Delivered By The Market Leader

**Company Background**
- Founded May 2000
- 2000+ customers
- 500+ employees, offices worldwide
- Acquired by HP Nov 2010

**Analyst Recognition**
- #1 in Market Share – Last three reports
- #1 In-use for both SIEM and Log Management
- SIEM Leader’s Quadrant - SIX years running

**Industry Recognition**

---

www.arcsight.com © 2010 ArcSight Confidential
Delivered By The Market Leader

Source: Gartner (May 2011)
SIEM Market Evolution

Security
- Perimeter
- Network

Compliance
- Reporting
- Forensics

Business Risk
- Fraud
- Theft

Malware
- Hackers

HP ArcSight ESM

Regulations
- Audits

HP ArcSight Logger

Users
- Data
- Transactions

HP ArcSight IdentityView

Perimeter

Network

Business
Problem: Billions Spent on Identity Tools, but Risk Still Grows

Access Governance Issues Remain:
- Shared Account Usage
- Excessive Privilege
- “Zombie” Accounts
- Slow Revocation of Access
- Non-Existent or Unenforced Access Policy

High Risk Users Operate Unwatched:
- Administrators
- Contractors
- DBAs
- Terminated Employees
- Shared Accounts
Solution: Visibility Requires Activity Information

ArcSight IdentityView

- Badge Swipes
- Database Queries
- USB Files Saved
- VPN Logins
- Files Accessed
- Emails Sent
- Screen Prints
- Web Surfing
- Hosted Apps
HP ArcSight IdentityView Value Proposition

**IdentityView Key Features:**
- Correlates user identity across accounts and systems
- Compares user activity to role to detect violations
- Enriches all monitored events with user data for better context

**IdentityView Gives Organizations:**
- High business value use cases for user monitoring
- Lower risk from malicious insiders, shared and privileged accounts, and high risk users
- Increased compliance with IAM best practices

Understand **who** is on your network, **what** data they are seeing, and **which** actions they take with that data
# IdentityView vs. Traditional Identity Management

<table>
<thead>
<tr>
<th>IdentityView</th>
<th>IDM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitors what access rights are actually used</td>
<td>Must be configured with what access rights theoretically should be</td>
</tr>
<tr>
<td>Leverages identity information and activity data that’s already every organization already has</td>
<td>Must be populated with data for each system’s ideal access rights, which must come from business units</td>
</tr>
<tr>
<td>Extends a security monitoring process that already exists</td>
<td>Imposes additional processes on organizations that fall on business users and managers</td>
</tr>
<tr>
<td>Flexibly collects and organizes identity data to provide complete picture of users across all systems</td>
<td>Requires deep integration with each source of identity information</td>
</tr>
</tbody>
</table>
Identity Correlation

- Correlate common identifiers such as email address, badge ID, phone extension
- Events occurring across devices that identify users by different attributes
- Attribute the event to a unique “identity” allowing correlation across any type of device

Identifiers
- rjackson
- 348924323
- jackson@arc.com
- robertj
- rjackson_dba
- 510-555-1212

Identity
- Robert Jackson
Identity Correlation in Practice

With IdentityView, a simple event

1. Correlates an IP with a user
2. Identifies the associated username
3. Enriches the event with user data
User Activity: New Orientation for Security Monitoring

Traditional SIEM

- IP Address
- Events
- Scan Data
- Location
- Asset Data

IdentityView

- User
- Events
- Access Rights
- Roles
- Attributes
Key Use Case: High-Risk User Monitoring

Enterprises use IdentityView to monitor high-risk users, like DBAs, administrators, contractors, or terminated employees, who access:
- Systems outside their normal role
- Highly sensitive systems
- Systems using shared accounts

Diagram:

- DBAs
- Systems
  - Dev DB
  - Finance DB

Alert:
- Role Violation
Key Use Case: Executive Dashboards

IdentityView captures the riskiest users and aggregates them into the riskiest departments. Organizations use these metrics to:

- Present meaningful security metrics to executive management
- Prioritize security investments and awareness training
## Key Use Case: User Access Reports for Certification

<table>
<thead>
<tr>
<th>Identity</th>
<th>Account Name</th>
<th>Type</th>
<th>Dept.</th>
<th>Manager</th>
<th>Name</th>
<th>Attacker Address</th>
<th>Target Address</th>
<th>Device Vendor</th>
<th>Device Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>John Doe</td>
<td>cjvdak</td>
<td>Full Time</td>
<td>Customer Services</td>
<td>Morris Hicks</td>
<td>Successful Network Login</td>
<td>10.1.1.1</td>
<td>192.168.10.10</td>
<td>Microsoft</td>
<td>Windows</td>
</tr>
<tr>
<td>doej</td>
<td></td>
<td>Full Time</td>
<td>Customer Services</td>
<td>Morris Hicks</td>
<td>Customer record updated</td>
<td>10.1.1.1</td>
<td>192.168.20.20</td>
<td>Peoplesoft</td>
<td>CRM</td>
</tr>
<tr>
<td>cjvdak</td>
<td></td>
<td>Full Time</td>
<td>Customer Services</td>
<td>Morris Hicks</td>
<td>Limeware P2P detected</td>
<td>10.1.1.1</td>
<td>106.203.99.233</td>
<td>McAfee</td>
<td>Intrushield</td>
</tr>
<tr>
<td>cjvdak</td>
<td></td>
<td>Full Time</td>
<td>Customer Services</td>
<td>Morris Hicks</td>
<td>Virus quarantined</td>
<td>10.1.1.1</td>
<td></td>
<td>McAfee</td>
<td>EPO</td>
</tr>
<tr>
<td><a href="mailto:jdoe@company.com">jdoe@company.com</a></td>
<td></td>
<td>Full Time</td>
<td>Customer Services</td>
<td>Morris Hicks</td>
<td>email to competitor.com</td>
<td>10.1.1.1</td>
<td>106.203.99.233</td>
<td>Microsoft</td>
<td>Exchange</td>
</tr>
</tbody>
</table>

Reports and workflow to capture user access across all systems, satisfying audit review and attestation requirements.
Key Use Case: Activity Based Role Modeling

- Provide a complete role-based activity report that identifies systems and applications accessed by role, department, or attribute
- Expedite IDM deployments by mining roles based on user activity
- Identify user and access changes made outside of IDM systems

<table>
<thead>
<tr>
<th>Department</th>
<th>Target Hostname</th>
<th>Device Vendor</th>
<th>Device Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human Resources</td>
<td>finance.arcsight.com</td>
<td>SAP</td>
<td>General Ledger</td>
</tr>
<tr>
<td></td>
<td>dc01.arcsight.com</td>
<td>Microsoft</td>
<td>Windows</td>
</tr>
<tr>
<td></td>
<td>quickarrow.com</td>
<td>Bluecoat</td>
<td>Proxy</td>
</tr>
<tr>
<td></td>
<td>erp.arcsight.com</td>
<td>SAP</td>
<td>SAP</td>
</tr>
<tr>
<td></td>
<td>file01.arcsight.com</td>
<td>Microsoft</td>
<td>Windows</td>
</tr>
<tr>
<td></td>
<td>mail.arcsight.com</td>
<td>Microsoft</td>
<td>Exchange</td>
</tr>
</tbody>
</table>
Key Use Case: Tracking a Rogue DBA

**Query:** Roles by Actor  
**Start Time:** 8/31 17:03:50  
**End Time:**  
**Last Update:** 31 Aug 2010 17:04:36 PDT  
**Drilldown Filter:** Role Name IntersectsList ("DBA")  
**Filter:** No Filter

<table>
<thead>
<tr>
<th>Full Name</th>
<th>Role Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bay Ganyo</td>
<td>DBA</td>
</tr>
<tr>
<td>Erika Mustermann</td>
<td>DBA</td>
</tr>
<tr>
<td>Ford Fairlane</td>
<td>DBA</td>
</tr>
<tr>
<td>Jan Modaal</td>
<td>DBA</td>
</tr>
<tr>
<td>Jan Novak</td>
<td>DBA</td>
</tr>
<tr>
<td>Jean Dupont</td>
<td>DBA</td>
</tr>
<tr>
<td>Josh Coleman</td>
<td>DBA</td>
</tr>
<tr>
<td>Juan Del Pueblo</td>
<td>DBA</td>
</tr>
<tr>
<td>Merrilyn Smith</td>
<td>DBA</td>
</tr>
<tr>
<td>Pinco Pallino</td>
<td>DBA</td>
</tr>
<tr>
<td>Robert Jackson</td>
<td>DBA</td>
</tr>
<tr>
<td>Varsa Pupkin</td>
<td>DBA</td>
</tr>
<tr>
<td>Walter Pinge</td>
<td>DBA</td>
</tr>
</tbody>
</table>
Key Use Case: Tracking a Rogue DBA
Key Use Case: Tracking a Rogue DBA
Key Use Case: Tracking a Rogue DBA

<table>
<thead>
<tr>
<th>End Time</th>
<th>Name</th>
<th>ActorByIP.Full Name</th>
<th>Attacker User Name</th>
<th>Target User Name</th>
<th>Attacker Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>31 Aug 2010 15:12:00 PDT</td>
<td>Login to Known Shared Account by Actor</td>
<td>Robert Jackson</td>
<td>Robert Jackson</td>
<td>SYSDBA</td>
<td>192.168.4.20</td>
</tr>
<tr>
<td>31 Aug 2010 15:11:12 PDT</td>
<td>Request Blocked</td>
<td>Robert Jackson</td>
<td>Robert Jackson</td>
<td>SYSDBA</td>
<td>192.168.4.20</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Threat Score Increase</th>
<th>Name</th>
<th>Active Directory</th>
<th>Previous</th>
<th>Fired</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/31 17:14:12</td>
<td>Robert Jackson</td>
<td>SOLUTIONS.LOCAL</td>
<td>64</td>
<td>1</td>
<td>65</td>
</tr>
<tr>
<td>8/31 17:13:40</td>
<td>Robert Jackson</td>
<td>SOLUTIONS.LOCAL</td>
<td>63</td>
<td>1</td>
<td>64</td>
</tr>
<tr>
<td>8/31 17:13:10</td>
<td>Robert Jackson</td>
<td>SOLUTIONS.LOCAL</td>
<td>62</td>
<td>1</td>
<td>63</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role Name</td>
</tr>
<tr>
<td>DBA</td>
</tr>
<tr>
<td>Senior Analysts</td>
</tr>
</tbody>
</table>
Key Use Case: Tracking a Rogue DBA
Actor Category Model
Case Studies

**Global Financial Services Firm**
- **Driver:** Ease compliance pain from quarterly access reviews
- **Deployment:** AD, IdentityView
- **Use cases:**
  - Gather and reconcile information from 25+ AD forests
  - Present managers clear, easy-to-read access reports for each of their employees
  - Streamlined workflow for managers to approve access reports for their direct reports each quarter

**Large Utility**
- **Drivers:** Monitor offshore developers, improve security metrics and dashboards
- **Deployment:** AD, IdentityView
- **Use cases:**
  - Detect suspicious activity by offshore contractors, like any access to production systems
  - Assign threat scores to all users and departments, which are presented in executive dashboards
# Case Studies

## Health Care Provider
- **Driver:** Track access to patient records to preserve privacy and comply with HIPAA
- **Deployment:** Epic, IdentityView

Use cases:
- Identify personnel accessing the records of people they live near, or “neighbor snooping”
- Detect unauthorized access to the records of celebrity or otherwise high-profile patients

## National Military Branch
- **Driver:** Preventing classified data leakage from shared computers used by military personnel
- **Deployment:** Active Directory, IdentityView, proxy logs

Use cases:
- Attributing access from shared computers and using shared accounts to individuals
- Making Data Leak Prevention (DLP) technology identity-aware
- Monitoring outbound communications channels for classified data
To learn more, contact the HP ArcSight team at:

HPEnterpriseSecurity-info@hp.com or
+44 (0)870 626 2045

HP Enterprise Security, European HQ
Building 3, Chiswick Business Park, 566 Chiswick
High Road, London, W4 5YA, UK
EMEA Headquarters: +44 (0) 870 626 2045
www.hpenterprisesecurity.com