Hybrid Active Directory security and governance

Complete solution for optimized hybrid Active Directory security posture

Office 365 is Microsoft's fastest growing commercial product ever[1], and it's reportedly been purchased by more than 70 percent of Fortune 500 companies in the last year[2]. These companies recognize that implementing the cloud can drastically reduce their IT operations and maintenance costs, empower mobile workforces, and increase scalability and business continuity.

Some companies, however, don't realize that Office 365 requires an Azure Active Directory (AD) instance, as Azure AD provides the directory service for Office 365 applications. Moreover, it's estimated that 75 percent of enterprises with more than 500 employees using Office 365 will sync their on-premises AD accounts with Azure AD[3].

That means, at the heart of your hybrid AD environment, security is crucial. With all of your systems and users relying on AD, and the addition of data and permissions replicating to the cloud, it is more important than ever to have an AD security lifecycle methodology in place. And that's where we come in.

Quest's unique end-to-end solution helps you assess, detect, mitigate, remediate and recover to stay more productive, more secure and more aligned to your business.

Improve your hybrid Active Directory security posture by taking control of your on-premises AD.

BENEFITS:

- Ensure users don't have more access than they should with in-depth reports on access and permission levels
- Quickly overcome unauthorized security changes with automated alerts when there are changes to privileged AD resources
- Continually and automatically remediate unauthorized changes to sensitive resources
- Get a full 360-degree view into security incidents so you can understand what went wrong, why the incident occurred in the first place, as well as the scope of damage
- Automatically recover from destructive security incidents to minimize downtime and loss of productivity

[1] https://blogs.office.com/2015/07/13/news-from-wpc-invested-in-partner-growth/
[2] http://www.office365adoption.com/how-fortune-500-companies-are-leveraging-office-365/
[3] https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect/

Quest solutions for hybrid AD security and governance enable you to improve your security posture by taking control of your on-premises AD and extending those safeguards to the cloud. We enable you to realize Office 365's inherent benefits quickly, easily and with confidence that your infrastructure is secure. Our end-to-end solution helps you be more productive, secure and aligned to your business with tools to:

- Understand who has access to what resources
- Know in real time when suspicious activities occur
- Remediate unauthorized actions immediately
- Recover from accidental and malicious security incidents

CAPABILITIES

Continuous assessment — Understand who has access to what: permissions, privileged groups, sensitive business groups, GPOs and data. Conduct a thorough assessment and know your security configuration baseline to easily identify your surface attack area, vulnerabilities and risk profile. Get clear visibility and reporting so you can stay in the know when it comes to your AD, Windows computers and file shares.

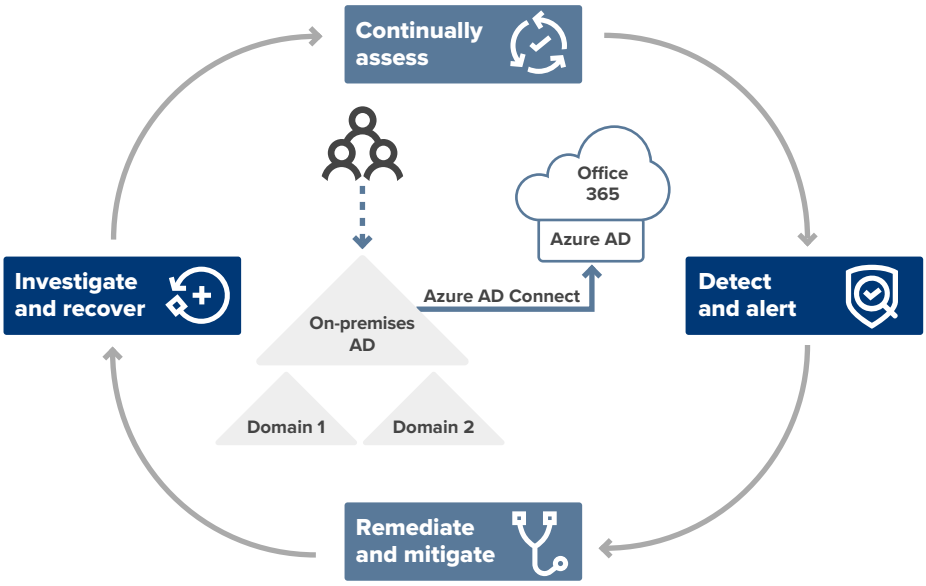
Detect and alert — Know when suspicious/anomalous activities occur. With real-time monitoring, you'll be able to quickly detect and react to potential insider attacks. Proactive security measures enable you to take immediate action and reduce the risk of exposure caused by insider attacks or data breaches.

Remediate and mitigate — Remediate unauthorized actions immediately across AD and your Windows environment. Respond to alerts quickly to minimize damage from unsanctioned changes. Automated security policy enforcement across AD also reduces the risk of human error and mitigates the potential for recurrence. With our end-to-end solution for hybrid AD security and governance, you'll improve operational efficiency and give IT staff more time to focus on innovation rather than spending all their time securing systems.

Investigate and recover — Reduce incident response time investigations across your Windows environment. Correlate security baseline information with fine-grained auditing to get a 360-degree contextual view of how the security incident occurred as well as the most likely path(s) that led to the breach. You'll be able to automate your AD business continuity plan (BCP) to minimize your recovery time objective (RTO) in the event of a security incident that causes partial or total damage across your AD infrastructure.

ABOUT QUEST

Quest helps our customers reduce tedious administration tasks so they can focus on the innovation necessary for their businesses to grow. Quest® solutions are scalable, affordable and simple to use, and they deliver unmatched efficiency and productivity. Combined with Quest's invitation to the global community to be a part of its innovation, as well as our firm commitment to ensuring customer satisfaction, Quest will continue to accelerate the delivery of the most comprehensive solutions for Azure cloud management, SaaS, security, workforce mobility and data-driven insight.



Quest's hybrid Active Directory security solution all the way around your infrastructure

Quest
4 Polaris Way, Aliso Viejo, CA 92656 | www.quest.com
If you are located outside North America, you can find local office information on our Web site.

DataSheet-HybridDirectorySecurity-US-KS-24063