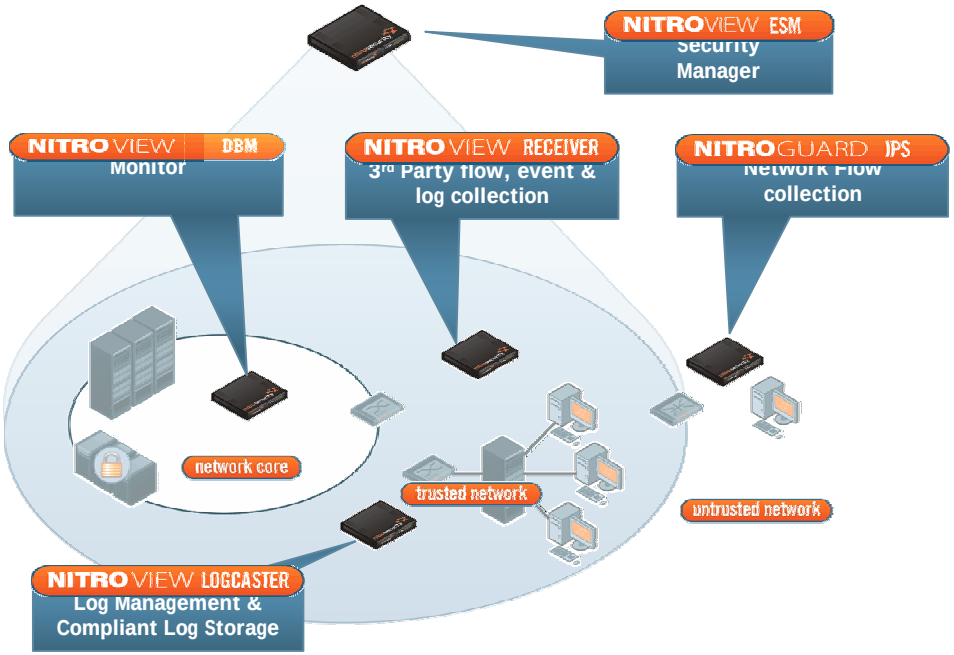
Incorporating Database Security into the SOC/NOC

Suncoast Oracle Users Group
FL - 8/27/2009

Agenda

- DB Security Primer
- Integrated DB Security
- DAM Features / Demo

NITROVIEW



Database Security Primer

Data Discovery

Classify sensitive data

Vulnerability Assessment

Database & host hardening

Leakage Prevention

Enforce use policy
De-identify data for sharing

Data Access Policy

Define roles, rights, realms

Database Monitoring

Audit log
Identify/block attacks

Protecting Data-at-Rest

Encryption
Secure backups

Database Security Challenges

- Technical Challenges
  - Data is constantly in motion
  - Huge volumes of activity to monitor and log
  - Compliance mandates segregation of security duties from DBAs
  - Log full audit-trail of administrator activity
  - Business & DBAs require monitoring without impacting application performance
- Budgetary & Resource Limitations
  - Databases (imp nevertheless) are only a component of overall security
  - Staffing (need someone other than the DBA) – can it be the SOC/NOC?
- SOC/NOC perception of databases & apps - it's a different beast
  - Hard to deploy & manage
  - Events not easily understood by SOC/NOC teams

Top Database Security Threats

- Excessive Privilege Abuse
- Legitimate Privilege Escalation
- Privilege Elevation
- Database Platform Vulnerabilities
- SQL Injection
- Weak Audit Trail
- Denial of Service
- Database Communication Protocol
- Weak Authentication
- Backup Data Exposure

Primary Use Cases

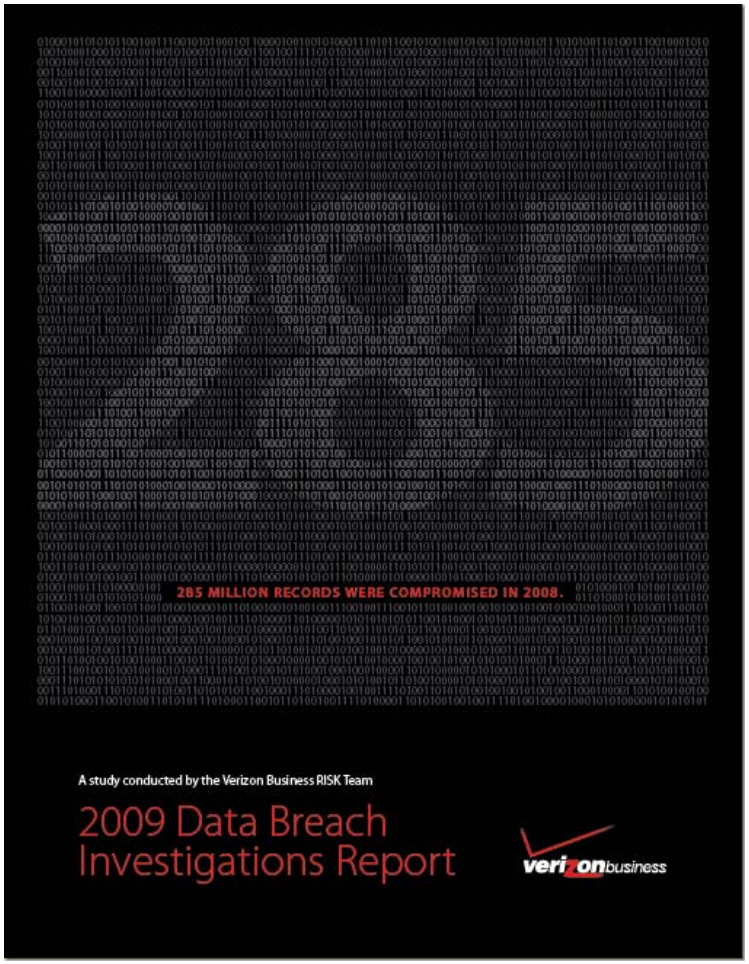
Privileged user monitoring

Fraud detection & monitoring

Database protection

Source GNC Computer News

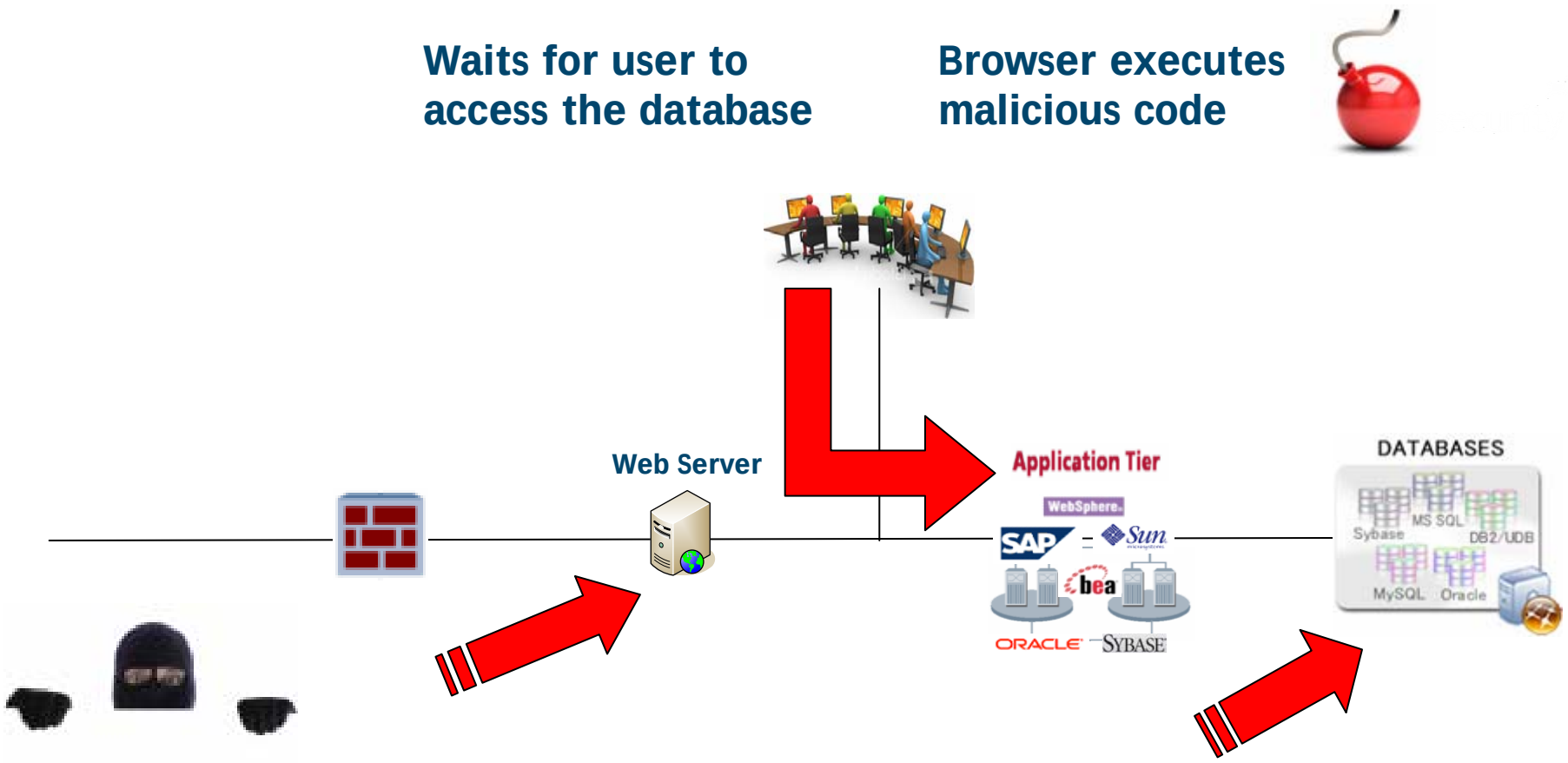
Verizon Data Breach Investigations Report



- Most widely used attack path
  - Web application, 79%
- Most widely compromised asset by number of records
  - Database server, 75%
- Most compromised data type
  - Payment card data, 98%
- Type of assets misused
  - Database Server, 23%

- Encryption provides limited effectiveness
- Auditing DDL != Security

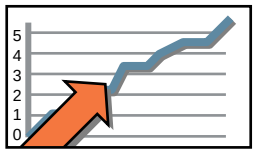
Attack Scenario - Many Ways to Skin a Cat



Role of the SOC & NOC

NOC

Optimize repeatable tasks



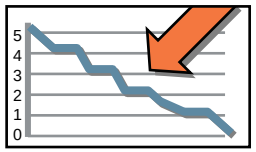
- Availability
- Performance
- Capacity

Common collection and reporting

Different event analytics

SOC

Discover and investigate "abnormal" activity



- User
- Payload
- Behavior

- 24/7 network security monitoring (SIEM integration)
- Use SIEM for change detection

Controlled by IT Security:

- Privileged user monitoring
- Security incident management

Workflow integration

Source Gartner

Role of a DBA in Preventing Breaches

- Ensure essential controls are met
- Find, track, and assess data
- Collect and monitor logs
- Audit user accounts and credentials
- Test and review web applications

Rise of the Application Security Officer (ASO)

ASO's Role: Bridge between SOC/NOC and Application Teams

Application Aware Baseline Example – Theft of User Credentials

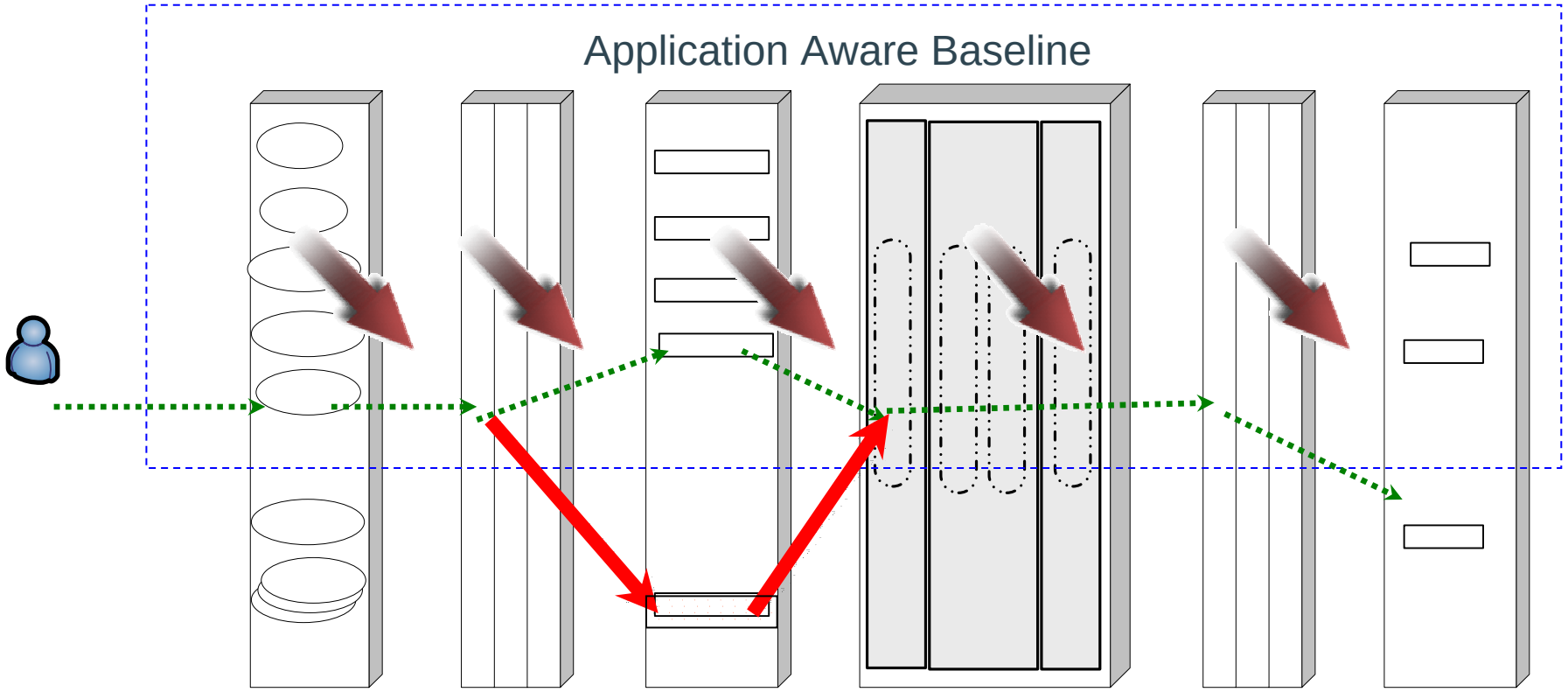
Violation Check

- User → Environment: ✓
- User → Terminal: ✗
- User → Operation: ✓
- Operation → Environment: ✓
- User → Object: NO CHECK

Sample Result

ACTION value:
env_u_NOVIOL-term_ISVIOL-op_
NOVIOL-env_op-NOVIOL-obj-NOCHK

VIOLATION value: ISVIOL ✗



Pitfalls with Native Database Audit Controls

- Performance Impact
- Information in native logs is inferior
- Cannot correlate series of events for root cause analysis
- Cannot discover and prevent database attacks
- Cannot monitor content – who accessed sensitive data?
- Cannot track a person using a generic database login or application
- Cannot mask sensitive content
- Software only solutions (harder to deploy & manage)
- No integration with SIEM, Log Mgmt, Alerting, Enterprise solutions
- No secure central logging, reporting and notification
- Hard to segregate database security duties from the DBA

Monitoring Technologies

- Requires SIEM, DAM, DLP, Application Monitoring, etc.
- Increased cost from multiple technologies
- Reduced productivity from multiple consoles

Source Gartner

	SIEM	DAM	DLP	Fraud Detection
Application activity	◔	◔	○	●
Application access	◑	◔	◔	●
Database activity	◑	●	◔	◔
File access	◑	◔	●	◔
DB activity: privileged user	◑	●	○	○
System activity: privileged user	●	◔	○	○
Network activity: user	◑	◔	◔	◔

○ User activity at this layer is not visible

◑ User activity at this layer is visible in a broad set of use cases, but other technologies provide deeper monitoring.

● This technology is a primary monitoring method for this layer.

◔ User activity at this layer is visible, but monitoring is limited to the primary use cases of the technology.

Security Solution Technologies: Deployment Phases

SOX, PCI, HIPAA, Breach Disclosure Laws

- Phase I – VA, Antivirus, Firewall, IPS/IDS, Access Control
- Phase II – SIEM Deployment (Network Perimeter & Host)
- Phase III – Monitor Databases & Applications
- Phase IV – Prevent Leakage of Sensitive Data (DLP)

Integrated Database & Application Security

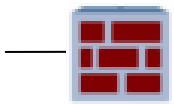
SOC/NOC
Compliance
DBA's
Management

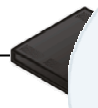
Incidence response
VA integration
User activity profiling
Event correlation
Central policy & mngt
Analysis/forensics
Reporting, alerting

Monitor all OS security events - users logging in/out, access/change to database config files & backups

Block database exploits and SQL Injection attacks before they reach the network core

NitroView Receivers





NitroG

DBM agent

NitroView APM

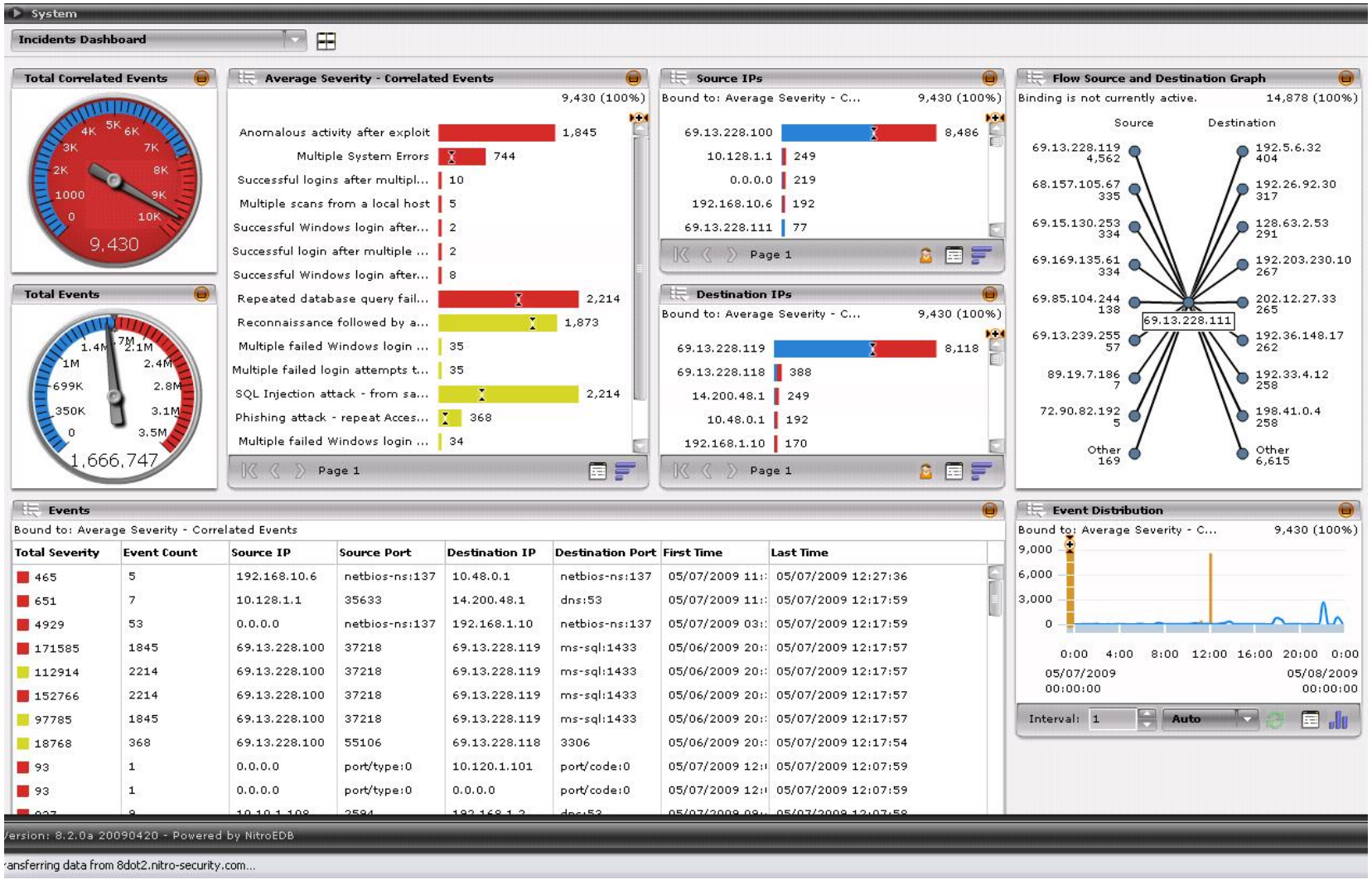
Monitor potential leakage of sensitive database content via email, chat, web, P2P

Full-session capture of **SQL** activity, db content use, db server discovery

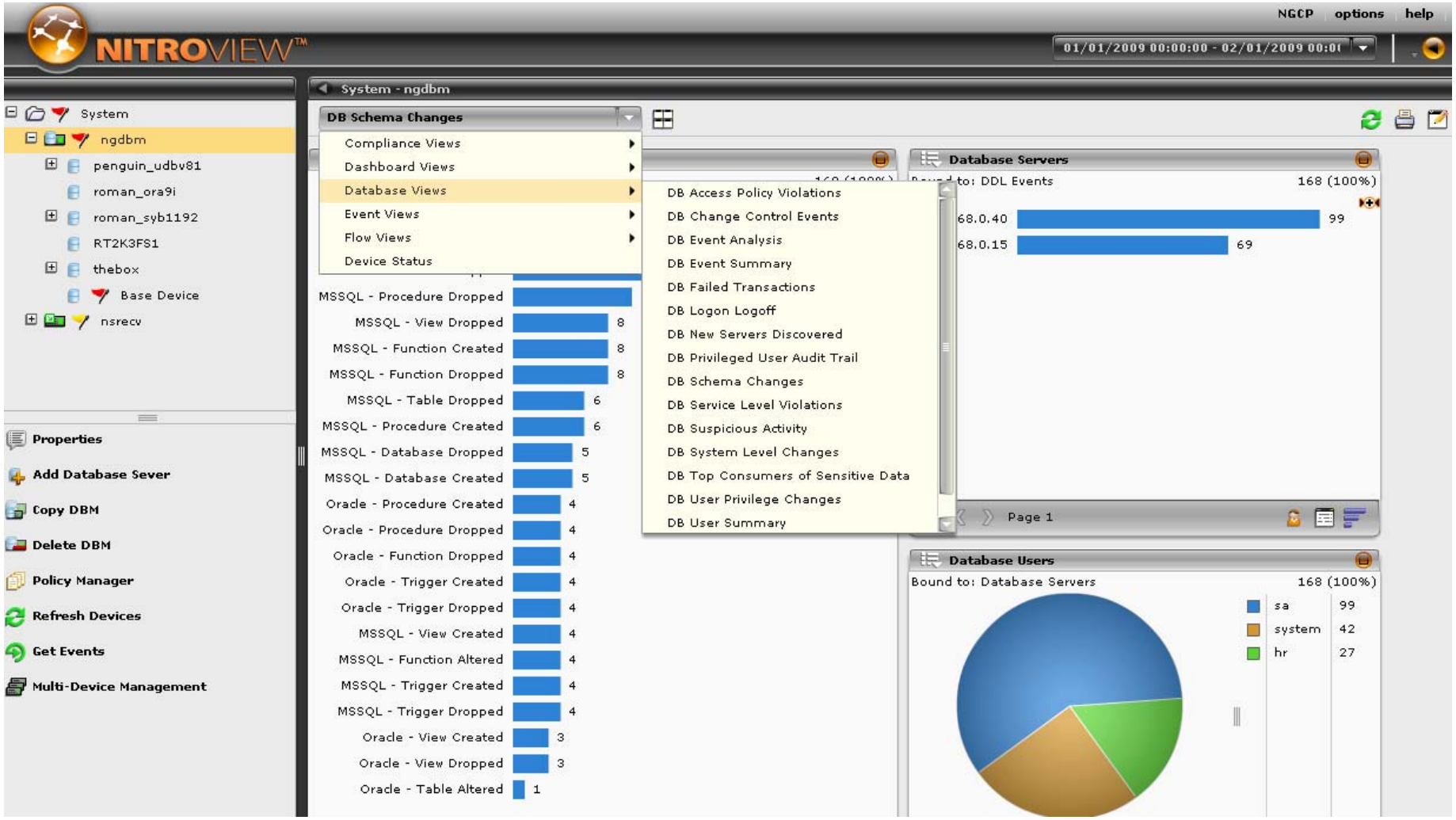
Log DBA console activity

Database Activity & Event Correlation

- Advanced Visualization, Activity Baselining, Event Analysis & Drill-down

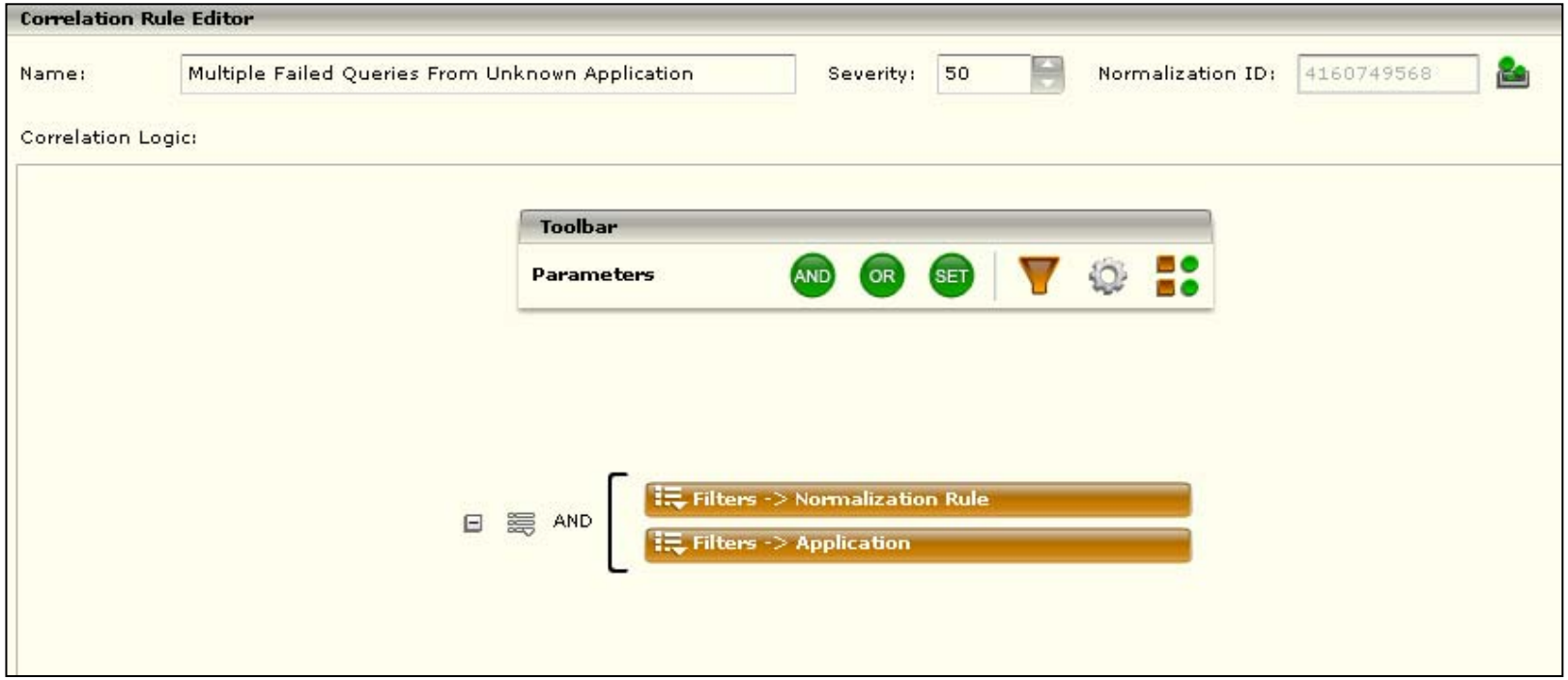


Pre-defined Database Views and Graphical Reports

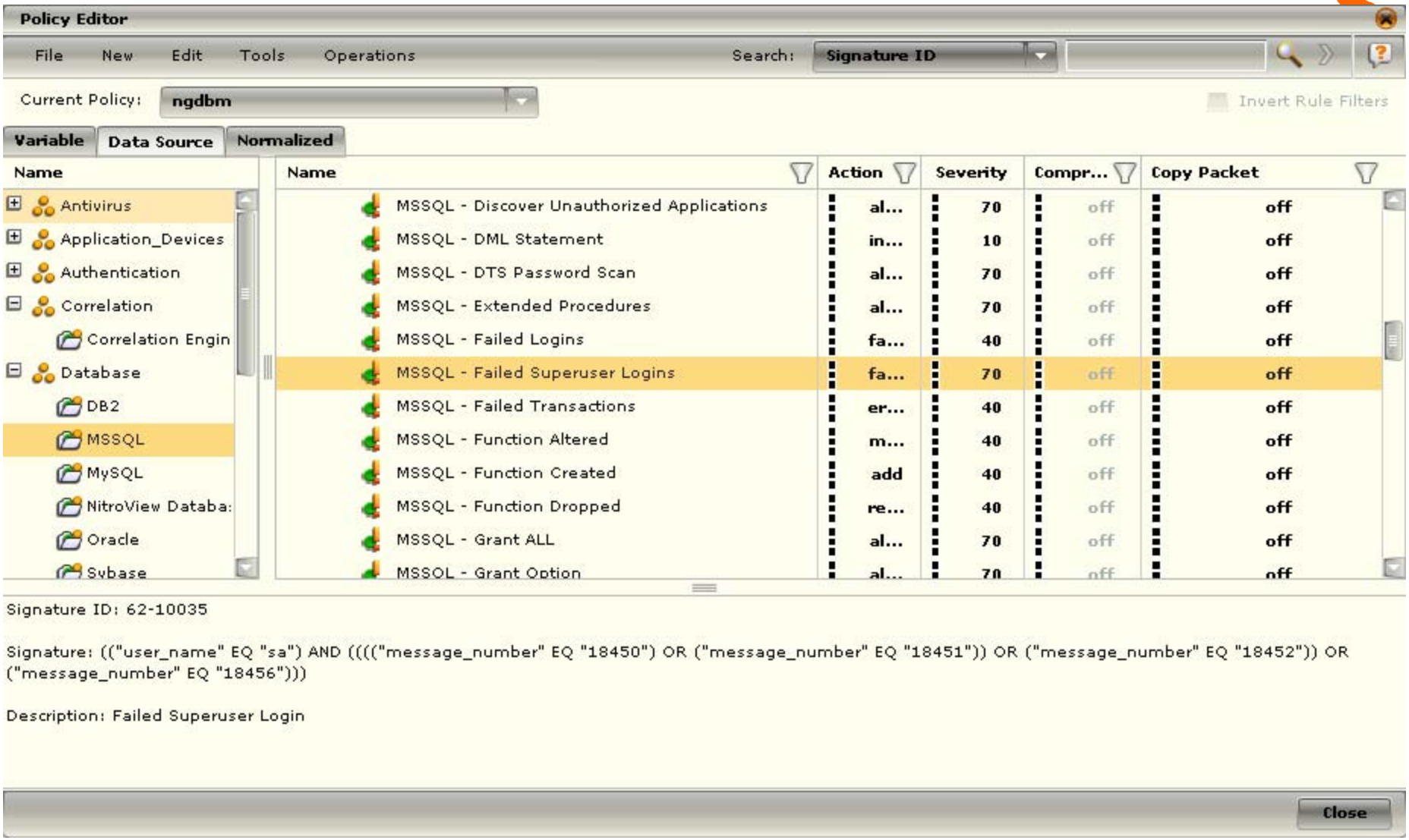


Correlation Rule Editor

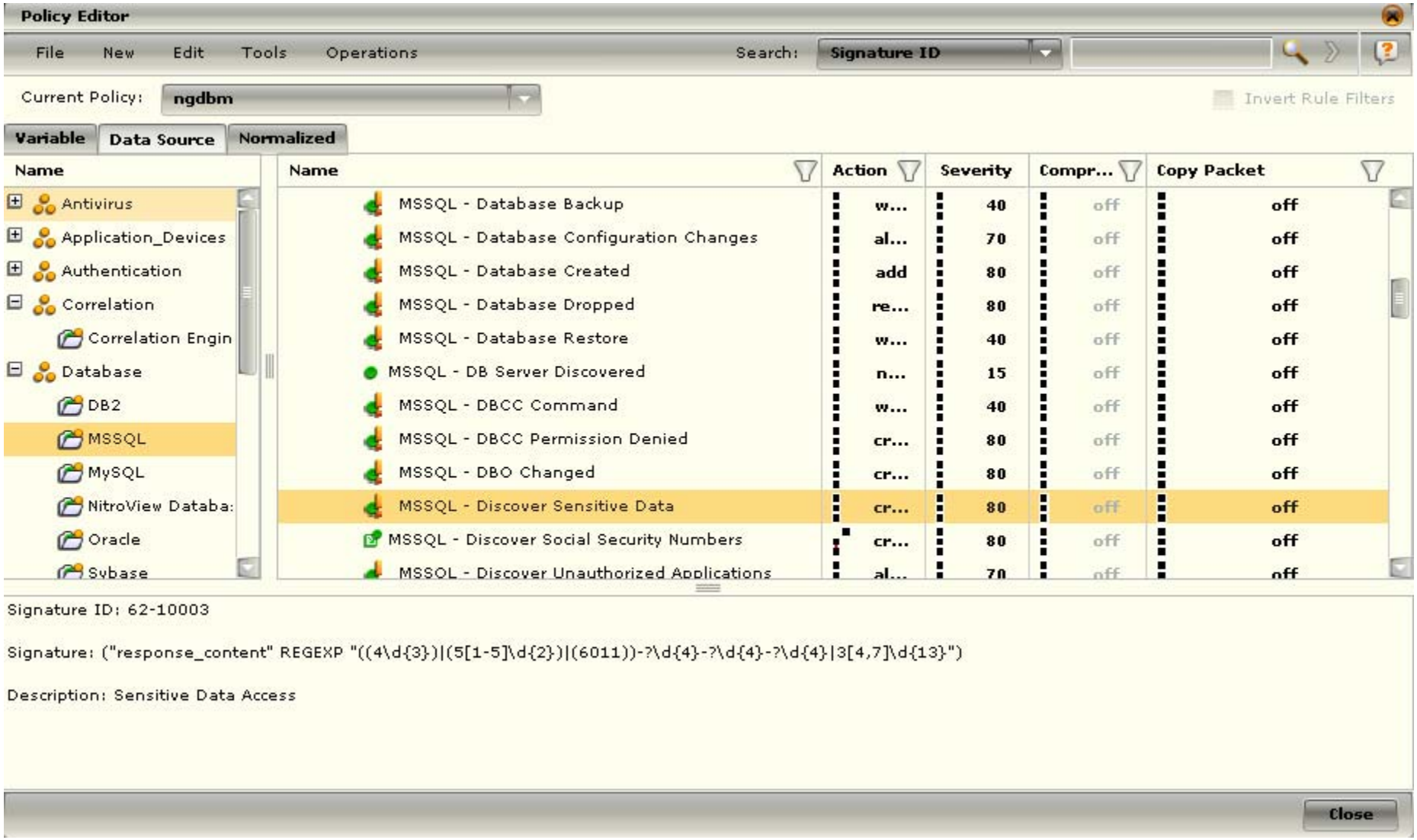
- Correlation with security events, flows, application logs, identity & VA tools
- Over 150 devices support out-of-box



Central Policy Management & Rollout

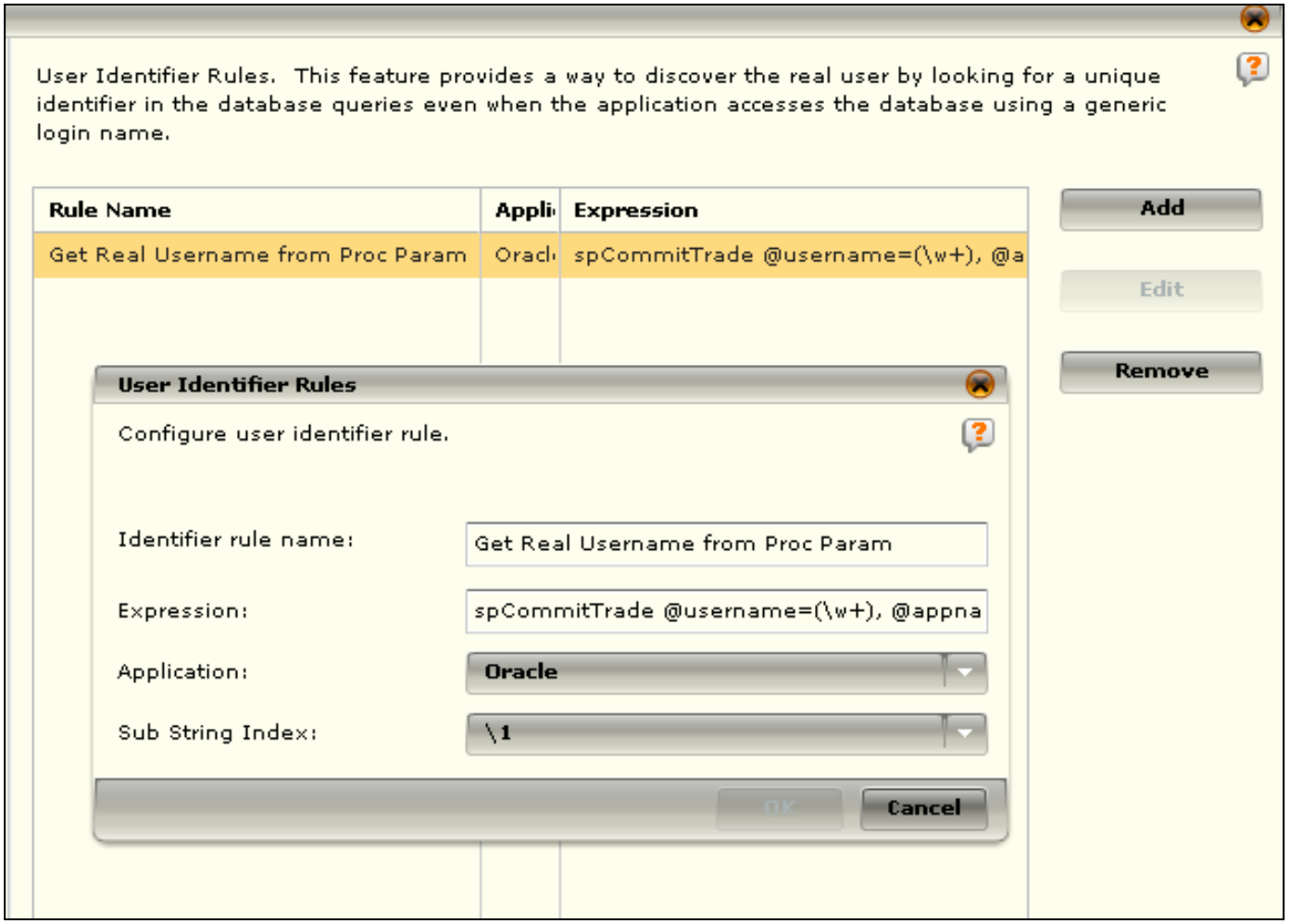


Discovery of Sensitive Content



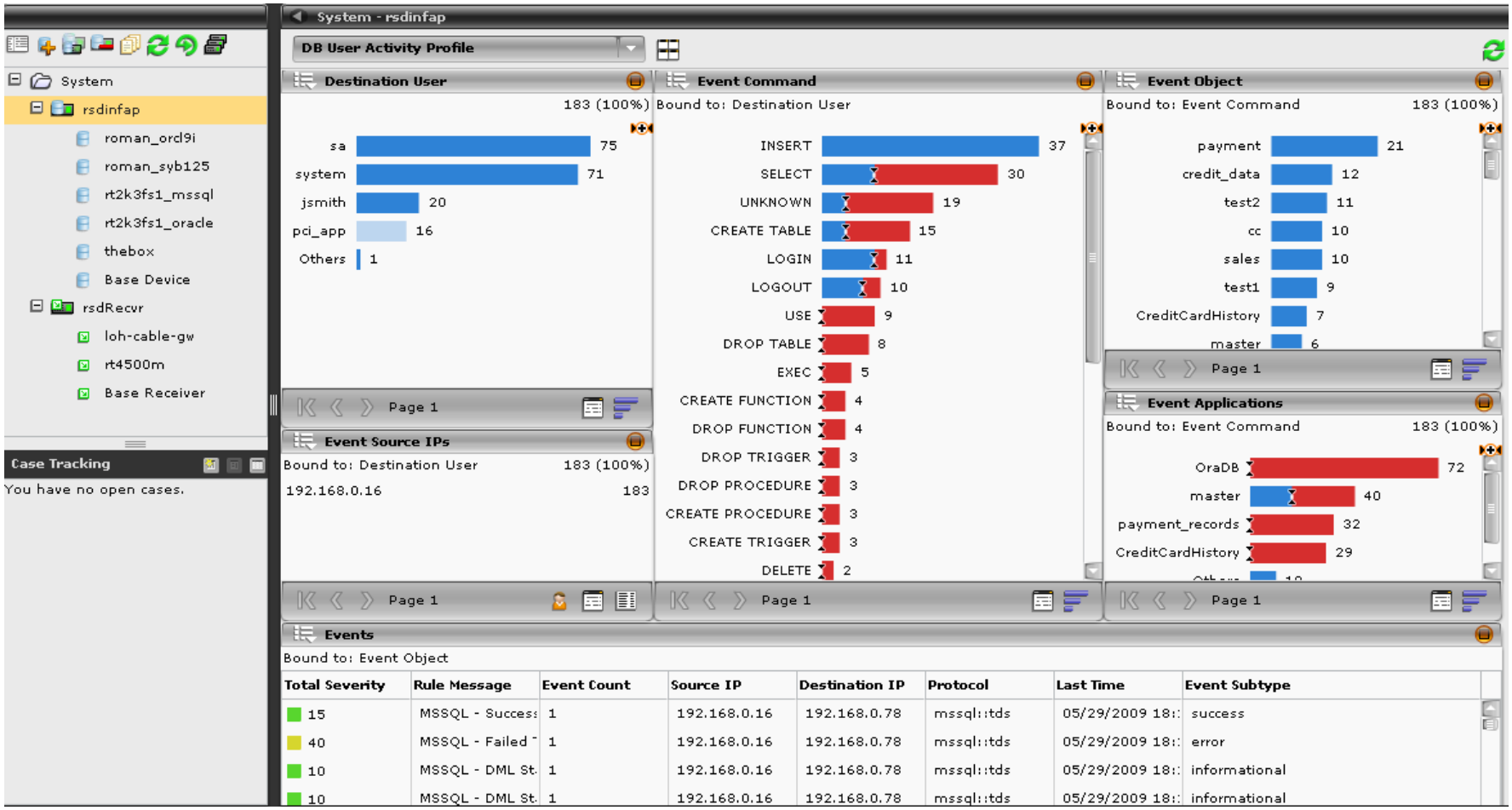
Application User Tracking

- Correlating the SQL transaction with another data source
- Identifying a user-identifier/token in the SQL

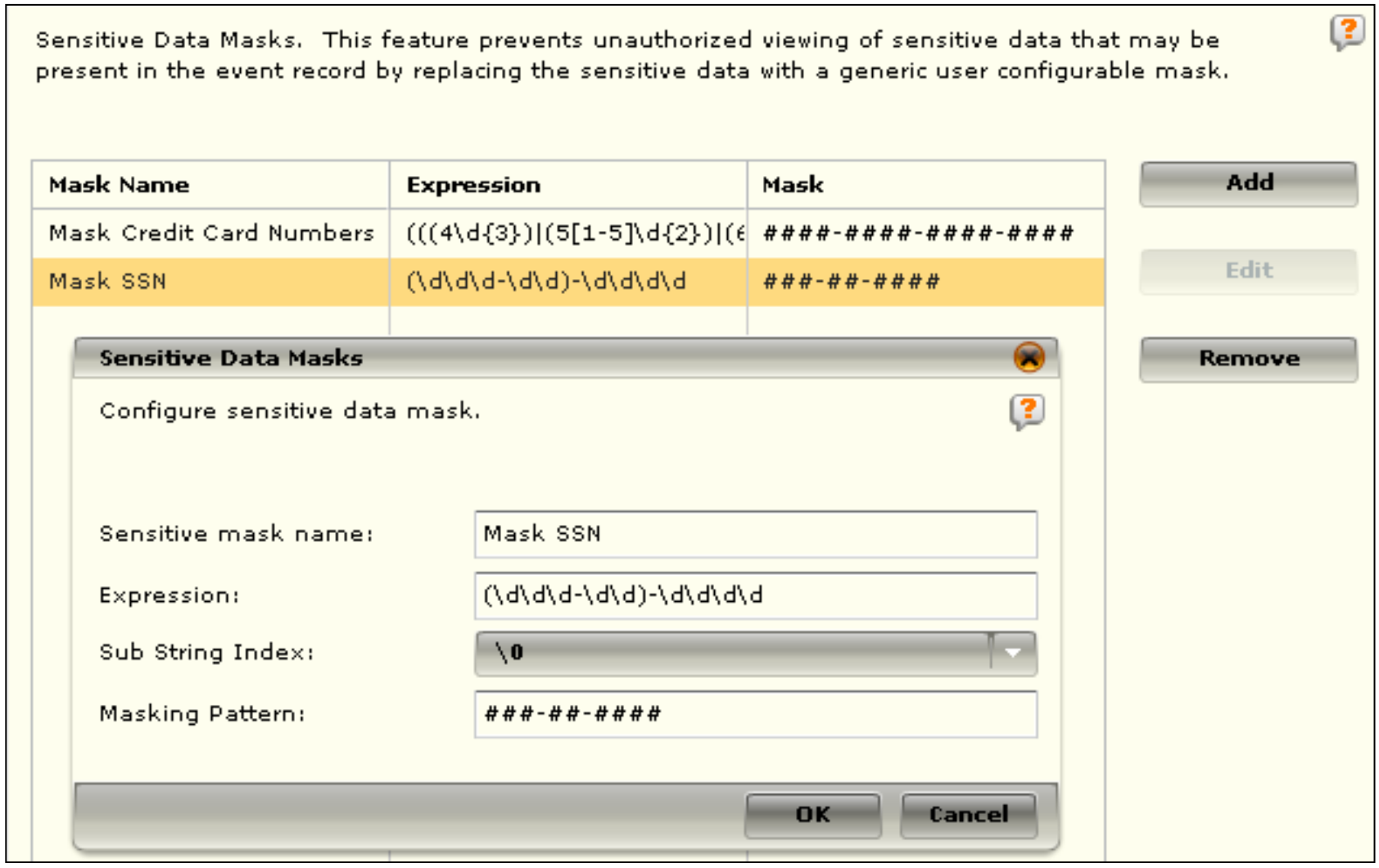


User Activity Profiling

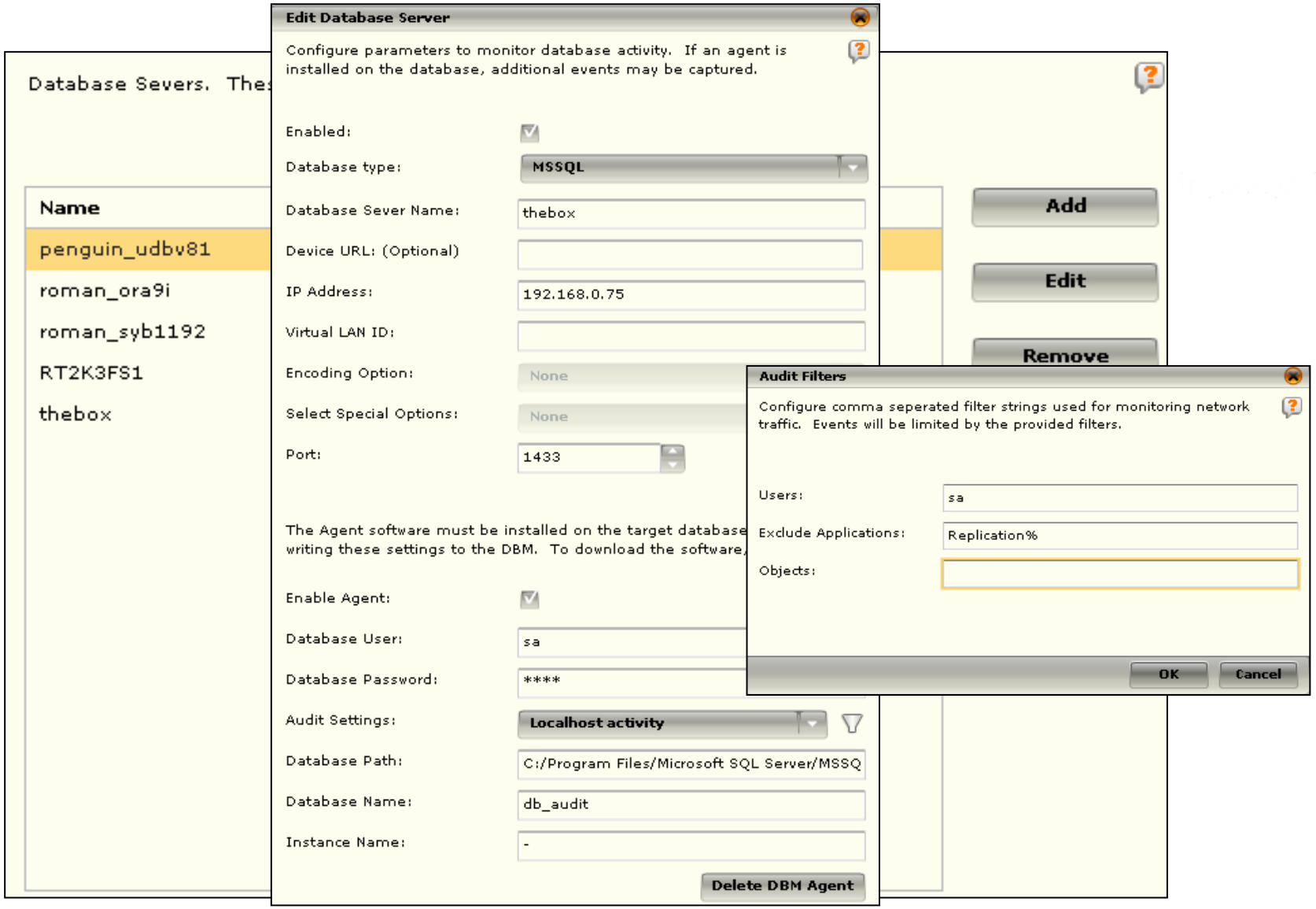
- Commands and objects are accessed by a user and deviation from normal behavior



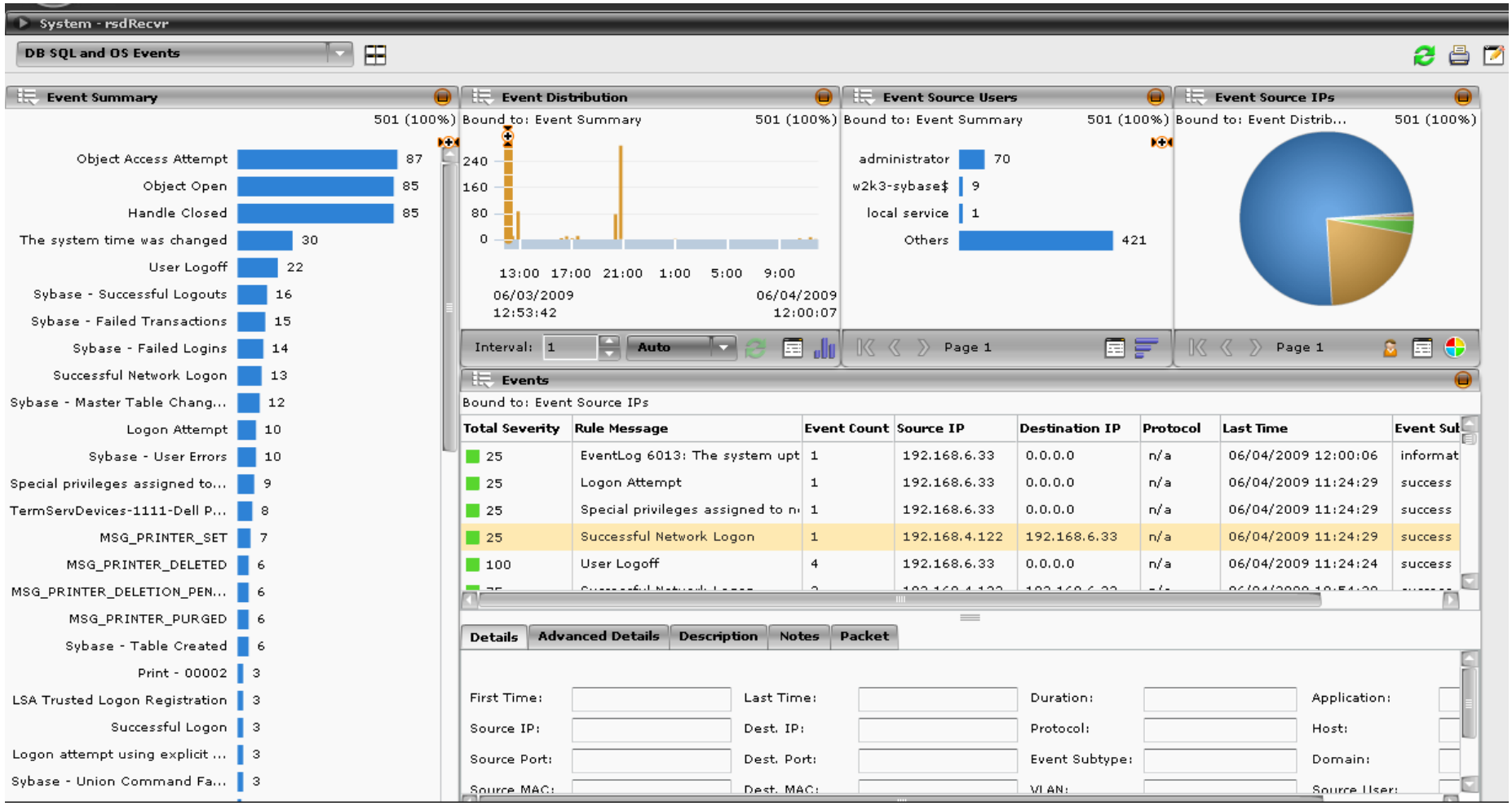
Sensitive Data Masking



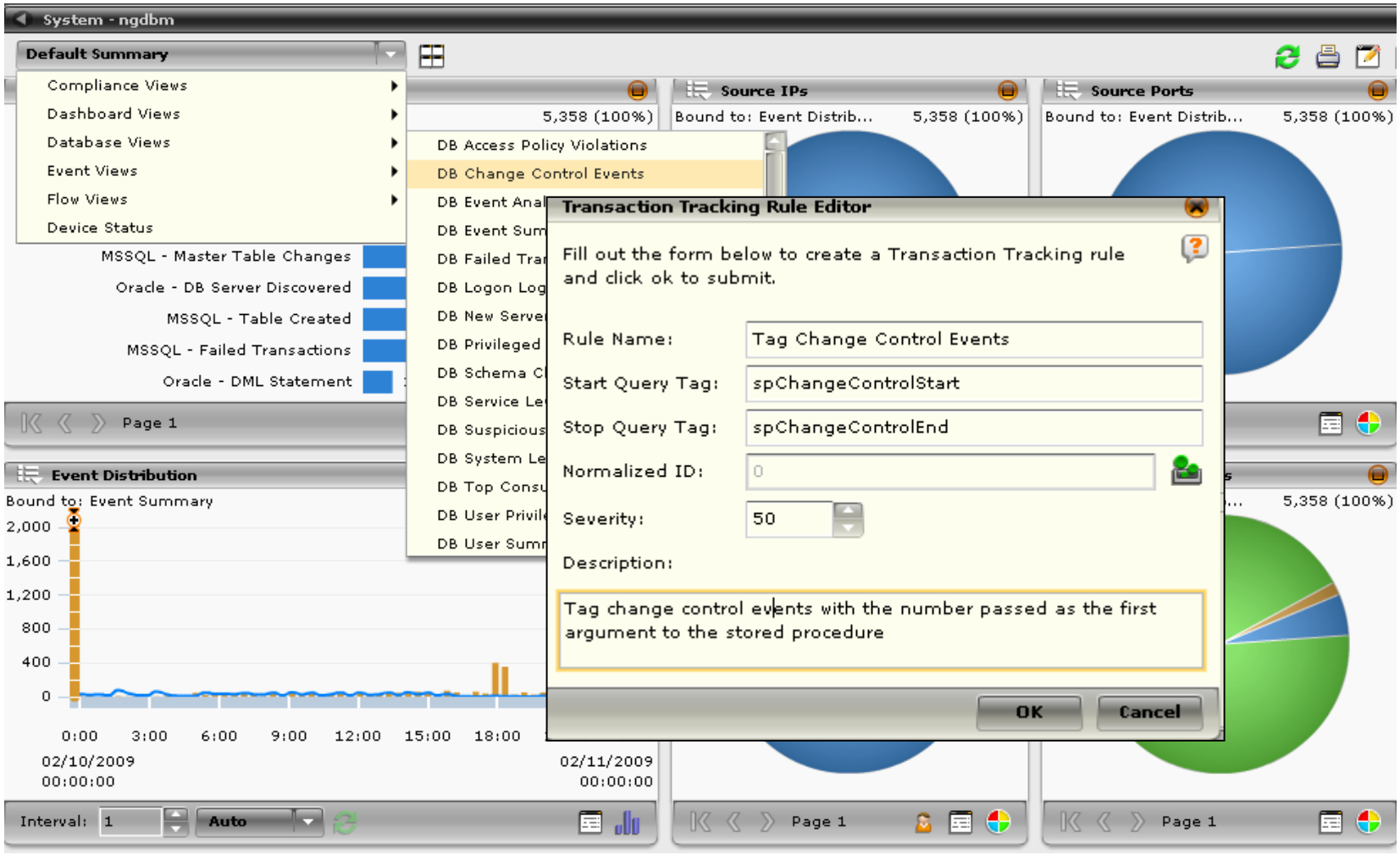
Integrated Agent Management



Monitoring of Database Config & Backup Files

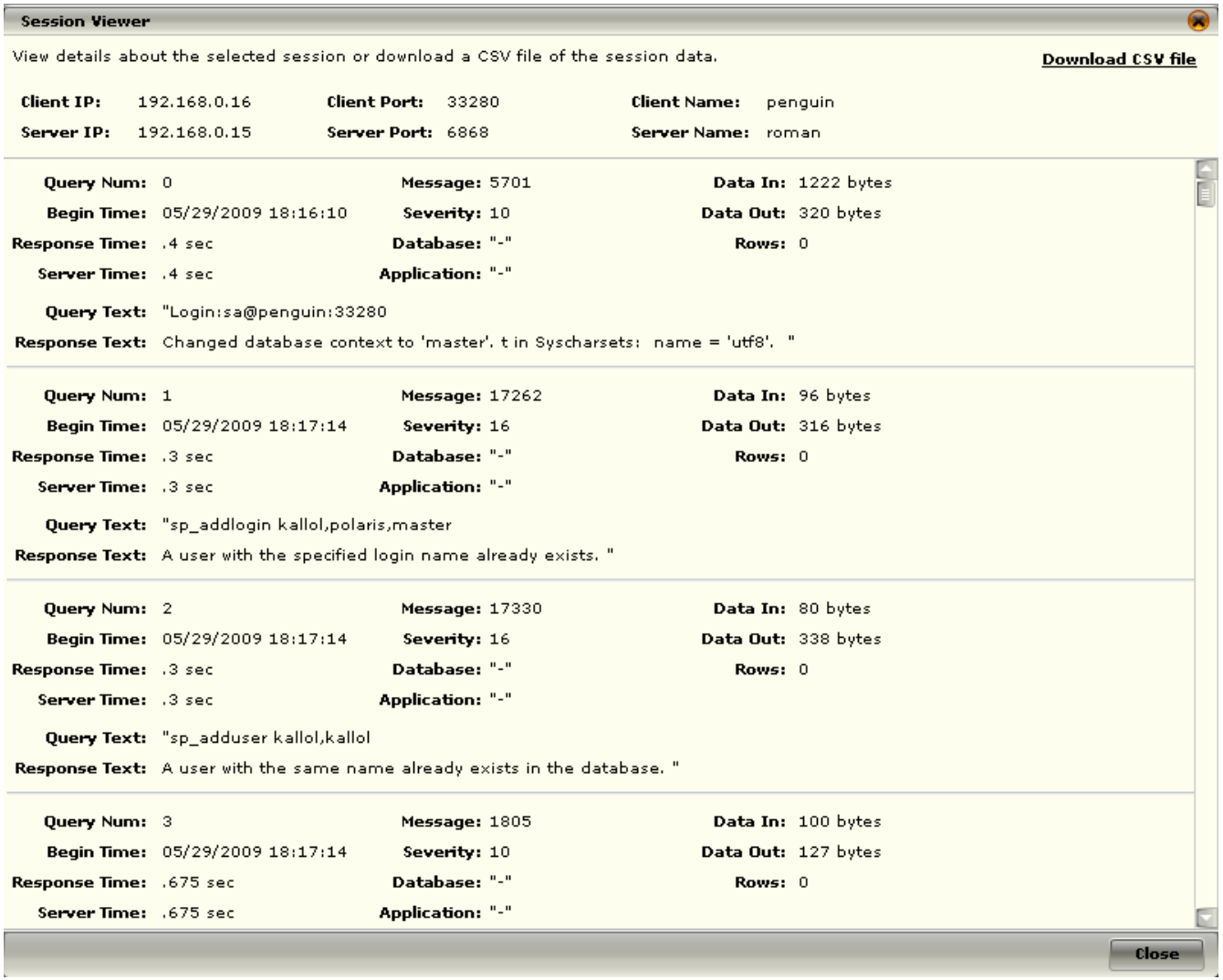


Database Change Control Management



Full Session Detail

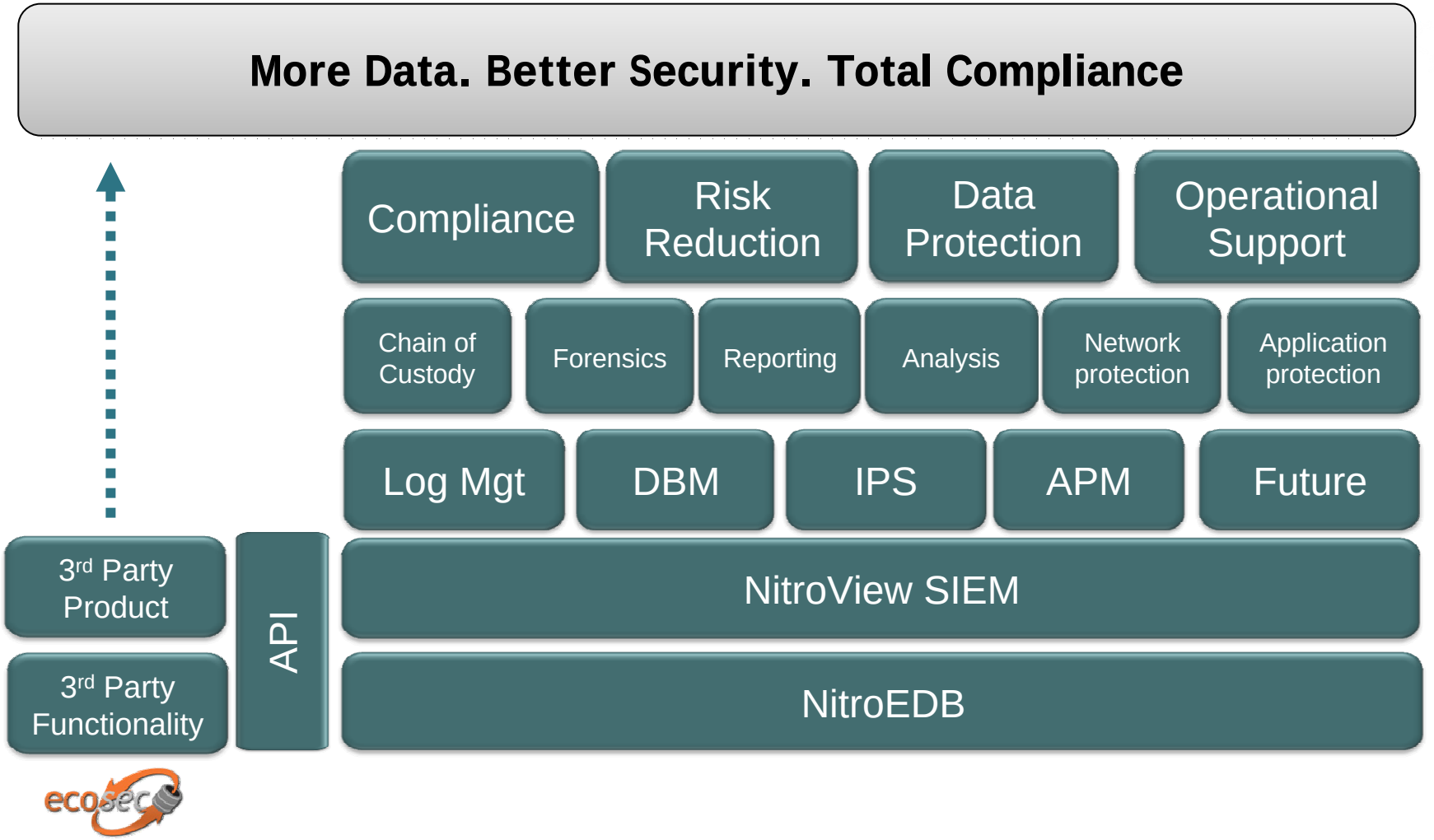
- Drill-down from an event to full session detail



Full Session Detail

sec_flag	begin_time	end_time	response_time	server_response_time		begin_time_skew	client_ip	server_ip	
	client_port	server_port	query_number	query_exit_status		data_in	data_out	packets_in	
	packets_out	network_time	client_name	user_name	application_name		server_name	nt_client_Name	
	nt_user_Name	nt_domain_Name	query_type	error_code	error_severity	error_message	client_pid	return_rows	
	query_text	database_name	spid						
2	9/6/2005 12:17	9/6/2005 12:17	0.008	0.004	5	192.168.1.5	192.168.1.100	55870	
	1433	0	0	615	168	3	2	0.004	
	roman	sa	TSQL	192.168.1.100	-	-	-	2	0
	0	-	14131	0	Login:sa@roman:55870		master	51	
2	9/6/2005 12:17	9/6/2005 12:17	0.003	0.001	5	192.168.1.5	192.168.1.100	55870	
	1433	1	4096	50	193	2	2	0.002	
	roman	sa	TSQL	192.168.1.100	-	-	-	1	0
	0	-	14131	0	USE Northwind	Northwind	51		
2	9/6/2005 12:17	9/6/2005 12:17	0.002	0.002	5	192.168.1.5	192.168.1.100	55870	
	1433	4	4096	50	17	1	1	0.000	
	roman	sa	TSQL	192.168.1.100				1	0
	0	-	14131	0	INSERT INTO test1 values (123,1,'test 1')			Northwind	51
10248	Northwind	51							
2	9/6/2005 12:17	9/6/2005 12:17	0.001	0.001	5	192.168.1.5	192.168.1.100	55870	
	1433	15	4096	65	264	1	1	0.000	
	roman	sa	TSQL	192.168.1.100	-	-	-	1	
	587333632	16	Error::DELETE statement conflicted with COLUMN REFERENCE constraint 'FK_Order_Details_Orders'.						
The conflict occurred in database 'Northwind', table 'Order Details', column 'OrderID'.					CROW	14131	0	DELETE FROM	
Orders WHERE OrderId IN ('11072', '11076')			Northwind	51					
2	9/6/2005 12:17	9/6/2005 12:17	0.000	0.000	5	192.168.1.5	192.168.1.100	55870	
	1433	16	0	0	0	0	0	0.000	
	roman	sa	TSQL	192.168.1.100	-	-	-	0	0
	0	-	14131	0	Logout:sa@roman:55870		Northwind	51	

Web API


More Data. Better Security. Total Compliance
Compliance
Risk Reduction
Data Protection
Operational Support
Chain of Custody
Forensics
Reporting
Analysis
Network protection
Application protection
Log Mgt
DBM
IPS
APM
Future
3rd Party Product
3rd Party Functionality
API
NitroView SIEM
NitroEDB
ecosec

Auto Discovery of Databases & Easy 1-Step Setup

- Database Discovery
- Setup & Configuration
  - Add DBM Device, Add Database Servers, Add Optional Database Agents