Quest

90%

of organizations feel vulnerable to insider threats.[1]

Strengthen your cyber resilience against hybrid AD & Office 365 security threats

THE CHALLENGE

It seems like every week there's a new data breach in the headlines, and with the recent explosion of Office 365 and Micosoft Teams adoption, we expect the headlines to keep coming in. Whether caused by ransomware - which is expected to hit organizations every 11 seconds in 2021 - cyber attacks, or misuse and abuse of privileged access, your security is under constant threat. Microsoft reports that 300B threats on email and nearly 7B threats on endpoints were blocked over the last 12 months.[2]

As a result, security experts advise taking an "assume breach" mindset: Accept that sooner or later you're going to have someone prowling around your network looking to cause damage or steal your critical data. With that mindset established, your objective should be to increase cybersecurity resilience throughout your Office 365 and hybrid AD environments.

HOW THIS AFFECTS YOU

To strengthen your organization's cyber resiliance, you have to accomplish these goals:

- **Support the needs of your business by implementing new technologies — but do it in a secure way.** Getting to the cloud faster or expanding BYOD can drive business goals, but you have to minimize the security risks.
- **Protect all your sensitive data.** Data growth has been meteoric in recent years, and much of it is unstructured data in cloud repositories like SharePoint Online and OneDrive, instead of a few databases in a locked datacenter right in the building. As a result, it's much harder to even know what you have, much less keep it all secure.
- **Comply with a growing number of increasingly stringent data privacy regulations.** Not so long ago, only certain industries were heavily regulated and ISO certification was good enough. But now regulations like PCI, GDPR and CCPA are reaching deep into every industry. You must not only establish compliance but continually maintain it as regulations emerge and evolve.
- **Pass audits and avoid damaging headlines.** It takes around 280 days to identity and contain a data breach, and these breaches could result in devastating costs - $3.86 million on average.[3] Failed audits can result in steep fines and even put your organization out of business. It's up to you to protect your business.

For many organizations, the common-sense approach to accomplishing these goals will be to invest in perimeter security, invest in SEIM tools and rely on native tools or PowerShell. Unfortunately, each method has its risks. Investing in perimeter security can leave AD security lagging. SIEMs drain budgets, are difficult to use, and rely on native event logs to operate. Native event logs have critical gaps and lack fidelity, meaning attackers slink around a staggering 101 days on average before being discovered.[4]

1 Cybersecurity Insiders, "Insider Threat 2018 report"

2 Microsoft, "Earnings Conference Call" April 2021

3 IBM, "How much would a data breach cost your business?"

4 FireEye, "M-Trends 2018 Report."

"We've had pen testers come in and be very surprised that they could not get past the Change Auditor object protection."

— Enterprise Administrator, Large Retail Chain

Your go-to security and compliance solution

A BETTER WAY

Our view on cyber resilience is that even the best perimeter defenses can do nothing to stop perpetrators from eventually breaking through. That's why you must have strong internal security and governance.

WHAT YOU CAN DO ONLY WITH QUEST

With our unique focus on identity-centered security coupled with market-leading AD management, Quest helps organizations secure their internal Microsoft environment to protect the most critical and targeted assets, Active Directory accounts and Office 365 resources.

We have a complete lifecycle of security solutions that enable you to protect the entirety of your complex on-prem or hybrid environment. This includes:

Remediate and mitigate

Defense against the insider threat starts with proper governance. Quest® solutions automate administration tasks, including user provisioning and deprovisioning, to close security holes and reduce risk. Approval-based workflows add an extra layer of governance and control.

Proactively identify vulnerabilities

IT environments are dynamic, so you also have to regularly check for vulnerabilities. Quest solutions deliver automated, consolidated reporting across your on-premises, hybrid or cloud environment, so you can easily determine who has access to what and how they got that access.

Moreover, you can right-size permissions right from the reports. You can also discover where your most sensitive data resides so you can make sure it is protected, easily review your GPOs, and even prevent critical objects from being changed in the first place.

Detect and alert on suspicious activity

Quest solutions also enable you to sound the alarm faster on active threats by providing real-time auditing of user and admin activity and alerts on privilege escalation, improper changes and other suspicious activity. You can even automate responses, such as blocking the activity, disabling the user or reversing the change.

Quickly investigate and recover from attacks

It takes organizations an average of 69 days to contain a data breach.[1] Quest enables you to get to the bottom of security incidents quickly and easily with centralized data collection and a Google-like search and forensic investigation engine. Moreover, you can build a virtual test lab for DR planning and accelerate disaster recovery – from bare metal provisioning to clean OS restore and AD forest recovery.

Maintain and prove regulatory compliance

Together, these capabilities enable you establish, maintain and demonstrate compliance with a wide range of regulations. Plus, Quest solutions offer smart, scalable log compression, so you can store your audit data cost-effectively for years while ensuring it is available for security investigations and audit checks.

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.

SolutionBrief-MPM-SecuritySolution-US-LR-66939