SecureSphere Directory Services Monitoring

Security and Compliance for Microsoft Active Directory

SecureSphere Directory Services Monitoring Benefits

- Secure Active Directory and meet compliance requirements for monitoring all changes
  - Understand the "Who, What, When, Where, and How" of each change
- Discover and respond immediately to critical activity
  - Enforce security polices to generate alerts on unwanted or suspicious changes in Active Directory
- Automate the auditing process and demonstrate compliance with flexible, customizable reports
  - Easily analyze extensive audit data with graphical reporting capabilities and interactive audit analytics

SecureSphere Directory Services Monitoring (DSM) helps organizations achieve security and compliance goals for Microsoft Active Directory. It ensures that critical concerns such as separation of duty, privileged user monitoring, escalation of privileges, and high impact changes are addressed and controlled. SecureSphere Directory Services Monitoring provides continuous visibility into directory services activity that enables security, compliance, and IT professionals to audit, alert, analyze, report, and respond to changes in real time.

Directory services such as Active Directory are the critical system of record for the user accounts and group memberships used for authentication and access control across an organization. Active Directory plays a central role in defining data access rights for enterprise data assets such as Microsoft SharePoint, file servers, and NAS devices. Increasingly, organizations are using Active Directory to establish database access rights as well. Changes within Active Directory therefore can have broad security and compliance implications for sensitive business data. The centralized, highly leveraged nature of directory services requires that organizations have continuous visibility and control over changes made within Active Directory.

SecureSphere Directory Services Monitoring extends Imperva's market-leading Web, database, and file security products to provide an end-to-end view of data, users, rights, and activity across the data center.

Audit All Active Directory Changes

Comprehensive change auditing is necessary to secure Active Directory and demonstrate compliance with regulatory requirements. Active Directory plays a core role in controlling user and group access to enterprise IT resources such as critical applications and files servers, thus all Active Directory administration and changes demand governance. Organizations must also maintain a high-integrity audit trail of Active Directory change activity to meet compliance mandates and monitor privileged users.

Natively, Active Directory offers basic auditing capabilities that do not provide a centralized audit trail across domain controllers and do not provide enough detail to explain precisely what changes were made. SecureSphere DSM provides continuous monitoring and detailed auditing of changes made within Active Directory so that organizations have a complete audit trail showing the "Who, What, When, Where, and How" of each activity. This enables security and compliance staff to understand exactly who accessed, moved, changed, or deleted objects in Active Directory.

Enforce Security Policies in Real Time

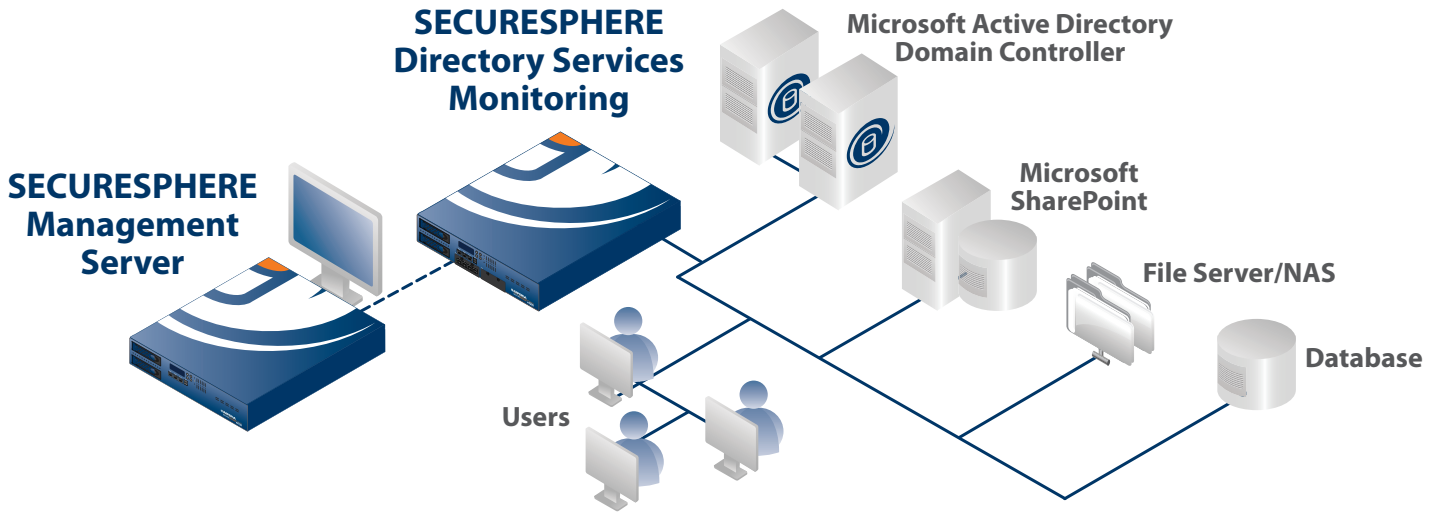
Material changes, such as a modification to configuration settings, can pose significant security risks for an organization. Therefore, it is critical that enterprises have the ability to monitor for, and respond immediately to, high-impact changes in Active Directory. SecureSphere DSM delivers a flexible, granular security policy framework to meet the following security objectives:

- **Privileged User Monitoring and Separation of Duties**. The users and groups in Active Directory are used across the organization to provision access to critical applications and sensitive data. Simply adding a user to a group effectively grants that user access to all of the resources the group can already access. Active Directory administrators therefore are privileged users and wield a tremendous amount of power and control over user rights. The compliance implication is that Active Directory changes must be monitored as part of the separation of duties requirements of virtually all regulations.
- **Protection Against Advanced Threats**. From a security perspective, the centralized role of directory services in access control makes them an attractive target for hackers. Advanced threats such as malware and targeted attacks seek to compromise IT resources, such as Active Directory, that give the attackers access to sensitive business data. Monitoring for unwanted Active Directory changes can help provide early signs of an attack.
- **Strengthening Internal Controls**. Businesses need to quickly assess and respond when Active Directory changes deviate from corporate policy or security best practices. Enterprise best practices necessitate real-time alerting, notification, and external actions to drive remediation efforts.

Aggregate, Analyze, and Report on Active Directory Activity

Despite being one of the most fundamental assets for the IT organization, Active Directory changes are challenging to analyze. Active Directory's out-of-the-box auditing generates large quantities of raw activity data, which necessitates dedicated storage as well as analysis and reporting applications to extract value.

SecureSphere DSM provides greater visibility into Active Directory change activity by aggregating and consolidating audit data into a secured, actionable repository. SecureSphere interactive audit analytics enable administrators to slice and dice the audit trail for forensic investigations and identify relevant data for compliance reports. SecureSphere's flexible reporting framework allows organizations to easily understand security status, automate the auditing process, and demonstrate compliance.



IMPERVA

www.imperva.com