Datacenter Security Automation
Modern Datacenter – An intelligent infrastructure

- Improve performance and efficiencies
- Respond to changes
- Manage security, privacy, and compliance
Modern datacenter security components

- Privileged User Management
- Next Generation Security mechanism
- Threat Intelligence
- Security, privacy and compliance
Privileged User Management
Privileged Accounts
Everywhere In the Enterprise

- Servers & Workstations
  - Every hardware platform
  - Every operating system

- Datacenter Appliances
  - Routers and switches
  - Application accelerators
  - Security appliances

- Applications
  - Line-of-business
  - Web services
  - Database and middleware
  - Backup services
  - Identity and access management
  - Systems management
Privileged Accounts
What Are The Risks?

- Do we know where all of our privileged accounts are?
- Do the wrong people have access to sensitive data?
- Who is sharing credentials? Who is accountable?
- Are inconsistent & invisible access policies inviting abuse?
- Will our passwords fail to withstand dictionary and social attacks?
- Where are developer “back doors”?
- Does lack of automation make it impractical to comply with policies?
- Are manual processes wasting resources & leaving security holes?
- Will manual account changes lead to application failure & downtime?
- Are privileged accounts being used for tasks that don’t require them?
- If one IT asset is compromised, will others be exploited as a result?
- Will we fail our next IT audit?
1. **Identify** and document critical IT assets, their privileged accounts and interdependencies.

2. **Delegate** so that only appropriate personnel can access privileged accounts in a timely manner, using the least privilege required, with documented purpose, during designated times.

3. **Enforce** rules for password strength, uniqueness and change frequency, synchronizing changes across dependencies.

4. **Audit** and alert so that the requesters, purpose and requested duration are documented and management is made aware of unusual access and other events.
Customer Value

Executive Management (CISO / CIO)
- Protect corporate assets
- Comply with regulatory requirements
- Improve corporate agility against new security threats

IT Director
- Increase operational efficiency
- Prove that policies and IT processes are aligned
- Reduce the risk of planned changes and unplanned events

Administrator
- Automate tedious, error-prone tasks
- Mitigate security threats in a changing environment
- Eliminate security monitoring and compliance uncertainty
User Activity Monitoring
69% of reported breaches involve a trusted user.

76% of data breaches involve accounts with access to sensitive data.

Source: Data Breach Investigations Report Verizon
Do you know Your Risky Users?

- **Business Users**: 84% of Insider based breaches involve users with no admin rights.
- **IT Users**: 62% of admin-caused breaches due to human error.
- **Contractors**:
Find out Who’s Doing what?

Identify and Manage User-based Risks
Monitor all user activity
Real-time and historical reporting
User behavior analysis and alerting
Integrates with SIEM & IAM
USER RISK MITIGATION

Monitoring, Detection & Rapid Incident Response

**Analyze**
Monitor and baseline user activity

**Detect**
Instantly detect changes in actual user behavior that warrant investigation

**Respond**
Isolate users, systems and data in real-time and historically with detailed forensic data
Database Security
The Security Landscape is changing rapidly

Data Explosion  Consumerization of IT  Everything is Everywhere  Attack Sophistication

Extending the perimeter; focus shifts to protecting the DATA

Moving from traditional perimeter-based security...
Data is the key **target** for security breaches.....

... & Database Servers Are The Primary Source of Breached Data

### Table 10. Compromised assets by percent of breaches and percent of records*

<table>
<thead>
<tr>
<th>Type</th>
<th>Category</th>
<th>All Orgs</th>
<th>Larger Orgs</th>
</tr>
</thead>
<tbody>
<tr>
<td>POS server (store controller)</td>
<td>Servers</td>
<td>50%</td>
<td>1%</td>
</tr>
<tr>
<td>POS terminal</td>
<td>User devices</td>
<td>35%</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>Desktop/Workstation</td>
<td>User devices</td>
<td>18%</td>
<td>34%</td>
</tr>
<tr>
<td>Automated Teller Machine (ATM)</td>
<td>User devices</td>
<td>8%</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>Web/application server</td>
<td>Servers</td>
<td>6%</td>
<td>80%</td>
</tr>
<tr>
<td>Database server</td>
<td>Servers</td>
<td>6%</td>
<td>96%</td>
</tr>
<tr>
<td>Regular employee/end-user</td>
<td>People</td>
<td>3%</td>
<td>1%</td>
</tr>
<tr>
<td>Mail server</td>
<td>Servers</td>
<td>3%</td>
<td>2%</td>
</tr>
<tr>
<td>Payment card (credit, debit, etc.)</td>
<td>Offline data</td>
<td>3%</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>Cashier/Teller/Waiter</td>
<td>People</td>
<td>2%</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>Pay at the Pump terminal</td>
<td>User devices</td>
<td>2%</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>File server</td>
<td>Servers</td>
<td>1%</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>Laptop/Netbook</td>
<td>User devices</td>
<td>1%</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>Remote access server</td>
<td>Servers</td>
<td>1%</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>Call Center Staff</td>
<td>People</td>
<td>1%</td>
<td>&lt;1%</td>
</tr>
</tbody>
</table>

*Database servers contain your client’s most valuable information:
- Financial records
- Customer information
- Credit card and other account records
- Personally identifiable information
- Patient records

- High volumes of structured data
- Easy to access
Continuous monitor access to sensitive **DATA** including databases, data warehouses, big data environments and file shares to...

1. **Prevent data breaches**
   - Prevent disclosure or leakages of sensitive data

2. **Ensure the integrity of sensitive data**
   - Prevent unauthorized changes to data, database structures, configuration files and logs

3. **Reduce cost of compliance**
   - Automate and centralize controls
   - Simplify the audit review processes

4. **Protect Data in an efficient, scalable, and cost effective way**

**Increase operational efficiency**
- Automate & centralize internal controls
- Across heterogeneous & distributed environments
- Identify and help resolve performance issues & application errors
- Highly-scalable platform, proven in most demanding data center environments worldwide

**No degradation of infrastructure or business processes**
- Non-invasive architecture
- No changes required to applications or databases
Data Security Solution

Data at Rest
- Discovery Classification
- Masking Encryption

Configuration
- Vulnerability Assessment
- Entitlements Reporting

Data in Motion
- Activity Monitoring
- Blocking Quarantine
- Dynamic Data Masking

Discover
- Where is the sensitive data?
- How to secure the repository?
- How to protect sensitive data?

Harden
- Who should have access?
- What is actually happening?

Monitor
- Compliance Reporting
- Security Alerts / Enforcement

Protect
- How to protect unauthorized activities?
- How to prevent unauthorized activities?
- How to protect sensitive data to reduce risk?
Data Security solutions protect structured and unstructured sensitive data

Discover
- DB and Data Discovery
- Data Classification
- Enterprise Integrator
- Entitlement Reporting
- Queries & Reports
- Threshold Alerts
- Compliance Workflow
- Group Management
- Security Integrations
- IT Integrations
- Data Level Security
- Incident Management
- User/Roles Management
- HR Integrations
- Portal Management
- Self Monitoring
- Data Export Options
- Data Imports Options

Harden
- Assessment reports
- Data Protection Subscription
- Configuration Changes

Monitor
- Data Activity Monitoring
- Real-time alerts
- App end-user identification
- Normalized audit creation
- Compliance reporting
- Compliance workflow
- Federate large deployment
- Central control
- Central audit collection

Protect
- Blocking access
- Masking sensitive data
- Users Quarantine

Advanced DAM
- Blocking access
- Masking sensitive data
- Users Quarantine

Data Redaction
- Redact sensitive documents

Masking for Applications
- Masking on the browser

"Base Product"
- Discovery Classification
- Masking Encryption
- Vulnerability Assessment
- Entitlement Reporting
- Activity Monitoring
- Blocking Quarantine

Vulnerability Assessment
- File-level encryption
- Role-based access control
- File access auditing

Data Encryption
- Static Data Masking
- Static masking
- Semantic and format preserving
Application Security
Securing Applications is a Challenge

Your Application Portfolio
Different Types & Sources
- Financial
- HR
- Logistics
- Intranet
- Outsource
- In-house
- Legacy
- Open Src

Your Policies
- Data Privacy
- Regulatory Compliance
- Accountability

Your SDLC Processes
- Large and diverse application portfolios
- Mobile applications
- In-house and outsource development
- External & internal regulatory pressure
- Pockets of security expertise
- Yet another task for developers

Need an efficient, scalable, automated way to develop and deliver secure applications...
Threat Intelligence & Analysis

Provides Specific Analysis of:

- Vulnerabilities and exploits
- Malicious/Unwanted websites
- Spam and phishing
- Malware
- Other emerging trends

Most comprehensive vulnerability database in the world

- Entries date back to the 1990's
Build security into your application development process

Efficiently and effectively address security defects before deployment

Collaborate effectively between Security and Development

Provide Management visibility

Adopt a **Secure by Design** approach to enable you to design, deliver and manage smarter software and services

Proactively address vulnerabilities early in the development process
App Scan helps finding more vulnerabilities using advanced techniques

**Static Analysis**
- Analyze Source Code
- Use during development
- Uses Taint Analysis / Pattern Matching

**Dynamic Analysis**
- Analyze Live Web Application
- Use during testing
- Uses HTTP tampering

**Run-Time Analysis**
- Combines Dynamic Analysis with run-time agent
- More results, better accuracy

**Hybrid Analysis**
- Correlate Dynamic and Static results
- Assists remediation by identification of line of code

**Client-Side Analysis**
- Analyze downloaded Javascript code which runs in client
- Unique in the industry
Next- Gen Prevention Mechanisms
WHAT’S CHANGED?

THE EVOLUTION OF THE ATTACK

- Mobility threat
- Identity compromise
- Zero-day exploits / vulnerabilities
- Unknown & polymorphic malware
- Evasive command-and-control
- Known threats

Organizational risk
Common traits for breached networks

1. A port based firewall
2. A static IPS
3. Zero Day Malware used to manipulate platforms in the network
4. Identity credentials hijacked
Laterally hop into the data center for initial infection there

ENTER THE DATA CENTER

Laterally hop into the data center for initial infection there

REACH THE TARGET

Lateral Data Center motion for a foothold on the target VM

DELIVER MALWARE

Deliver secondary malware and communicate with attacker

ENDPOINT OPERATIONS

Move laterally and infect additional hosts

STEAL DATA

Steal intellectual property

Prevent attacks by stopping one step in the kill-chain

Understanding the Attack Kill-chain

Attack kill-chain

BREACH PERIMETER

Initial compromise and malware delivery

Initial compromise and malware delivery

DELIVER MALWARE

Deliver secondary malware and communicate with attacker

Prevent attacks by stopping one step in the kill-chain

ENDPOINT OPERATIONS

Move laterally and infect additional hosts

STEAL DATA

Steal intellectual property

Copyright © 2015 - Nanigel Solutions. All Rights Reserved.
REQUIREMENTS FOR THE FUTURE

DETECT AND PREVENT THREATS AT EVERY POINT ACROSS THE ORGANIZATION

- At the mobile device
- At the internet edge
- Between employees and devices within the LAN
- At the data center edge, and between VM’s
- Within private, public and hybrid clouds
Requirements for Security in today's Threat Landscape

1. **Application** based security rules
   – Including the ability to decrypt flows
2. Rules based on **User Identity/User Groups**
3. **Sandbox Technology** to detect unknown malware
4. **Threat** Prevention updates to enable dynamic prevention signatures for malware
5. **URL Technology** to enable dynamic prevention of malware Command & Control
Security Information & Event Management
What were the major risks and vulnerabilities?

Are we configured to protect against advanced threats?

What security incidents are happening right now?

What was the impact to the organization?

Security Intelligence
The actionable information derived from the analysis of security-relevant data available to an organization

Vulnerability
Pre-Exploit
Exploit
Post-Exploit
Remediation

**PREDICTION / PREVENTION PHASE**
- Gain visibility over the organization’s security posture and identity security gaps
- Detect deviations from the norm that indicate early warnings of APTs
- Prioritize vulnerabilities to optimize remediation processes and close critical exposures before exploit

**REACTION / REMEDIATION PHASE**
- Automatically detect threats with prioritized workflow to quickly analyze impact
- Gather full situational awareness through advanced security analytics
- Perform forensic investigation reducing time to find root-cause; use results to drive faster remediation
Providing actionable intelligence

**INTELLIGENT**
Correlation, analysis and massive data reduction

**AUTOMATED**
Driving simplicity and accelerating time-to-value

**INTEGRATED**
Unified architecture delivered in a single console
Embedded intelligence offers automated offense identification

Automated Offense Identification
- Unlimited data collection, storage and analysis
- Built in data classification
- Automatic asset, service and user discovery and profiling
- Real-time correlation and threat intelligence
- Activity baselining and anomaly detection
- Detects incidents of the box

Extensive Data Sources
- Security devices
- Servers and mainframes
- Network and virtual activity
- Data activity
- Application activity
- Configuration information
- Vulnerabilities and threats
- Users and identities
- Global threat intelligence
Extend clarity around incidents with in-depth forensics data

**Automated Offense Identification**
- Unlimited data collection, storage and analysis
- Built in data classification
- Automatic asset, service and user discovery and profiling
- Real-time correlation and threat intelligence
- Activity baselining and anomaly detection
- Detects incidents of the box

**Directed Forensics Investigations**
- Rapidly reduce time to resolution through intuitive forensic workflow
- Use intuition more than technical training
- Determine root cause and prevent re-occurrences

**Suspected Incidents**

**Prioritized Incidents**

**Embedded Intelligence**
An integrated, unified architecture in a single appliance
Answering questions to help prevent and remediate attacks

| What was the attack? | Is the attack credible? | How valuable are the targets to the business? | Who was responsible for the attack? | Where are they located? | What was stolen and where is the evidence? | Are any of the assets vulnerable? | How many targeted assets are involved |

<table>
<thead>
<tr>
<th>Offense 909</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Magnitude</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Source IPs</strong></td>
</tr>
<tr>
<td><strong>Destination IPs</strong></td>
</tr>
<tr>
<td><strong>Network(s)</strong></td>
</tr>
<tr>
<td><strong>Assigned to</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Offense Source Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP</strong></td>
</tr>
<tr>
<td><strong>Username</strong></td>
</tr>
<tr>
<td><strong>Host Name</strong></td>
</tr>
<tr>
<td><strong>Asset Name</strong></td>
</tr>
<tr>
<td><strong>Offenses</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Last 5 Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Notes</strong></td>
</tr>
<tr>
<td><strong>Username</strong></td>
</tr>
<tr>
<td><strong>Creation Date</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Forensics Reconstructions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Case</strong></td>
</tr>
<tr>
<td><strong>Collection</strong></td>
</tr>
<tr>
<td><strong>IP</strong></td>
</tr>
<tr>
<td><strong>Start</strong></td>
</tr>
<tr>
<td><strong>End</strong></td>
</tr>
<tr>
<td><strong>Status</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Top 5 Source IPs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Source IP</strong></td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td>10.0.110.221</td>
</tr>
</tbody>
</table>
Immediate discovery of network assets
Proactive vulnerability scans, configuration comparisons, and policy compliance checks

Simplified deployment
Automated configuration of log data sources and asset databases

Automated updates
Stay current with latest threats, vulnerabilities, and protocols

Out-of-the-box rules and reports
Immediate time to value with built-in intelligence
Identify and quickly remediate
Deploy comprehensive security intelligence and incident forensics

Address regulation mandates
Automate data collection and configuration audits

Detect insider fraud
Adopt next-generation SIEM with identity correlation

Consolidate data silos
Collect, correlate and report on data in one integrated solution

Better predict business risks
Engage entire lifecycle of risk management for network and security infrastructures
Consolidation and integration help reduce costs and increase visibility.

An integrated, unified architecture in a single web-based console.

### Traditional SIEM

6 products from 6 vendors are needed

<table>
<thead>
<tr>
<th>Flows</th>
<th>Packets</th>
<th>Vulnerabilities</th>
<th>Configurations</th>
<th>Logs</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARBOR</td>
<td>EMC</td>
<td>QUALYS</td>
<td>algosec</td>
<td>loglogic</td>
<td>ArcSight</td>
</tr>
<tr>
<td>NETWORKS</td>
<td>RSA</td>
<td>REDSEAL</td>
<td>FIREMON</td>
<td>McAfee</td>
<td>RSA</td>
</tr>
<tr>
<td></td>
<td>SOLERA</td>
<td>RAPID7</td>
<td>skybox</td>
<td>splunk</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RIVERBED</td>
<td>TENABLE</td>
<td>tufin</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Security Intelligence Platform**

**Intelligence and Analytics**