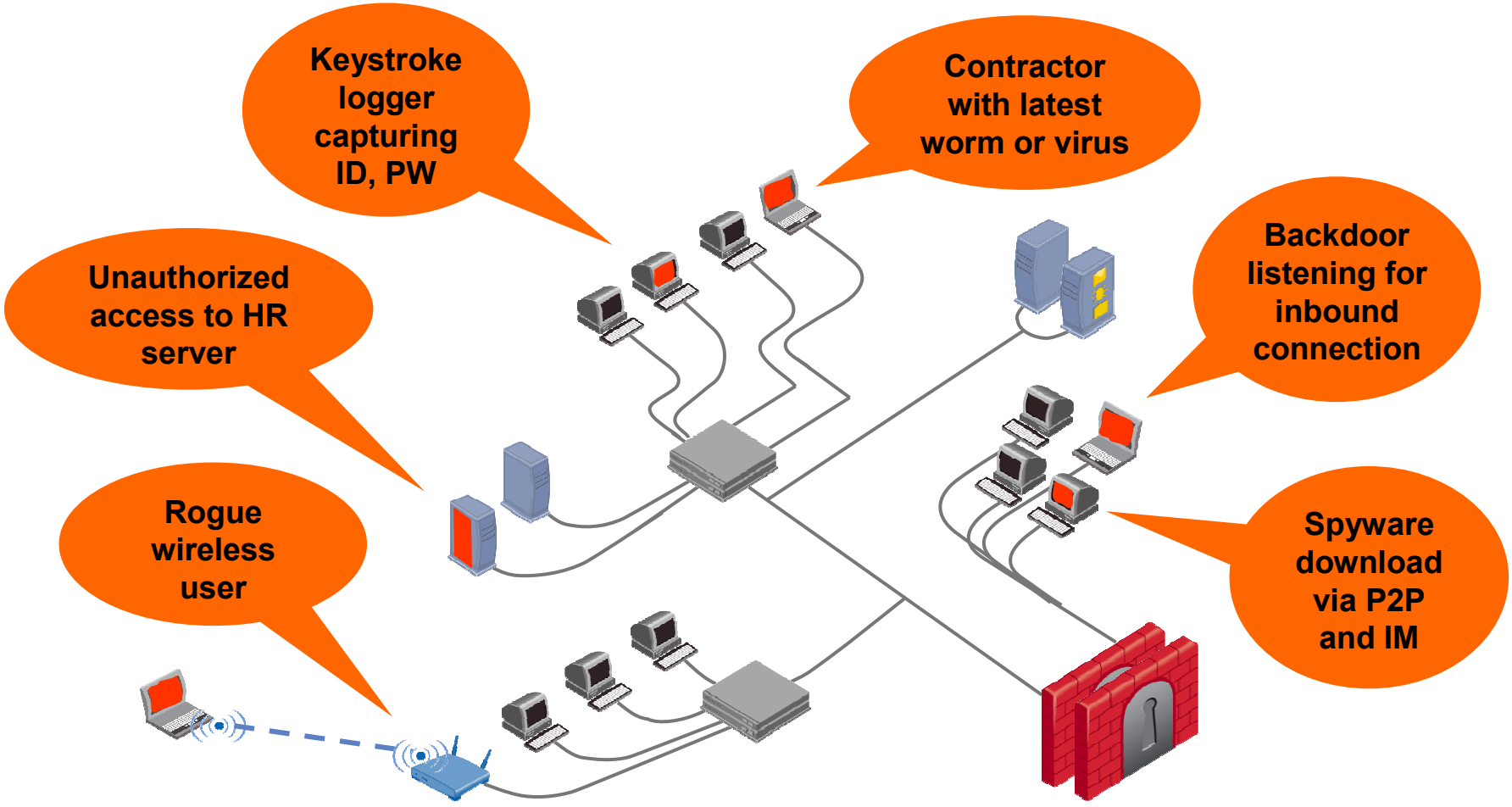
Intelligent Security

1 June 2006

Agenda

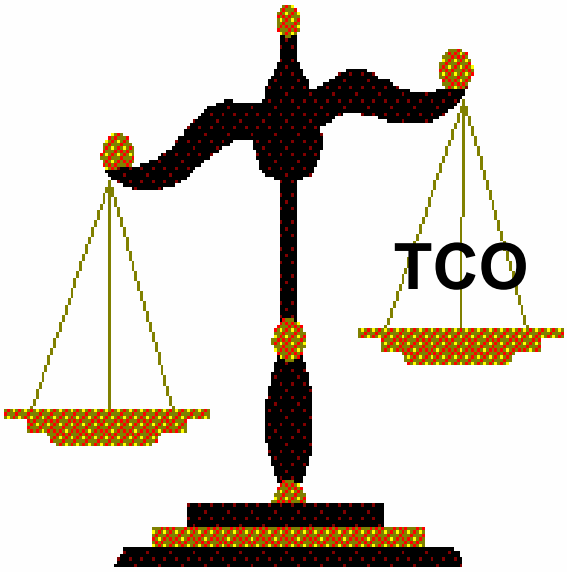
- Risks to Endpoints
- Business Requirements to Secure Endpoints
  - Policy management
  - Access rights
  - Network protection
- Integrity Endpoint Security Solution
  - IPS
  - Program Controls
  - Anti-X
  - Compliance Enforcement
- Deployment Options
  - Scalability
  - Manageability

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

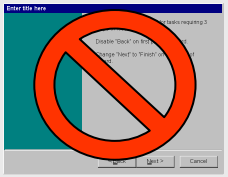
- **Goals:**
  - Make security easier
  - Remove administrative time burden
  - Provide higher security at a lower cost
- **Advisory Services**
  - Known good - Application Authenticity Service
  - Known Bad - Malware Identification Service
  - Best Practices Policy
    - Based on expert analysis of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

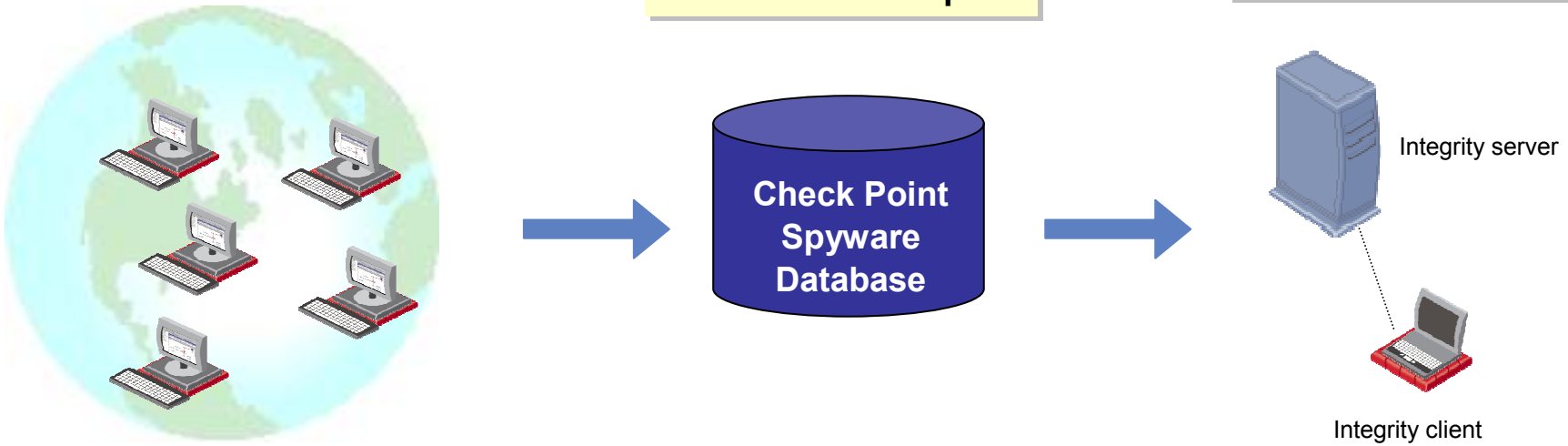
- Anti-Spyware Tool
  - Central Management
    - Scheduled scans
    - Easy-to-manage categories
    - Exception lists
    - Comprehensive Reporting
  - Integrity Client module with:
    - Spyware detection
    - Disablement
    - Quarantining
    - Removal

Integrated Anti-Spyware

Millions of ZoneAlarm Users Automatically Report Details of Newly Detected Spyware

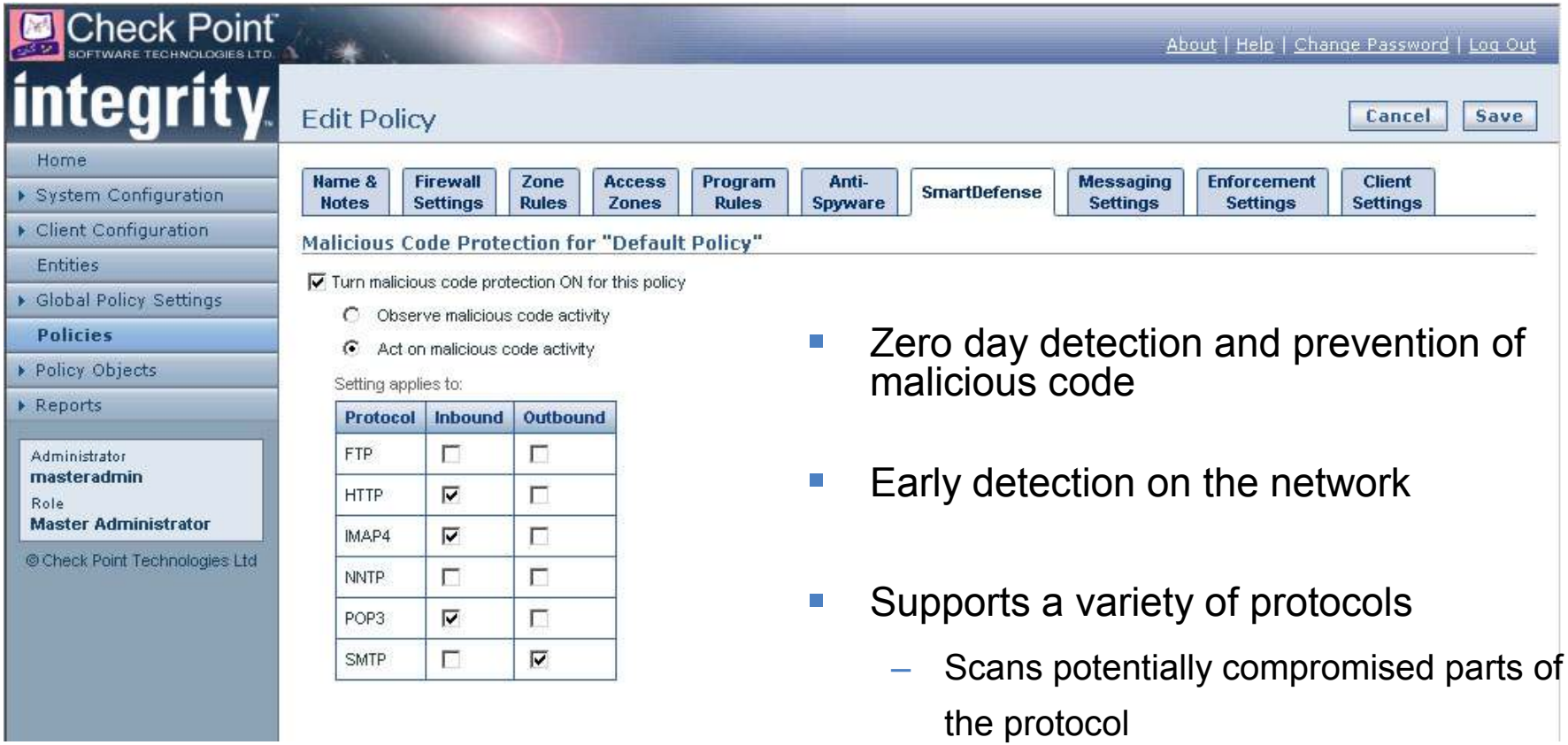
Check Point Security Services Develops Timely Detection & Removal Techniques

Updates Automatically Sent to Integrity Users



No Additional Management or Client Software Required

Host IPS Functionality



- 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

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

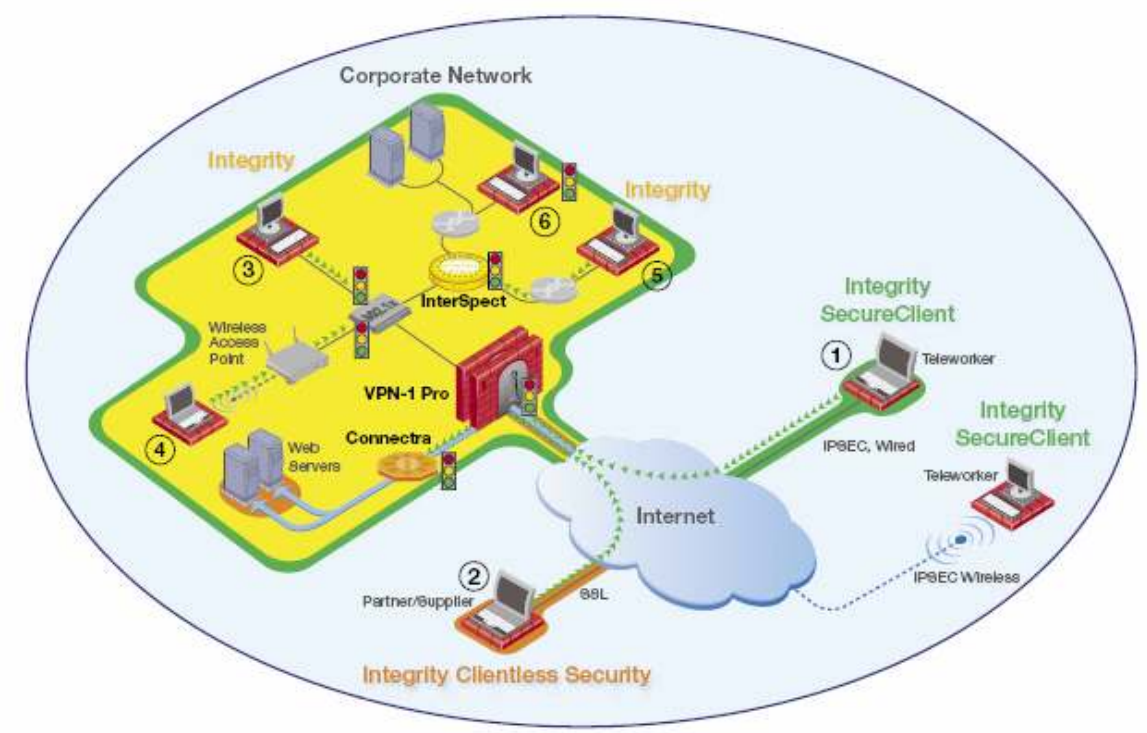
- Specify one or more Anti-Virus Packages (“OR” logic).
- Check for running process, DAT and software versions.

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

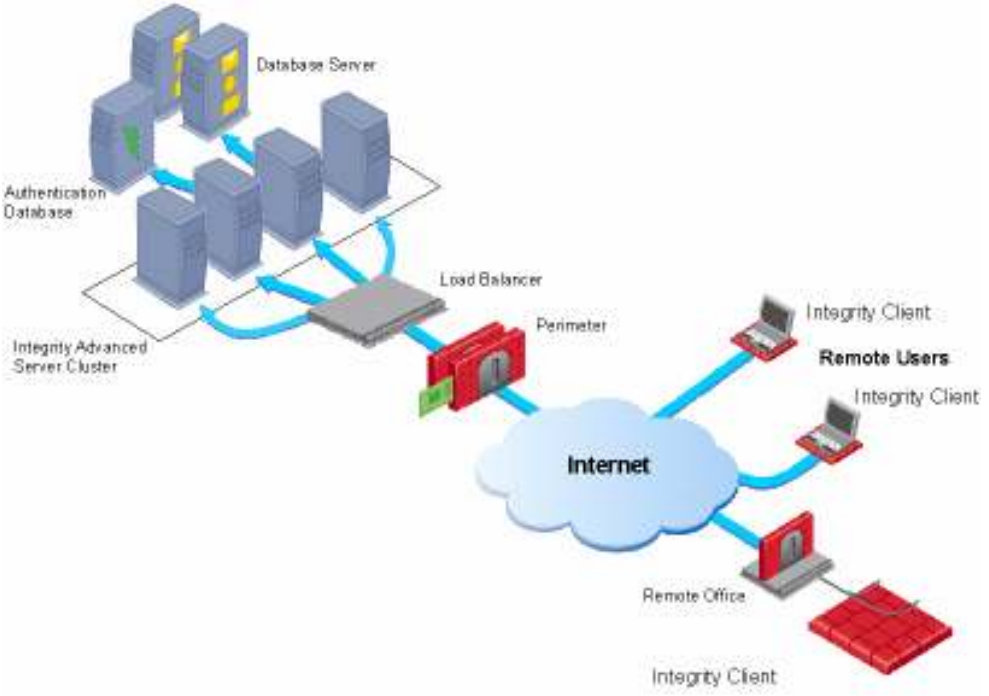
1. IPSec VPN
2. SSL VPN
3. 802.1x Switches
4. 802.1x Access Points
5. InterSpect
6. LAN Quarantine



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

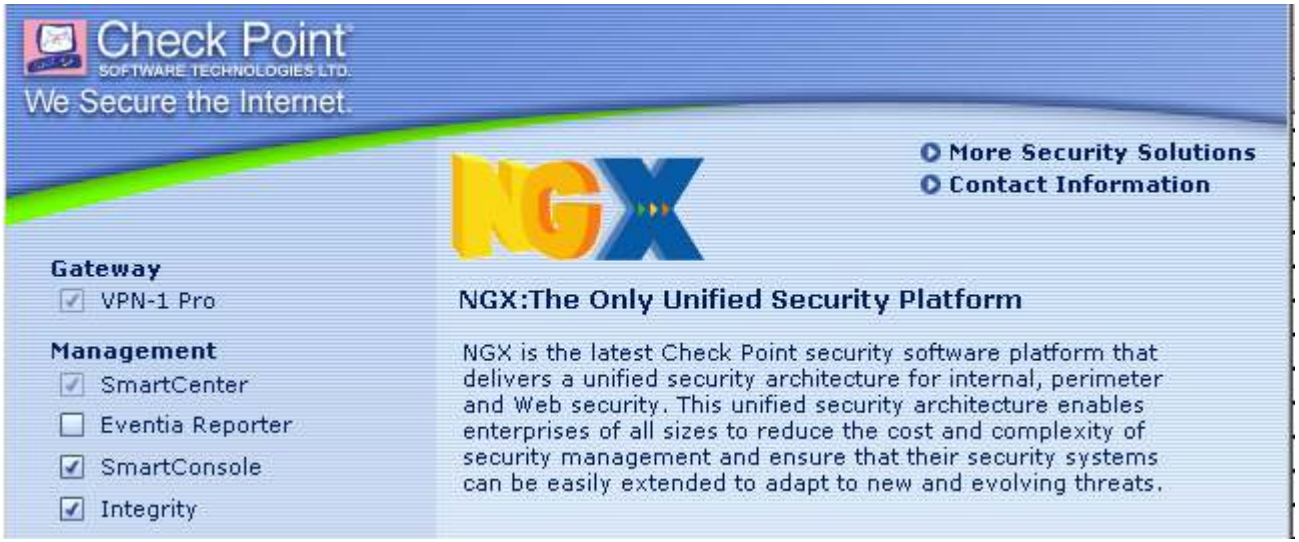
- Check Point SMART integration
  - Data Management
    - Send all relevant client logs to SmartCenter
    - Special log views in SmartView Tracker
    - Integrity Monitoring using SmartView Monitor
    - Integrity Reporting with Eventia Reporter
  - Shared Objects
    - Integrity objects in SmartDashboard
    - 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

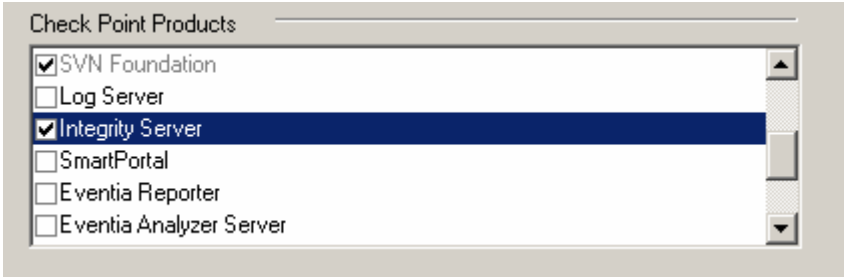
Integrity integration

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

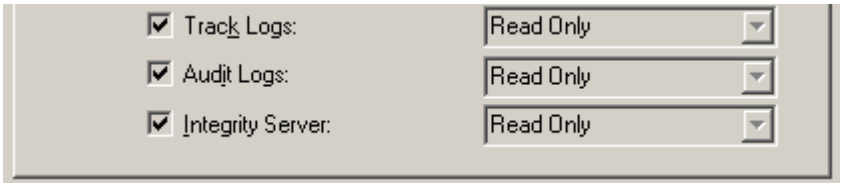


Integrity integration (cont)

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

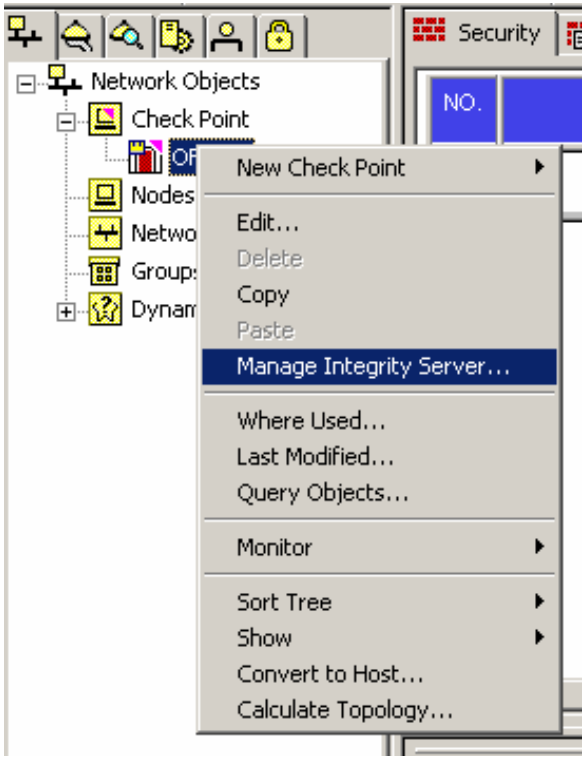


- An administrator defined via SmartDashboard can be assigned with permission to access integrity server.



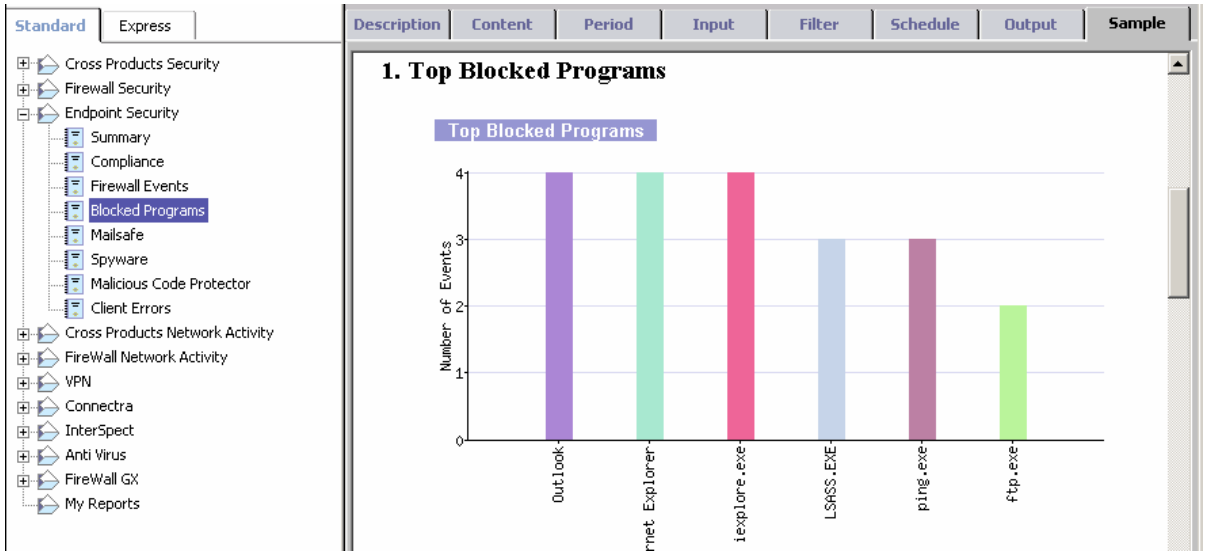
Integrity integration (cont)

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

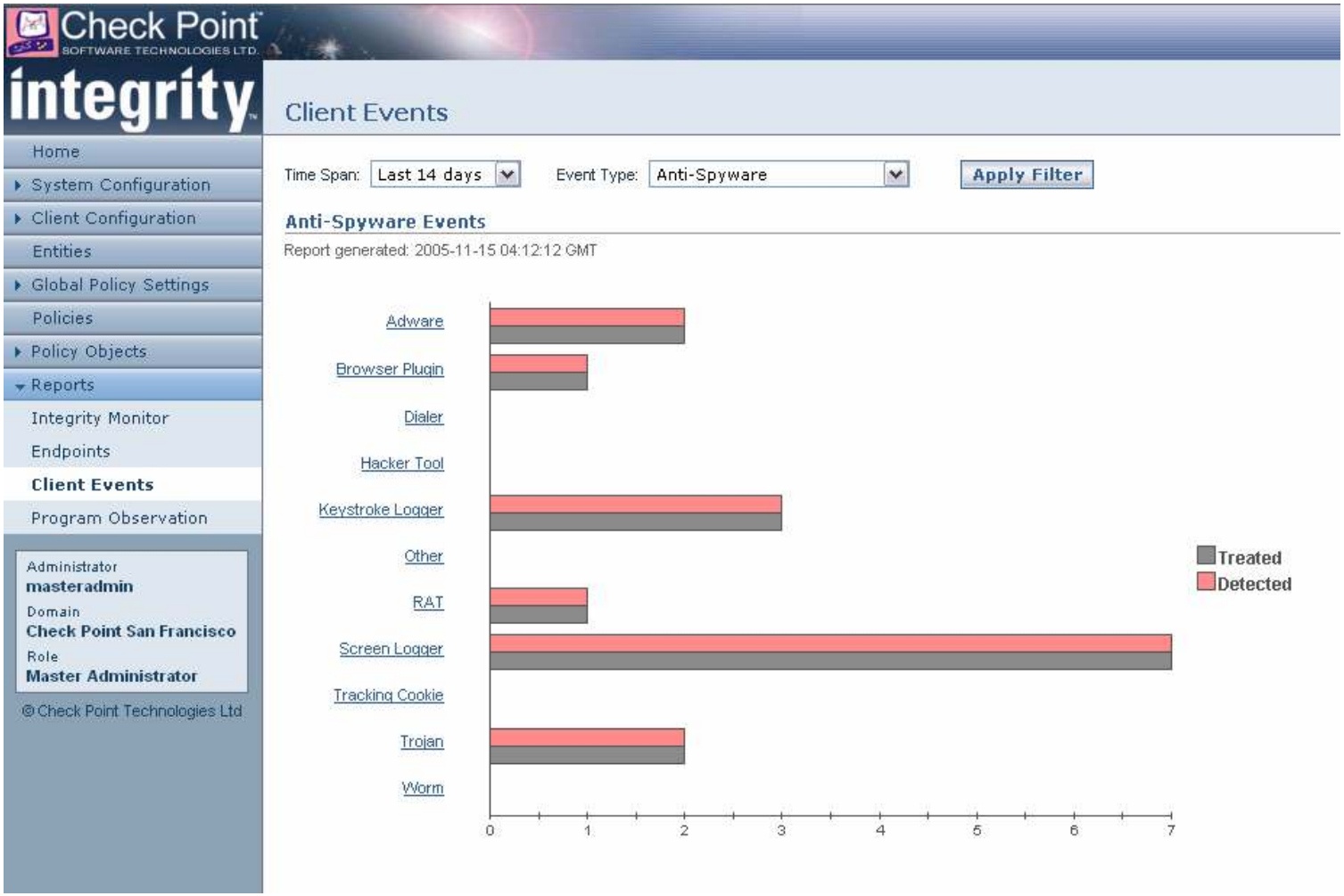


New Reporting Capabilities

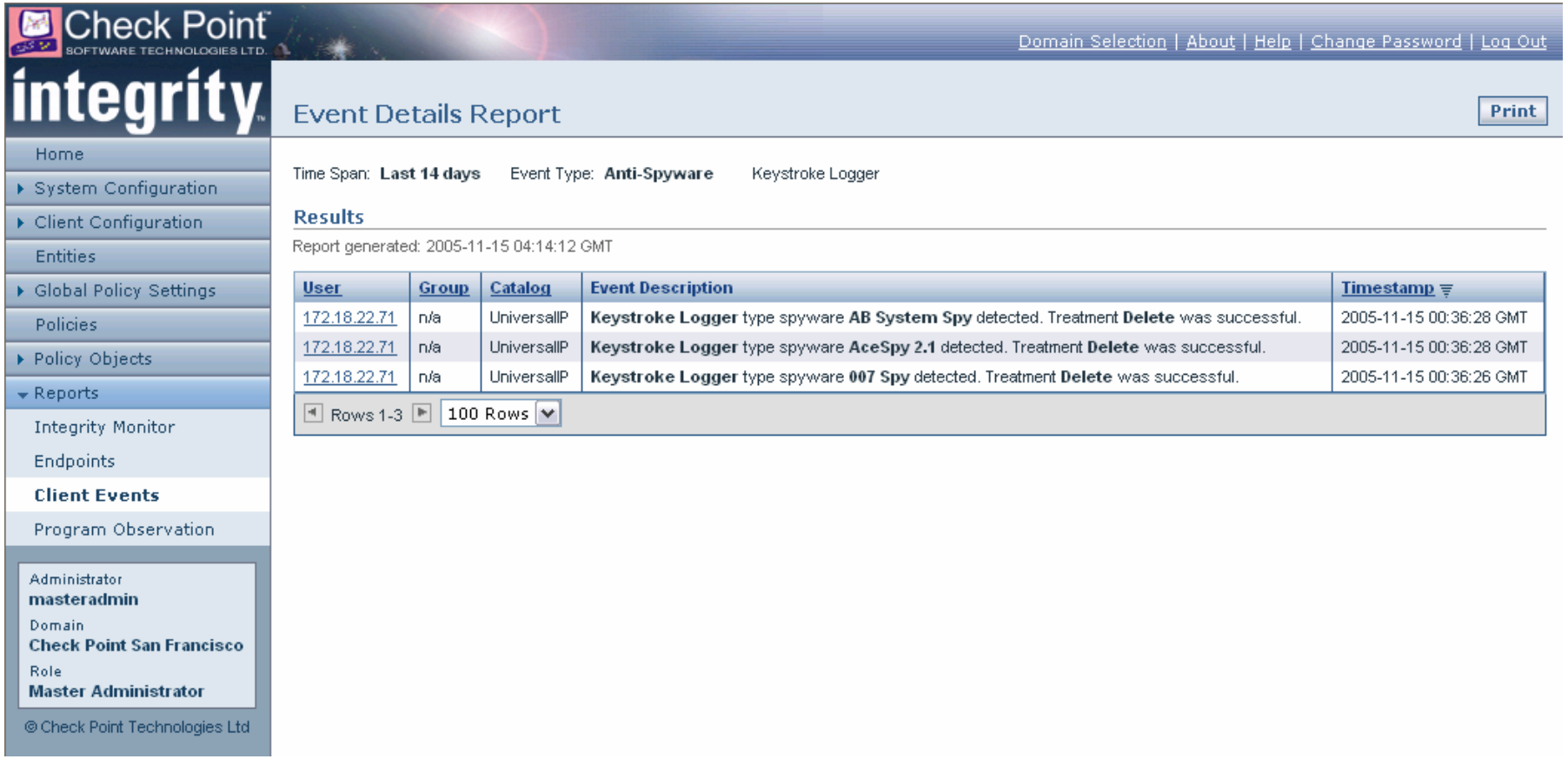
- Reporting now includes:
  - Eventia Suite Integration
  - Integrity Monitor
  - Improved logging
  - More filtering & drill-down options
  - More charting
  - More information



Spyware Reporting

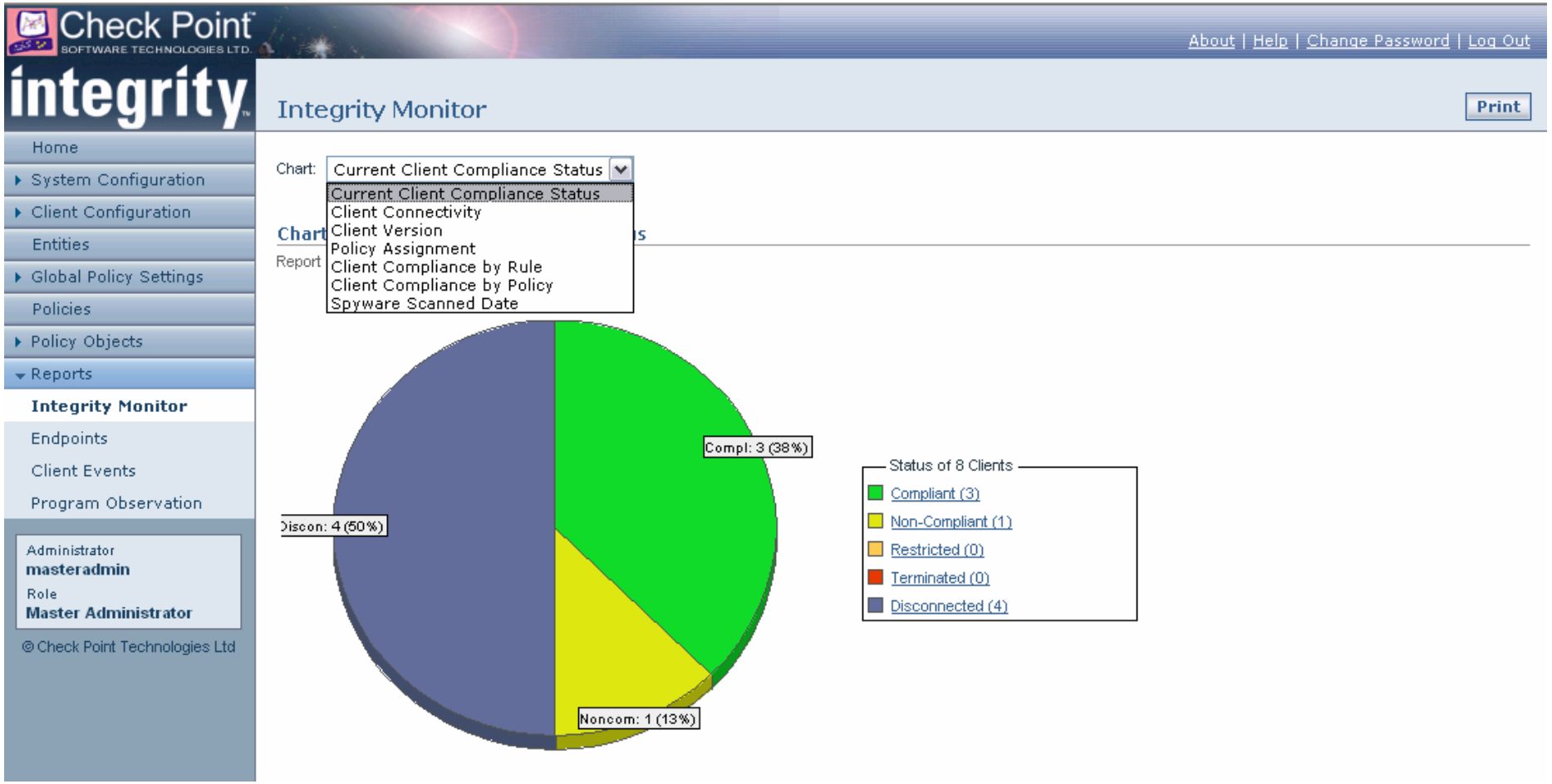


Spyware Details Report

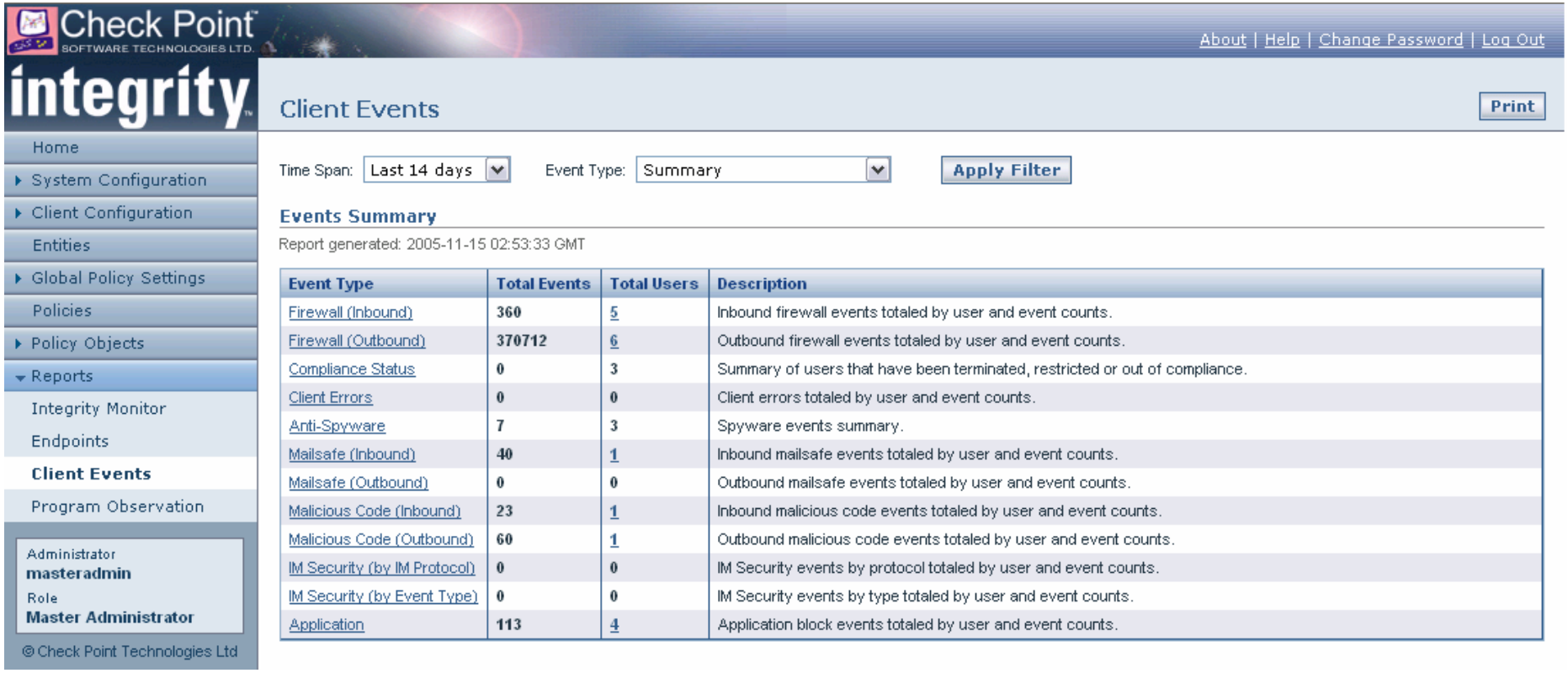


User Report

Integrity Monitor



Summary Report



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