What’s new in R71

Jani Ekman
June 10, 2010
Check Point Makes DLP Work
Agenda

1. What is Data Loss?
2. Key Challenges of DLP
3. Introducing Check Point DLP
4. Summary

Check Point DLP
Makes data loss prevention work
Data Loss Prevention

What is DLP?

E-mail sent to the wrong recipient, intentionally or by mistake.

Company document uploaded to an external website.

Data breaches have happened to all of us.
Data Breaches—Headline Examples

Brand Damage
Compliance
Liabilities
Costly Fines
It’s Not Just About Regulatory Compliance

<table>
<thead>
<tr>
<th>Compliance</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>► Customer data</td>
<td>► Intellectual property</td>
</tr>
<tr>
<td>► Corporate data</td>
<td>► Strategic plans</td>
</tr>
<tr>
<td>► Patient data</td>
<td>► Internal data</td>
</tr>
</tbody>
</table>

Chief Compliance Officer

Chief Security Officer
DLP Has Not Yet Been Solved!

Technology

Computers can not reliably understand human content and context

IT Staff

Challenge

Burden of incident handling

Exposure to sensitive data
John,

Let’s review the corporate strategy in our morning meeting.

Confidential data sent to the wrong recipient!

User prompted to take action

User remediates
John,
Let’s review the corporate strategy in our morning meeting.

John.Stevens@yahoo.com

Corporate Strategy

Data Loss Prevention Alert

An email that you have just sent has been quarantined.

Reason: attached document contains confidential internal data

The message is being held until further action.

Send, Discard, or Review Issue

Introducing Check Point Data Loss Prevention

Check Point Combines Technology and Processes to Make DLP Work

NEW!

Prevent
Move from detection to prevention

Educate
Users on corporate data policies

Enforce
Data loss business processes
Check Point Solves the DLP Challenge

New UserCheck™ Technology

Technology Challenge
Empowers users to remediate incidents in real time

IT Staff Challenge
Educates users on DLP policies without involving IT staff
How Does Check Point DLP Work?

MultiSpect™ Detection Engine

Simple Rule-based Policy Management

Full Network Enforcement
<table>
<thead>
<tr>
<th>Item</th>
<th>Name</th>
<th>Social Security Number</th>
<th>Job Title</th>
<th>Gross Pay</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>John Smith</td>
<td>987-65-4320</td>
<td>CEO</td>
<td>$200,000</td>
</tr>
<tr>
<td>2</td>
<td>Kevin Brian</td>
<td>987-65-4221</td>
<td>VP R&amp;D</td>
<td>$150,000</td>
</tr>
<tr>
<td>3</td>
<td>Margret White</td>
<td>769-65-7522</td>
<td>VP Marketing</td>
<td>$153,000</td>
</tr>
<tr>
<td>4</td>
<td>Bob Johns</td>
<td>342-62-3323</td>
<td>CFO</td>
<td>$140,000</td>
</tr>
<tr>
<td>5</td>
<td>Mike Riddle</td>
<td>777-43-4324</td>
<td>COO</td>
<td>$180,000</td>
</tr>
</tbody>
</table>

New MultiSpect™ Technology

**MultiSpect Detection Engine**

- Correlates data from multiple sources using open language
- Detects more than 600 file formats
- Over 250 pre-defined content data types
- Detect and recognize proprietary forms and templates

Correlates data from multiple sources using open language

**250+ Data Types**

MultiSpect Detection Engine

Detects more than 600 file formats

Over 250 pre-defined content data types

Detect and recognize proprietary forms and templates
Simple Rule-based Policy Management

Easily Define Policy to Detect, Prevent or Ask User
Unified Control and Deployment

Centralized Management

Data Loss Prevention

For Unified Control Across the Entire Security Infrastructure
Ease-of-Deployment

**Software Blade**

On Existing Gateways or Open Servers

**Dedicated Appliance**

DLP-1

**Network-based Inline Solution**

Be Up and Running Day-1!
Move from Detection to Prevention

- Proactively block intentional and unintentional data loss
- Inline network-based Software Blade running on any existing Check Point gateway
- Supporting HTTP, SMTP and FTP protocols
- UserCheck notification using either thin agent or a returning email to the user
- Scaling from hundred to thousands of users
Check Point DLP Summary

Check Point combines technology and processes **to make DLP work**

- **Prevent Data Breaches**
  Move from detection to prevention

- **Enforce Data Policies**
  Across the entire network

- **Educate and Alert Users**
  Without involving IT staff
Check Point DLP in Detail

Check Point DLP User Scenarios

Key DLP Technologies
Check Point DLP at Work

Scenario 1: Prevent
Block Web upload of proprietary information

Scenario 2: Enforce
Filter communications of confidential information based on policy exception

Scenario 3: Alert, Ask and Educate
Ask user to confirm and remediate potential breach
Preemptively Prevent Data Breaches

Web Upload of Proprietary Information

Check Point DLP blocks upload and notifies user

Software Developer

http://mywebuploads.com
Filter Based on Corporate Data Policies

Policy Exception Allows Email to Pre-selected Recipients

Corporate VP sends M&A contract to attorney

Hi James,

We have revised the terms of the acquisition. Attached is the Letter of Intent for your review.

Thanks,

David

Data Loss Prevention Alert

An email that you have just sent has been identified as containing sensitive information.

An email that you have just sent has been allowed based on DLP policy exception.

For additional details, please refer to the Corporate Data Security Policy

Alert notifies user of data policy
Alert, Ask and Educate Users

Check Point Brings User Remediation to DLP

User provides an explanation of his request to send

Hi,
This information is OK to send to our outside auditor.
Thanks, Matt
Key Technologies

UserCheck™ provides User Remediation

Align DLP Rules to Your Policies and Processes

MultiSpect™ Detection Engine
UserCheck Provides User Remediation

1. Mail sent or document uploaded

2. User alert

3. User remediation

Data Loss Prevention Alert
An email that you have just sent has been quarantined.

Reason: attached document contains confidential internal data

The message is being held until further action.

Send, Discard, or Review Issue

Non-disruptive

Real-time

Educational
Align With Your Business Processes

Adapts to Your Processes and Environment

Examples

► Spreadsheets with over 500 rows
► More than 5 financial terms
► External recipients in BCC
► More than 10 company names
► Profanity

Suspicious Communications

Identify unconventional business communication behavior
MultiSpect™ Detection Engine

Multi-data Correlation Prevents Potential Violations

Correlates a combination of data types

Prevents sending sensitive data to wrong recipients
MultiSpect Form Detection

Detect and Recognize Your Proprietary Forms

Forms/Partial

Recognize sensitive forms and templates

- HR forms / salary / offers
- Financial docs
- Patient records
- Insurance forms
- Bank forms

MultiSpect Form Detection

Detect and Recognize Your Proprietary Forms

Data Type Wizard

Documents Based on a Corporate Template

INSURANCE CLAIM FORM

Any person who knowingly and with intent to injure, defraud, or deceive any insurance company or other person submits an insurance application or statement of claim containing any materially false, incomplete or misleading information may be committing a crime and may be subject to civil or criminal penalties.

Group Plan or Program:

Policyholder: 
Policy Number: 
Certificate/ID Number: 

Present Address:
No. and Street: 
City or Town: 
State: 
Zip Code Country: 

Home Address:
No. and Street: 
City or Town: 
State: 
Zip Code Country: 

Telephone Number: 
Date of Birth: 
Male Female (Circle One)

If payment was made to someone other than the Insured, who is to receive payment?

Relationship to insured: 
Address: 

Date of Accident or Sickness: 
Nature of Accident or Sickness: 

If accident, describe fully how and where accident occurred:

If injured in play or practice of sport, indicate what sport:

Is the insured covered under any other group plan, health maintenance organization, government plan, or insurance policy? 
Yes ☐ No ☐

Insurance Company: 
Policy Number: 

Are you covered as a dependent under this policy? 
Yes ☐ No ☐

Are you covered under your school's domestic student accident and sickness insurance plan? 
Yes ☐ No ☐

Source of School:
MultiSpect Open Scripting Language

Extended Data Type Creation

- Create completely new data types
- Enhance existing data types
- Flexibly tailor DLP to your environment

Custom Data Type

- Open Scripting Language
## DLP-1 Appliance Specifications

<table>
<thead>
<tr>
<th>Specifications</th>
<th>DLP-1 2571</th>
<th>DLP-1 9571</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Performance</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of users</td>
<td>1,000</td>
<td>5,000</td>
</tr>
<tr>
<td>Messages/Hour</td>
<td>70K</td>
<td>350K</td>
</tr>
<tr>
<td>Throughput</td>
<td>700 Mbps</td>
<td>2.5 Gbps</td>
</tr>
<tr>
<td><strong>Specifications</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage</td>
<td>500 GB</td>
<td>2 x 1 TB (RAID 1)</td>
</tr>
<tr>
<td>NICs</td>
<td>6 Copper 1GbE</td>
<td>10 Copper 1GbE</td>
</tr>
<tr>
<td>Optional Bypass card</td>
<td>4 ports - 2 segments (pre-packaged appliance)</td>
<td>4 ports - 2 segments (orderable as accessory)</td>
</tr>
</tbody>
</table>
Check Point DLP Summary

Check Point combines technology and processes to make DLP work

Prevent Data Breaches
Move from detection to prevention

Enforce Data Policies
Across the entire network

Educate and Alert Users
Without involving IT staff
Turn Security Information into Action

Introducing SmartEvent Software Blade
Agenda

1. Security Management Challenges
2. Introducing SmartEvent
3. SmartEvent Key Benefits
4. Summary
Security Management Challenges

Getting Actionable Information

Leveraging Information to Stop Attacks Across the Enterprise
Customer Needs

Security management that provides

- **More Visibility**
  - To monitor critical events across security systems

- **Faster Remediation**
  - With more actionable information

- **More Simplicity**
  - For more efficiency and easy deployment
Introducing SmartEvent Software Blade

SmartEvent translates security information into action

More Visibility
Faster Remediation
Simple!
SmartEvent Software Blade

Better Visibility
Better Visibility

Monitor ONLY what is important!

Easily monitor top events
See through the mass and focus on critical events
Better Visibility Across Security Systems

View unified events for firewall, IPS, DLP, endpoint and more in a single console
Better Visibility for Easier Compliance

Unified compliance reporting

SOX Compliance

PCI Compliance

Logins by Date

Top users by Number of Logins

GTP Firewall Security Alerts

List

Risk Summary

0 1 2 3 4
Number of Events
0 5 10 15 20
0 50 100 150 200 250 300
Number of Events
0 1 2 3 4 5
Date
01-Jul-04 02-Jul-04 03-Jul-04 04-Jul-04 05-Jul-04 06-Jul-04 07-Jul-04

©2010 Check Point Software Technologies Ltd. | [Unrestricted] For everyone | 40
SmartEvent Software Blade

Faster Remediation
Faster Remediation

Stop attacks straight from the event screen

Change policy to prevent critical threats
Faster Remediation

Block malicious traffic from rogue nations

Geo Protection
Block network traffic to and from any country.

Policy for Specific Countries

Trojanland
Block traffic by country with Geo Protection

Identify traffic activity from Trojanland

Trojanland is now blocked
SmartEvent Software Blade

Simple
Ease of Deployment

Deployment Options

Software Blade

- Easily add to your existing security management

All-in-One Dedicated Appliance

- Pre-configured and plug-and-play
# Smart-1 SmartEvent Appliances

<table>
<thead>
<tr>
<th></th>
<th>Smart-1 SmartEvent 5</th>
<th>Smart-1 SmartEvent 25</th>
<th>Smart-1 SmartEvent 50*</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Storage</strong></td>
<td>1 x 0.5 TB</td>
<td>4 x 0.5 TB</td>
<td>4 x 1 TB</td>
</tr>
<tr>
<td><strong>Managed GWs</strong></td>
<td><strong>5 / 25</strong></td>
<td><strong>25 / 50</strong></td>
<td><strong>50 / 150</strong></td>
</tr>
<tr>
<td><strong>Logging Capacity</strong></td>
<td><strong>2GB per day</strong></td>
<td><strong>10GB per day</strong></td>
<td><strong>25GB per day</strong></td>
</tr>
</tbody>
</table>
Summary

Check Point SmartEvent translates security information into action

More Visibility across firewall, IPS, DLP, endpoint and more

Faster Remediation

Easy To Deploy
Raising the bar on UTM-1 and UTM software blades performance
Agenda

1. Raising the bar on Antivirus and URL Filtering software blades performance
2. UTM-1 firewall performance improvement
3. How to benefit from boost
3. Summary
New Performance Levels

AV & URLF software blades

Amazing boost for Antivirus and URL filtering software blades performance across systems

UTM-1

Enhanced firewall performance for 5 UTM-1 models

Simple Upgrade

Simply upgrade your existing UTM-1 device or software blades to new R71 software release
Raising the Bar on Antivirus & URL Filtering Software Blades Performance

Antivirus throughput 2-core system

X 15 Antivirus throughput improvement

AV & URLF Concurrent Sessions

Up to 80 X Anti-virus & URL Filtering connection capacity improvement
Raising the bar on UTM-1 performance

Better protection with better performance

NEW!
Raising the Bar on UTM-1 Performance

Up to 4x **Firewall** throughput improvement

AND

Up to 3x **IPS** throughput improvement

AND

Up to 4x **connection/second** improvement
Simple Software Upgrade

Simple Upgrade

1-2-3

Simple software upgrade to new R71 release

On same existing system or gateway

Immediate protection and performance boost
More protection, uncompromised performance

Activate today all layers of security on your gateway
Performance Improvement Summary

- Firewall x4
- IPS x3
- Connection/sec. x4
- Antivirus x15
- AV and URLF connection x80
Raising the Bar on UTM-1 Performance

Up to 4x **Firewall** throughput improvement

- Small office or branch
- SMB to medium branch

<table>
<thead>
<tr>
<th>Firewall throughput (Gbps)</th>
<th>$5,000</th>
<th>$10,000</th>
<th>$15,000</th>
<th>$20,000</th>
<th>$25,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>UTM-1 136</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UTM-1 276</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UTM-1 576</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UTM-1 1076</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UTM-1 2076</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UTM-1 3076</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Performance Improvement Summary

- Firewall x4
- Antivirus x15
- AV and URLF connection x80
Thank You!

Jani.ekman@checkpoint.com