Quest

90%

of organizations feel vulnerable to insider threats.[1]

Detect, defend against and recover from insider attacks

You've built awesome perimeter defenses — but are you prepared for the threats already inside your network?

THE CHALLENGE

It seems like every week there's a new data breach in the headlines. Everybody's worried about hackers, so organizations have historically invested heavily in perimeter defenses. But the reality is, over half of all breaches are caused by someone already inside the network,[2] such as an employee stealing IP to take to a new job or a fat-fingered admin making a critical configuration error. Often, it's actually an outside attacker who has taken over a legitimate account — Microsoft reports that 95M AD accounts are the target of cyberattacks every day[3] and that 10M Azure AD login attempts each day are cyberattacks.[4]

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. Even the best perimeter defenses can do nothing to stop them, so it's essential to also have strong Active Directory security and governance in place.

HOW THIS AFFECTS YOU

To combat the insider threat effectively, you have to:

- **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.** A data breach can result in devastating costs —$3.86 million on average.[5] Failed audits can result in steep fines and even put your organization out of business. It's up to you to protect your business.

To accomplish these goals, you need to get user permissions under control and keep a close eye on what everyone is doing. But native tools don't make it easy; in fact, 62 percent of users admit they have more access than they need.[6] SIEMs provide some visibility into user activity, but they are expensive to license and difficult to configure and use. Moreover, they're only as good as the data you feed into them —and native logs have major gaps and lack fidelity in critical areas. It's no wonder that attackers slink around a staggering 101 days on average before being discovered.[7]

1 Cybersecurity Insiders, "Insider Threat 2018 Report."

2 Ibid.

3 ZDNet, "Active Directory czar rallies industry for better security, identity," June 9, 2015.

4 Softpedia News, "Microsoft Sees Over 10 Million Cyberattacks per Day on Its Online Infrastructure," May 6, 2016.

5 Ponemon Institute, "2018 Cost of a Data Breach Study."

6 Ponemon Institute, "Closing Security Gaps to Protect Corporate Data: A Study of US and European Organizations."

7 FireEye, "M-Trends 2018 Report."

"Before, I had no control over changes to administrative groups whatsoever. With Change Auditor, I can easily monitor those critical changes just by looking at a folder in my mail."

— Dennis Persson, IT Systems Technician, Region Halland

Your go-to security and compliance solution

A BETTER WAY

What if you could limit the damage a user —or someone who steals their credentials — can do by ensuring each person has only the access rights they need to do their job? What if you could get alerted immediately when anyone does something risky? What if you could establish a baseline of normal behavior for each individual and spot any deviations promptly? And what if you could investigate and respond rapidly to threats?

WHAT YOU CAN DO ONLY WITH QUEST

Quest is the go-to vendor for security and compliance solutions for any on-premises or hybrid Microsoft environment. We offer a full suite of solutions that enable you to secure your internal environment as tightly as your perimeter and ensure continuous regulatory compliance.

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. Advanced user behavior analytics model individual user behavior patterns and detect anomalous actions. 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.[8] 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 slash the lengthy native AD forest recovery process down to a simple GUI-driven process.

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.

8 Ponemon Institute, "2018 Cost of a Data Breach Study."

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_SecurityCompliance-US-38251

Quest