

# ARCSIGHT IDENTITYVIEW

## Adding User Context to Security Monitoring

HP Enterprise Security Product Brief

Organizations have spent countless hours and tens of billions of dollars on identity management and directory systems, but still cannot answer basic questions such as:

- Are shared account IDs in use, and if so, who is using them?
- What did my DBAs do last week, and is it a problem?
- Are former employees still accessing our internal systems?

Answering these and similar compliance and risk-related questions requires a level of visibility that has been difficult for organizations to obtain. Some of the necessary information is contained within directory services, including Microsoft Active Directory. Other information is in the rules and workflows inside human resources (HR) and identity management (IdM) applications, or is stored across the enterprise in log files. But obtaining a comprehensive view of user activity and associated risk across the enterprise requires connecting and correlating information from all of these disparate systems.

ArcSight IdentityView provides complete visibility of all user activity by linking the user, role and group information in directory, HR and IdM systems with the actual activity logs across the enterprise. By analyzing what each user does and comparing those actions to the user's roles, ArcSight IdentityView can detect potentially risky activity, including data theft and unauthorized access to confidential information. Monitoring user activity enables managers to verify their internal controls are effective, reducing the risk of data theft and failed audits.

### Built-In User Monitoring Controls, Rules and Reports

ArcSight IdentityView helps organizations monitor the most common user scenarios:

- **Privileged User and Account Monitoring**  
By combining user and role information in the corporate directory or IdM system, with database, file and all other activity, ArcSight IdentityView can actively monitor the actions of privileged users for risky or unusual activity, a key requirement of many compliance programs.
- **IP Address to User Mapping**  
Many logs for important systems like proxies do not record user information, only IP addresses. Investigating user activity on those systems requires knowing which IP address the user had at a given time. ArcSight IdentityView solves this problem by correlating data between addressing systems (including DHCP, Kerberos and all log sources that use IP addresses) to attribute unauthenticated activity to individual users.
- **Shared Account Tracking**  
By correlating identity data, IP addresses and application logs, ArcSight IdentityView can attribute use of a shared account to a single individual. In legacy applications, this can help organizations comply with regulations such as the PCI standard, which specifically prohibit the use of shared accounts. As a result, organizations can improve compliance without rewriting legacy applications.

### Product Highlights

- Enhanced visibility of all user activity and processes
- Streamlined investigations via comprehensive user activity reports
- Executive dashboards organized by users, groups and departments
- **Terminated Employee/Contractor Access Detection**  
While users may be de-provisioned in the directory or IdM systems, these same users often have accounts active for applications or other systems. ArcSight IdentityView connects local system activity to user status in directory and IdM systems to ensure that terminated users don't access an enterprise's systems or applications.
- **Role-Based Controls Reporting**  
By applying role or department information to all accounts tied to each identity, ArcSight IdentityView can automatically produce complete activity reports by role, group or any other attribute. This capability allows managers to understand how internal controls and processes are working and if changes are required.



- **Multi-Account Correlation**

ArcSight IdentityView has the ability to tie multiple user accounts to a single identity and then correlate activity across those accounts. This enables discovery of risky actions across different accounts; for example, using a database account to extract confidential data, using a Windows account to create a file with the results, and using an email account to exfiltrate the data. It also facilitates investigations into a specific user's activity – a security team can run a single report, rather than hunting for suspicious activity across every system.

- **Separation of Duties Violation Detection**

With ArcSight IdentityView, organizations can set up rules that alert when a user performs actions that no single user should be able to perform. For example, if a user makes a change request and then approves that same request, ArcSight IdentityView can send an alert.

For more information about ArcSight IdentityView, visit <http://www.arcsight.com>.

## Executive-Level Dashboards and Reporting

With ArcSight IdentityView, management can quickly see which users, departments and groups are the source of the most security alerts and compliance risk. ArcSight IdentityView enriches security and activity logs with identity information, so executives can view security data organized in the same way as their companies (see Figure 1).

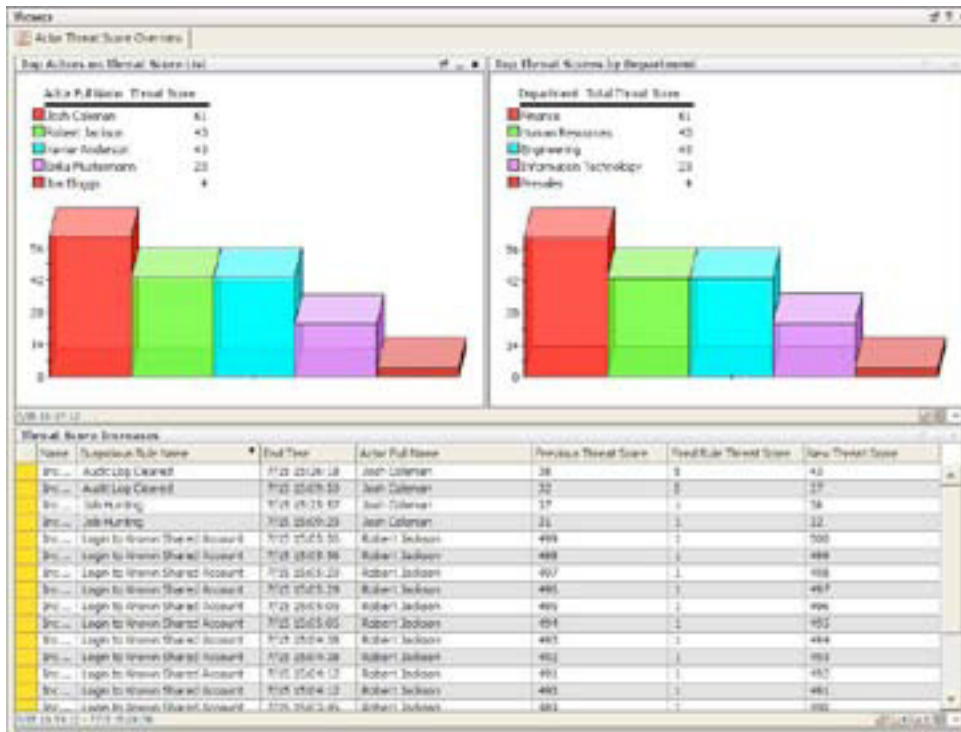


Figure 1: ArcSight IdentityView provides threat score information to identify the riskiest users by department, and displays their risky activity.

