Security Information and Event Management


Chris Bloom, RSA, The Security Division of EMC
Today’s Agenda

- The Evolving Landscape Around Security & Compliance
- How RSA enVision Turns Log Data Into Actionable Information
- The RSA enVision Difference
Challenge: Changing Threat Profile

- Attacks occur over long periods of time
  - TJX - Credit card data compromised over 17-month period at retailer
- Insiders perpetrating more and bigger thefts
  - Fidelity National - Database administrator at investment organization stole 2.3 million consumer records and successfully sold them
- “Cybercrime has become a $105B business that now surpasses the value of the illegal drug trade worldwide” (David DeWalt, McAfee CEO, September 2007)
Challenge: Compliance More Proscriptive, Complex and Expensive Than Ever

- **Specific mandates**
  - e.g. PCI, partner contracts etc. …
  - very prescriptive (thou shalt encrypt data at rest etc.)

- **Best practice based mandates**
  - e.g. EUDPD, HIPAA, SOX
  - “thou shalt exert best practice when thou dealest with my data”
  - However, leaves exact details of “how” and “what” open to interpretation.

- **Mandatory disclosure**
  - e.g. State privacy laws –
  - Don’t specify what has to be done, but…
  - If you lose my data you must inform us about it
Challenge: Infrastructures and organizations are getting ever more complex

- IT environments are seldom single, monolithic entities
  - Invariably a complex mass of conflicting technologies
  - Ill-defined priorities
  - All managed by a matrix organization

- It’s difficult to get visibility into the IT environment
  - What is out there?
  - What activities are taking place?
  - What will stop working when I make a change?
  - What impact will that have on the business?
Challenge: Explosive Growth of Security Data

- more growth: Estimated 58% CAGR for security information over next five years (ESG, 2006)
- more types: firewalls, VPNs, hosts, applications, storage …
- more uses: Security Operations, Compliance, Risk Management, Application Performance, IT Operations …
- more regulations: Sarbanes-Oxley, PCI, Basel II, GLBA, HIPAA, FISMA, etc. (more coming!) …
Today’s Agenda

- The Evolving Landscape Around Security & Compliance
- How enVision Turns Log Data Into Actionable Information
- The RSA enVision Difference
Logs Are a Goldmine of Data

- Unix
- Database
- Application
- Router
- Firewall
- Intrusion Prevention System
- File Server

Log File

Program installed
User account created
Failed login
Unauthorized access attempt
Database design change
RSA enVision Turns Log Data into Information

RSA enVision Supported Devices:
- Windows Server
- Netscreen Firewall
- Cisco IPS
- Juniper IDP
- Microsoft ISS
- Trend Micro Antivirus
- Device
- Device

Legacy:
- Integrated Incident Mgmt.
- Interactive Query
- Forensics
- Realtime Analysis
- Baseline
- Correlated Alerts
- Report

Analyze

Manage

Log Mgmt

SIEM

UDS

Interactive Query

Integrated Incident Mgmt.

Realtime Analysis

Forensics

Baseline

Correlated Alerts

Report

Collect

Collect

Collect

Correlated Alerts

SA enVision Supported Devices
RSA enVision: Purpose-Built Platform
Non-Intrusive, Extensible, Easy to Deploy

Security event & operations info. No data filtering
Parallel architecture ensures alert performance
Easy to deploy appliance packaging

No agents required
Flexible XML UDS engine

Customizable work environments
Fully customizable compliance & security reports
RSA enVision and LogSmart IPDB
All the Data™ with Consistently High Performance

Limitations of Relational Database

• Not designed for unstructured data (log)
• Requires processing (filter, normalize, parse)
• Unpredictable consumption: collection bottleneck impacts use of data (e.g. alerts)
• Data Loss: events are lost due to selective collection or system bottleneck
• Data Explosion: indexes & related data structure information is added (can result in <10x data)
RSA enVision and LogSmart IPDB

All the Data™ with Consistently High Performance

Data Explosion
- Not designed for unstructured data (log)
- Requires processing (filter, normalize, parse)

Data Loss
- Events are lost due to selective collection or system bottleneck

LogSmart IPDB
- Encrypted
- Compressed
- Authenticated

Relational Database
- DB OVERHEAD
- NORMALIZATION
- Data Loss
- Data Explosion
- Unpredictable Alerts

Parallel analysis
- REAL TIME ANALYZE
- Authenticated
- Compressed
- Encrypted
Manages the Lifecycle of Security Information

- User Defines Log Retention Policies
- RSA enVision Automatically Enforces Policies

Online Policy (~ 15 months)
Capture  Compress  Secure  Store Online  Retention Policy  Retain in Nearline  Retire

EMC Celerra  EMC Centera

© Copyright 2008 EMC Corporation. All rights reserved.
Scales from Single Appliance to Global Deployment

A-SRV: Analysis Server
D-SRV: Data Server
LC: Local Collector
RC: Remote Collector

© Copyright 2008 EMC Corporation. All rights reserved.
Presents Information in Easily Digestible Format

>1100 reports for regulatory compliance, security, and IT & network operations
**Integrates Seamlessly with EMC Storage**

**Online Storage**

<table>
<thead>
<tr>
<th>ST31XX Direct Attached</th>
<th>RSA enVision DAS2000</th>
<th>Single Appliance</th>
<th>1TB-2.5TB</th>
<th>&gt;2.75TB</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA enVision NAS3500</td>
<td>Based on EMC Celerra</td>
<td>Multi-Appliance</td>
<td>&gt;3.5TB - 7TB</td>
<td></td>
</tr>
<tr>
<td>Celerra Family - Integrated Network Attached</td>
<td>&gt;Enterprise Class</td>
<td>&gt;5TB +</td>
<td></td>
<td></td>
</tr>
<tr>
<td>With Celerra Gateway:</td>
<td>EMC Clarion Family</td>
<td>&gt;Enterprise Class</td>
<td>&gt;5TB +</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EMC Symmetrix Family</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Longer Retention Storage**

| Centera Content Addressed Storage Systems |

---

*External Network Attached Storage Recommended for all RSA enVision LS cluster deployments, Required for High Availability*
Options for Smallest to Largest Deployments

EPS

LS Series

ES Series

© Copyright 2008 EMC Corporation. All rights reserved.
Today’s Agenda

- The Evolving Landscape Around Security & Compliance
- How enVision Turns Log Data Into Actionable Information
- The RSA enVision Difference
### All the Data

- Ability to Collect, Manage & Analyze All the Data
- Single Global View
- Event Source Support
- Non-invasive Deployment
- Interoperable & Extensible

### All the Time

- Cradle to Grave ILM
- High Availability Infrastructure
- Uninterrupted Scalability
- High and Consistent Application Performance
- Low TCO

- Strong Customer Focused Organization
Advantage: Maximum Efficiency and Low TCO

Data Storage Advantage

GBs Per Day

Collection Rate Advantage

System Performance

© Copyright 2008 EMC Corporation. All rights reserved.
Advantage: Independently Acknowledged Industry Leader

Source: Gartner (May 2008)
## Advantage: Unparalleled Demonstrable Scalability

<table>
<thead>
<tr>
<th>Organization</th>
<th>Driver</th>
<th>Locations</th>
<th>Events</th>
<th>Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDS</td>
<td>Security</td>
<td>34</td>
<td>240K/Sec, 20B/Day, 76.8T/Year</td>
<td>30,000</td>
</tr>
<tr>
<td></td>
<td>• Configuration Control</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Access Control Enforcement</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Privileged User Monitoring</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Compliance &amp; Security</td>
<td>18</td>
<td>180K/Sec, 15.5B/Day, 5.6T/Year</td>
<td>20,000</td>
</tr>
<tr>
<td></td>
<td>• Real-Time Monitoring</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• False Positive Reduction</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Access Control Enforcement</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EDS</td>
<td>Compliance</td>
<td>28</td>
<td>450K/Sec, 38.8T/Day, 148T/Year</td>
<td>28,000</td>
</tr>
<tr>
<td></td>
<td>• SAS 70 Compliance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIG</td>
<td>Compliance &amp; Security</td>
<td>4</td>
<td>80K/Sec, 6.9B/Day, 2.5T/Year</td>
<td>4,000</td>
</tr>
<tr>
<td></td>
<td>• Log Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Monitoring Firewalls For Audits</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Compliance</td>
<td>3</td>
<td>95K/Sec, 8.2T/Day, 2.9T/Year</td>
<td>17,000</td>
</tr>
<tr>
<td></td>
<td>• Internal Audit</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Advantage: Unparalleled Client Base
Over 1300 Clients

Energy & Utility

Retail & Hospitality

Healthcare

Fortune 500

Financial Services
Summary

- Logs are a gold mine of information for
  - Improving security
  - Demonstrating compliance
  - Streamlining IT operations

- RSA enVision turns log data into information
  - Readable reports
  - Actionable alerts
  - At-a-glance dashboards

- RSA enVision is widely accepted as the leading SIEM solution
  - Unparalleled demonstrable scalability
  - Independently validated leadership
  - Invaluable install base
EMC²
where information lives®
Today’s Agenda

- The Evolving Landscape Around Security & Compliance
- How RSA enVision Turns Log Data Into Actionable Information
- The RSA enVision Difference
Challenge: Changing Threat Profile

- Attacks occur over long periods of time
  - TJX - Credit card data compromised over 17-month period at retailer

- Insiders perpetrating more and bigger thefts
  - Fidelity National - Database administrator at investment organization stole 2.3 million consumer records and successfully sold them

- “Cybercrime has become a $105B business that now surpasses the value of the illegal drug trade worldwide” (David DeWalt, McAfee CEO, September 2007)
Challenge: Compliance More Proscriptive, Complex and Expensive Than Ever

- **Specific mandates**
  - e.g. PCI, partner contracts etc. …
  - very prescriptive (thou shalt encrypt data at rest etc.)

- **Best practice based mandates**
  - e.g. EUDPD, HIPAA, SOX
  - “thou shalt exert best practice when thou dealest with my data”
  - However, leaves exact details of “how” and “what” open to interpretation.

- **Mandatory disclosure**
  - e.g. State privacy laws –
  - Don’t specify what has to be done, but…
  - If you lose my data you must inform us about it
Challenge: Infrastructures and organizations are getting ever more complex

- IT environments are seldom single, monolithic entities
  - Invariably a complex mass of conflicting technologies
  - Ill-defined priorities
  - All managed by a matrix organization

- It’s difficult to get visibility into the IT environment
  - What is out there?
  - What activities are taking place?
  - What will stop working when I make a change?
  - What impact will that have on the business?
Challenge: Explosive Growth of Security Data

more growth:
Estimated 58% CAGR for security information over next five years (ESG, 2006)

more types:
firewalls, VPNs, hosts, applications, storage …

more uses:
Security Operations, Compliance, Risk Management, Application Performance, IT Operations …

more regulations:
Sarbanes-Oxley, PCI, Basel II, GLBA, HIPAA, FISMA, etc.
(more coming!) …
Today’s Agenda

- The Evolving Landscape Around Security & Compliance
- How enVision Turns Log Data Into Actionable Information
- The RSA enVision Difference
Logs Are a Goldmine of Data

- Unix
- Database
- Intrusion Prevention System
- Application
- Router
- Firewall
- File Server
- Log File

- Program installed
- User account created
- Failed login
- Unauthorized access attempt
- Database design change
RSA enVision Turns Log Data into Information

RSA enVision Supported Devices

Log Mgmt

Windows Server
Netscreen Firewall
Cisco IPS
Juniper IDP
Microsoft ISS
Trend Micro Antivirus

Device
Device

Legacy

SIEM

UDS

RSA enVision Supported Devices

Collect
Collect
Collect

Baseline
Correlated Alerts
Report
Realtime Analysis
Forensics
Interactive Query
Integrated Incident Mgmt.

Analyze

Manage
RSA enVision: Purpose-Built Platform
Non-Intrusive, Extensible, Easy to Deploy

- Security event & operations info. No data filtering
- Parallel architecture ensures alert performance
- Easy to deploy appliance packaging
- No agents required
- Flexible XML UDS engine
- Customizable work environments
  Fully customizable compliance & security reports
Limitations of Relational Database

• Not designed for unstructured data (log)
• Requires processing (filter, normalize, parse)
• Unpredictable consumption: collection bottleneck impacts use of data (e.g. alerts)
• Data Loss: events are lost due to selective collection or system bottleneck
• Data Explosion: indexes & related data structure information is added (can result in <10x data)
Manages the Lifecycle of Security Information

- User Defines Log Retention Policies
- RSA enVision Automatically Enforces Policies

Online Policy (~ 15 months)
- Capture
- Compress
- Secure
- Store Online

Retention Policy
- Retain in Nearline
- Retire

ILM

EMC Celerra
EMC Centera

© Copyright 2008 EMC Corporation. All rights reserved.
Scales from Single Appliance to Global Deployment

A-SRV: Analysis Server
D-SRV: Data Server
LC: Local Collector
RC: Remote Collector

Chicago
WW Security Operations

London
European Headquarters

New York
WW Compliance Operations

Mumbai
Remote Office

© Copyright 2008 EMC Corporation. All rights reserved.
>1100 reports for regulatory compliance, security, and IT & network operations
### Online Storage

<table>
<thead>
<tr>
<th>RSA: ST31XX Direct Attached</th>
<th>RSA enVision NAS3500</th>
<th>Single Appliance</th>
<th>&gt;1TB-2.5TB, &gt;2.75TB</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA enVision DAS2000</td>
<td>Based on EMC Celerra</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSA enVision NAS3500</td>
<td></td>
<td>Multi-Appliance</td>
<td>&gt;3.5TB - 7TB</td>
</tr>
<tr>
<td>Based on EMC Celerra</td>
<td></td>
<td>Enterprise Class</td>
<td></td>
</tr>
<tr>
<td>Celerra Family - Integrated</td>
<td></td>
<td>Enterprise Class</td>
<td>&gt;5TB +</td>
</tr>
<tr>
<td>Network Attached</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>With Celerra Gateway:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EMC Clarion Family</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EMC Symmetrix Family</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Longer Retention Storage

- Centera Content Addressed Storage Systems

---

*External Network Attached Storage Recommended for all RSA enVision LS cluster deployments, Required for High Availability*
Options for Smallest to Largest Deployments

- **EPS**
  - 500
  - 1000
  - 2500
  - 5000
  - 10000
  - 30000

- **ES Series**
  - 7500
  - 300,000

- **LS Series**

# DEVICES
- 150
- 300
- 750
- 1250
- 1500
- 2048
- 30,000
Today’s Agenda

- The Evolving Landscape Around Security & Compliance
- How enVision Turns Log Data Into Actionable Information
- The RSA enVision Difference
Advantage: Best-in-Class Functionality

All the Data

- Ability to Collect, Manage & Analyze All the Data
- Single Global View
- Event Source Support
- Non-invasive Deployment
- Interoperable & Extensible

All the Time

- Cradle to Grave ILM
- High Availability Infrastructure
- Uninterrupted Scalability
- High and Consistent Application Performance
- Low TCO

- Strong Customer Focused Organization
**Advantage: Maximum Efficiency and Low TCO**

**Data Storage Advantage**

- Graph showing GBs per day for different events per second (EPS) for RDBMS and LogSmart IPDB.

**Collection Rate Advantage**

- Graph showing system performance in EPS for RDBMS and LogSmart IPDB.
Advantage: Independently Acknowledged Industry Leader

Source: Gartner (May 2008)
## Advantage: Unparalleled Demonstrable Scalability

<table>
<thead>
<tr>
<th>Organization</th>
<th>Driver</th>
<th>Locations</th>
<th>Events</th>
<th>Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>EDS</strong></td>
<td><strong>Security</strong></td>
<td>34</td>
<td>240K/Sec, 20B/Day, 76.8T/Year</td>
<td>30,000</td>
</tr>
<tr>
<td></td>
<td>- Configuration Control</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Access Control Enforcement</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Privileged User Monitoring</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>JP Morgan Chase</strong></td>
<td><strong>Compliance &amp; Security</strong></td>
<td>18</td>
<td>180K/Sec, 15.5B/Day, 5.6T/Year</td>
<td>20,000</td>
</tr>
<tr>
<td></td>
<td>- Real-Time Monitoring</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- False Positive Reduction</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Access Control Enforcement</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>EDS</strong></td>
<td><strong>Compliance</strong></td>
<td>28</td>
<td>450K/Sec, 38.8T/Day, 148T/Year</td>
<td>28,000</td>
</tr>
<tr>
<td></td>
<td>- SAS 70 Compliance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>AIG</strong></td>
<td><strong>Compliance &amp; Security</strong></td>
<td>4</td>
<td>80K/Sec, 6.9B/Day, 2.5T/Year</td>
<td>4,000</td>
</tr>
<tr>
<td></td>
<td>- Log Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Monitoring Firewalls For Audits</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Compliance</strong></td>
<td>- Internal Audit</td>
<td>3</td>
<td>95K/Sec, 8.2T/Day, 2.9T/Year</td>
<td>17,000</td>
</tr>
</tbody>
</table>
Advantage: Unparalleled Client Base
Over 1300 Clients

- Energy & Utility
- Retail & Hospitality
- Healthcare
- MSSP
- Fortune 500
- Financial Services
Summary

- Logs are a gold mine of information for
  - Improving security
  - Demonstrating compliance
  - Streamlining IT operations

- RSA enVision turns log data into information
  - Readable reports
  - Actionable alerts
  - At-a-glance dashboards

- RSA enVision is widely accepted as the leading SIEM solution
  - Unparalleled demonstrable scalability
  - Independently validated leadership
  - Invaluable install base