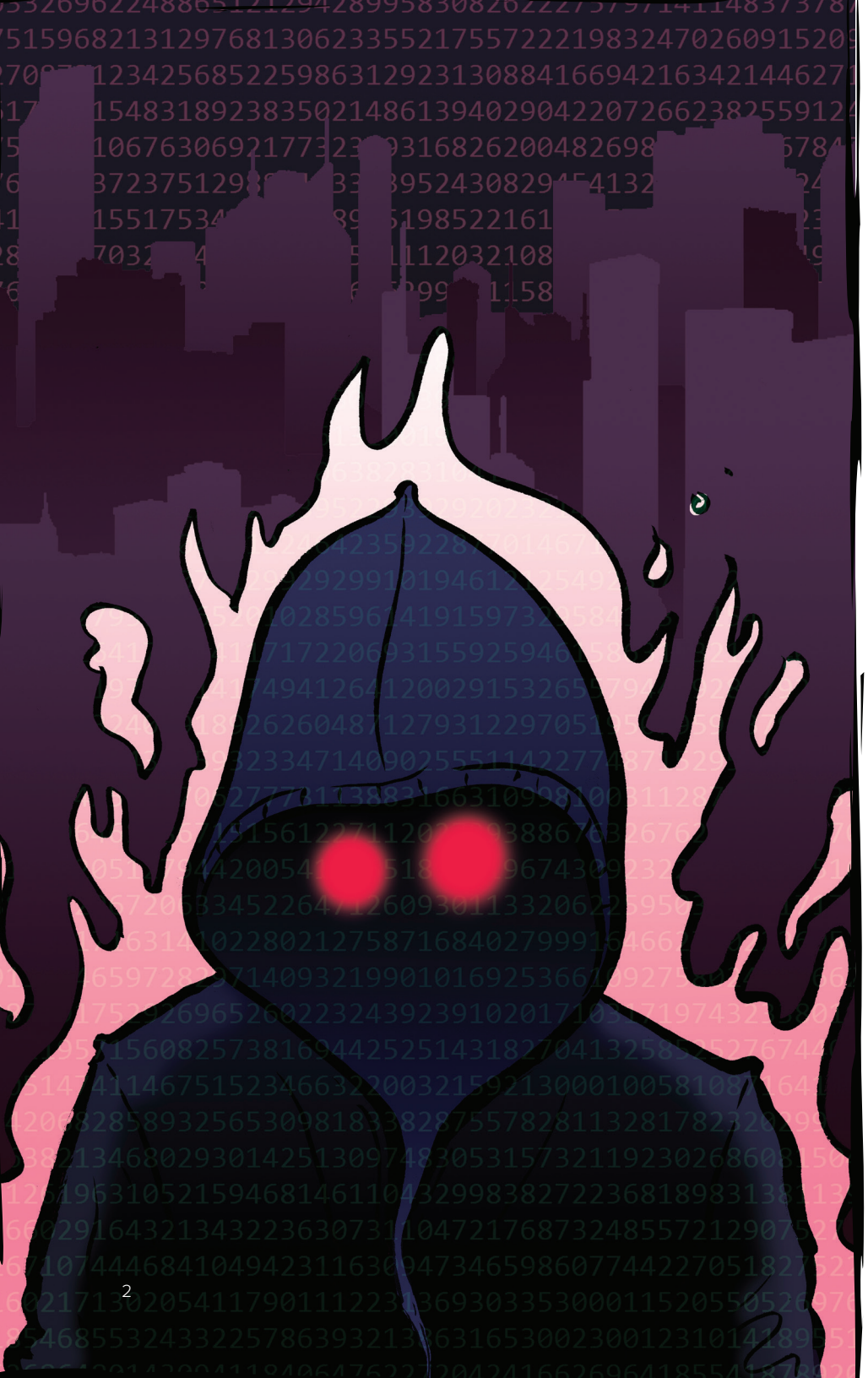
# Ultimate Cyber-Resiliency: a guide to combatting AD security villains

Defend your hybrid Active Directory from risks, threats and disaster.

Quest



## Introduction

In the world of cyber security, Active Directory (AD) is key. Every organization's Active Directory serves as a cornerstone, providing authentication and authorization for every critical resource across the environment. Suffice to say, ensuring that Active Directory is properly managed and secured is vital for continuity and success.

Unfortunately, that's easier said than done, considering how AD environments are complex and constantly evolving. Furthermore, the value that Active Directory holds makes it the number one target for nefarious cyber criminals. Intelligent and relentless, these dangerous adversaries know that controlling Active Directory means controlling the entire enterprise, so they are constantly coming up with new strategies, tools and methods to achieve their goal: AD domination.

In 2021, more than 25 billion brute-force attacks on Azure AD accounts were reported by Microsoft. And the 2022 annual Microsoft Digital Defense Report revealed that 88% of impacted customers did not employ AD and Azure AD security best practices. Additionally, the Microsoft report highlighted that insecure Active Directory configuration ranked among the top issues found among customers recovering from attacks.

The threat of attack is real, and it's not a matter of "if it happens" – it's a matter of "when it happens". Whether it's ransomware, insider threats, misconfigurations, or some other disaster – danger is coming. And hybrid Active Directory has become a common attack vector with attackers exploiting misconfigurations and weaker security postures in critical identity systems to gain broader access and impact to businesses.

The good news is that it's not all doom and gloom. In this eBook, you'll discover how Quest can help you achieve a full lifecycle of hybrid AD cyber-resiliency that mitigates risk before, during and after an attack. Grab a cape and a mask – we're about to conquer AD Active Directory security threats.



Quest

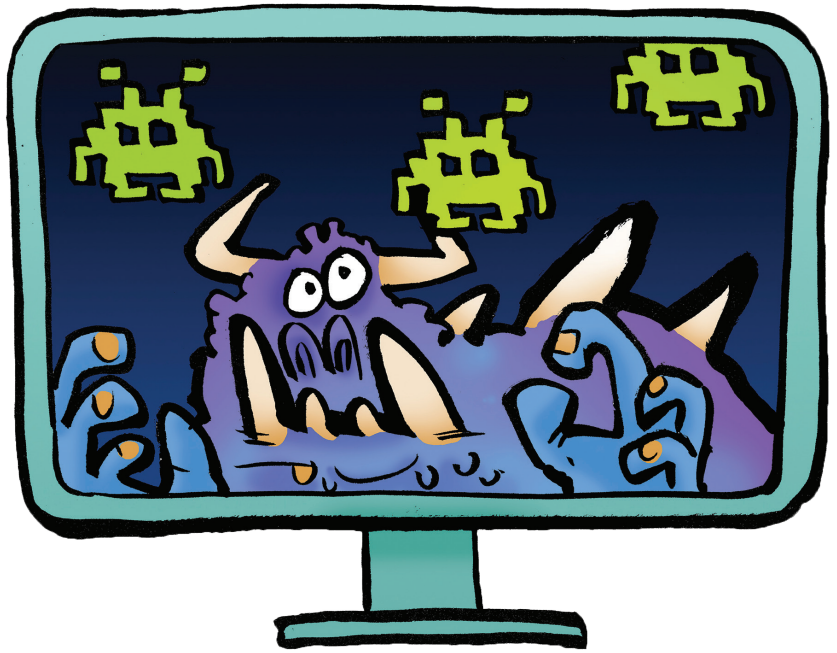
## Establishing the hybrid AD cyber risk management framework

To close gaps in their security infrastructure, many companies adapt their security risk management program to common frameworks, such as NIST (or other regional, vertical or country-specific alternatives). The NIST framework sets standards, guidelines and practices that should be considered when protecting your infrastructure from cybersecurity risk.


The NIST framework consists of the following pillars, or principles:

- **Identify**: Confirm what assets need protection and what weaknesses exist
- **Protect**: Establish safeguards and defenses to protect critical assets
- **Detect**: Investigate security occurrences and incidents
- **Respond**: Develop responses to contain security incidents
- **Recover**: Restore capabilities and data in case of disaster

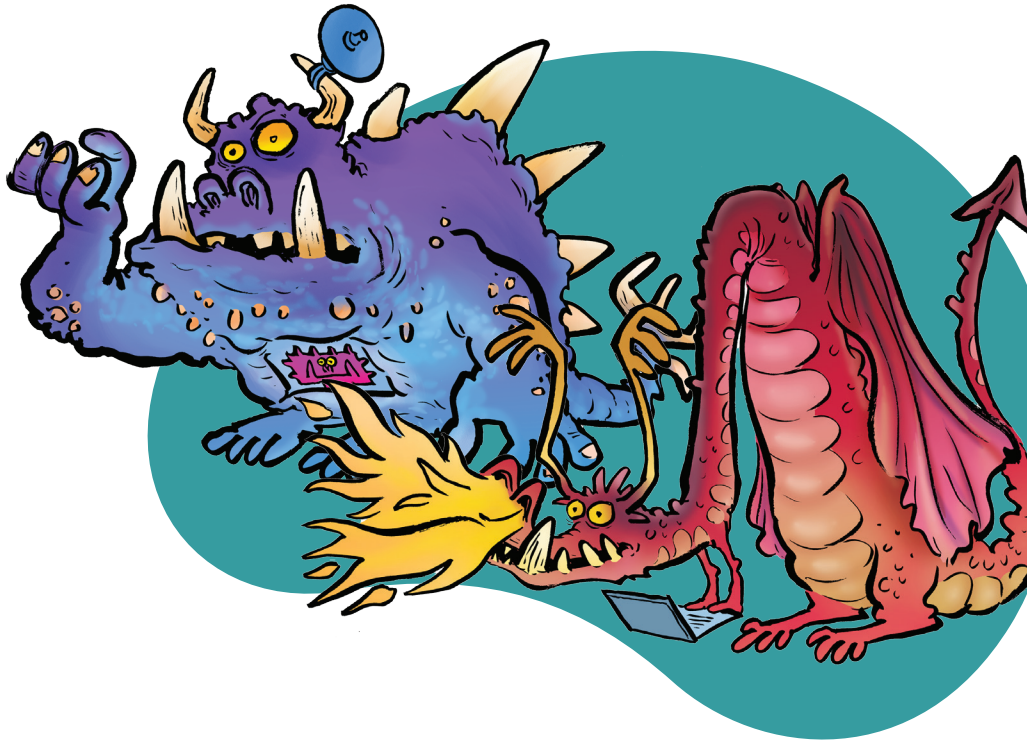
Fulfilling each pillar is key to ensuring the safety of your Active Directory. However, many companies find themselves faced with challenges when trying to achieve their goals in each of these NIST principles.

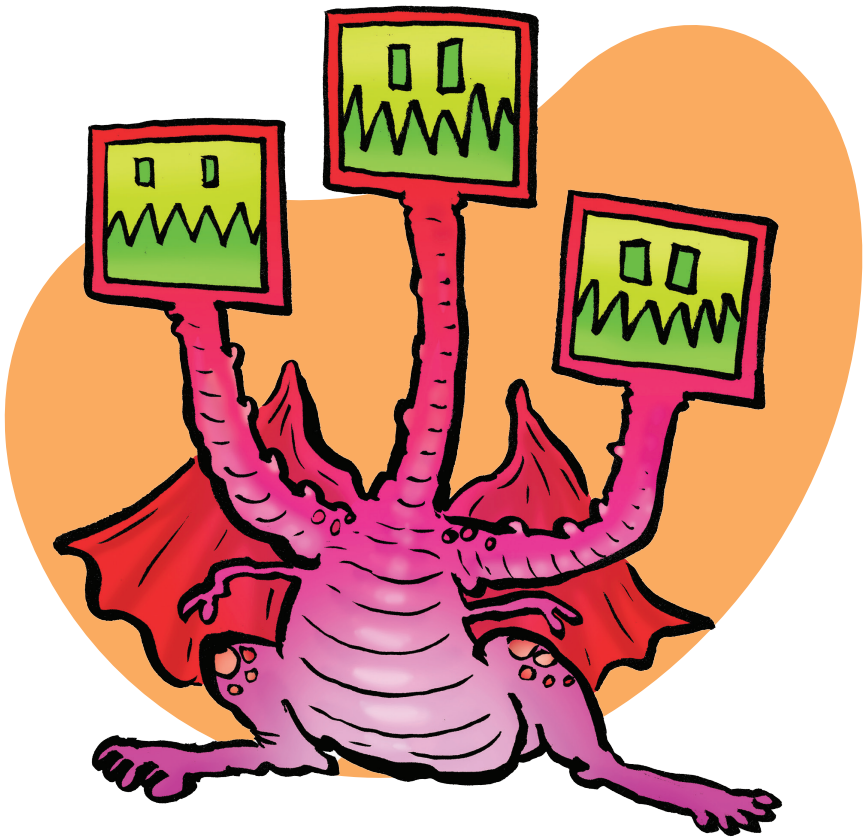




Quest

- **Identification Challenges**: As organizations grow – on premises and in the cloud – they often find themselves lacking visibility into critical aspects of their Active Directory, such as users, groups, permissions and applications. This means that they aren't sure who has access to what information! Furthermore, many organizations can't identify what their most critical assets are – their Tier Zero assets. Knowing what permissions exist in your AD and what your Tier Zero assets are make up a small step in ultimately identifying risk. What about identifying existing pathways and gaps that adversaries can exploit? Can you point out critical vectors that act as gateways to your entire infrastructure? Without visibility into these vital components of Active Directory, protecting yourself from daily threats and truly understanding your risk profile becomes a virtually impossible task.

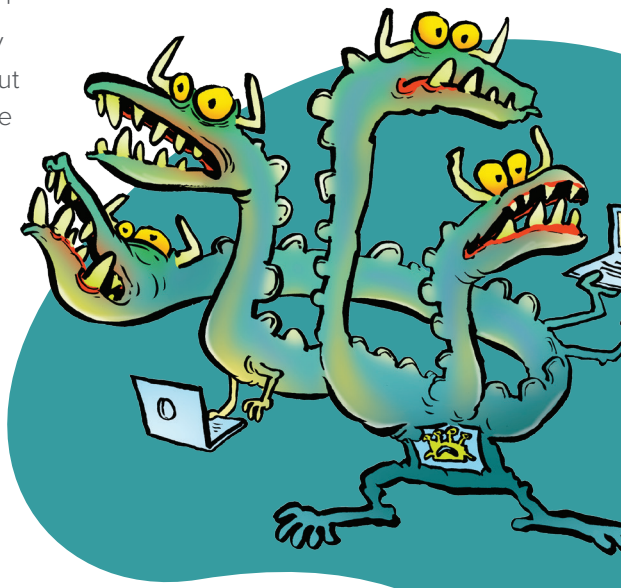




- **Protection Challenges**: Organizations today are adopting Azure AD and Office 365, which only increases their reliance on Active Directory, while doubling the attack surface and introducing additional opportunities for ransomware and other exploits. Unfortunately, vulnerability management for AD is cumbersome, time-consuming, and often impossible using system-provided auditing tools. Group Policy Objects (GPOs) can be a nightmare to control and manage, especially when you think about missing one GPO, that was created by a long-forgotten team and abandoned, can lead to massive detrimental effects to the security posture of thousands of systems in your network. And what about managing and protecting Office 365 tenants, which will only grow larger? Active Directory environments are constantly evolving and expanding – which means the vulnerabilities and assets you need to cover for are also evolving and expanding.

- **Detection Challenges**: While detecting configurations for both on-prem and the cloud, user and admin changes and activities is vital for security, Office 365 and Azure AD security logs do not provide consolidated views of on-premises and cloud activity. System-provided tools do not make it easy to identify exploits, vulnerabilities, and suspicious activity, leaving you scrambling to find out exactly what that new anomaly was – before it's too late.
- **Response Challenges**: Speaking of "before it's too late", let's say you realized that there was strange activity going on – what now? Most organizations find themselves lacking an efficient response system that lets them quickly investigate, analyze and – if needed – restore previous settings and permissions that were functioning before any change happened. Relying on your IT department's capabilities – with system-provided tools – will only lead to frustrating, time-consuming searches for the aforementioned configurations and anomalies, and a realization that you are not sure what the next steps should be.
- **Recovery Challenges**: The worst time to test a disaster recovery plan is in the middle of a disaster. But all too often that's exactly what happens. Microsoft's "Active Directory Forest Recovery Guide" outlines some 40 high-level steps that can be error prone and time-consuming if not automated. Performing manual processes or using native tools only risks malware re-infection, extended downtime and increased losses. You won't be able to confidently use your backups, if you have access to them at all, giving the threat actors time to do more damage and causing your organization to suffer more fiscal and reputational losses. Do you know which domains and users to recover first? How's your communication plan? Getting breached is chaotic enough, prolonging it with an untested plan only increases the chaos. You might think insurance is the answer, but when's the last time you read the fine print in your policy? Are you doing everything right to recoup your losses and get the operation up and running again? This can be due to ineffective tools, lack of cohesion between the tools being used, misguided support, overinvestment (and poor deployment) of perimeter security and underinvestment in identity protection.

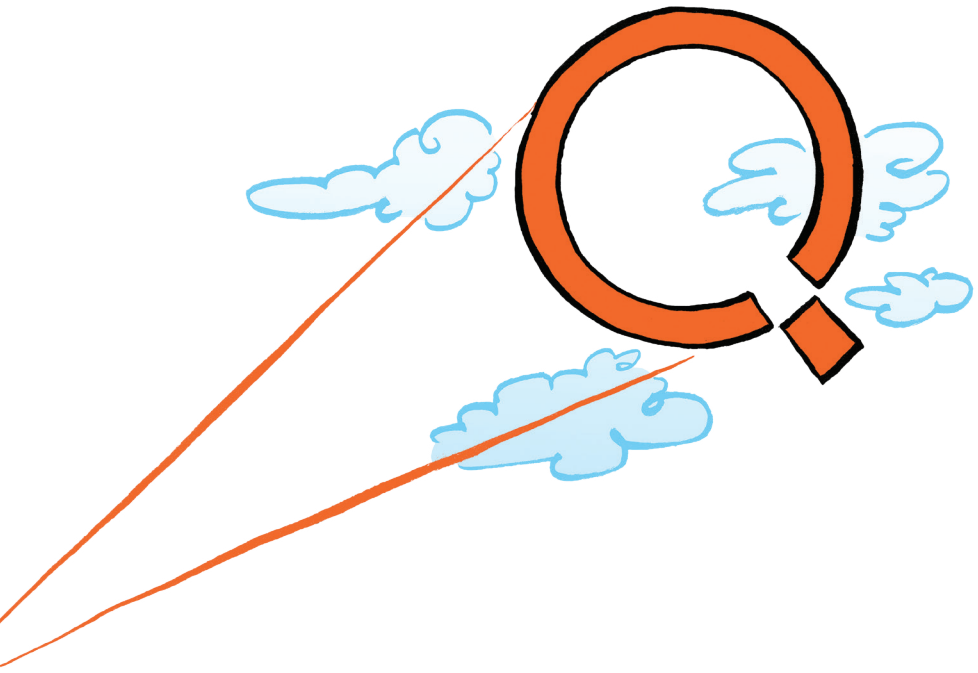
When it comes to Active Directory security, one must be vigilant about all aspects of their cyber-resilience infrastructure. If one pillar is weak, your entire Active Directory – and therefore, your entire enterprise – is at risk of crumbling. Adversaries love when a pillar of the cyber-resiliency framework gets neglected, because it serves as a very welcoming "Please come in!" sign to the rest of the Active Directory environment.





Quest

So, is there a way to ensure that all aspects of the NIST framework are developed and ready to take on the plethora of AD security challenges? Is there a hero to call upon?

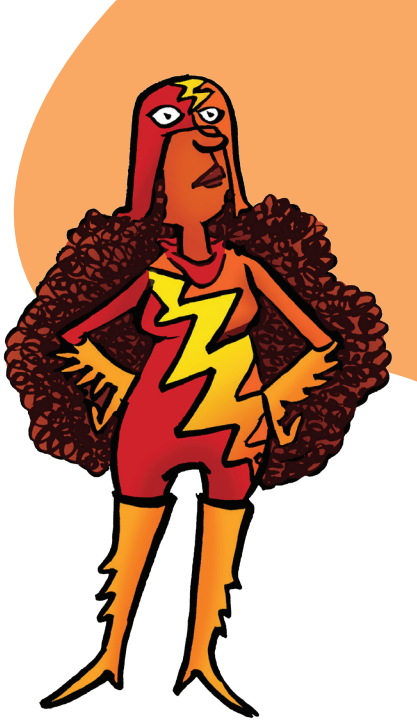


## The quest to cyber-resiliency

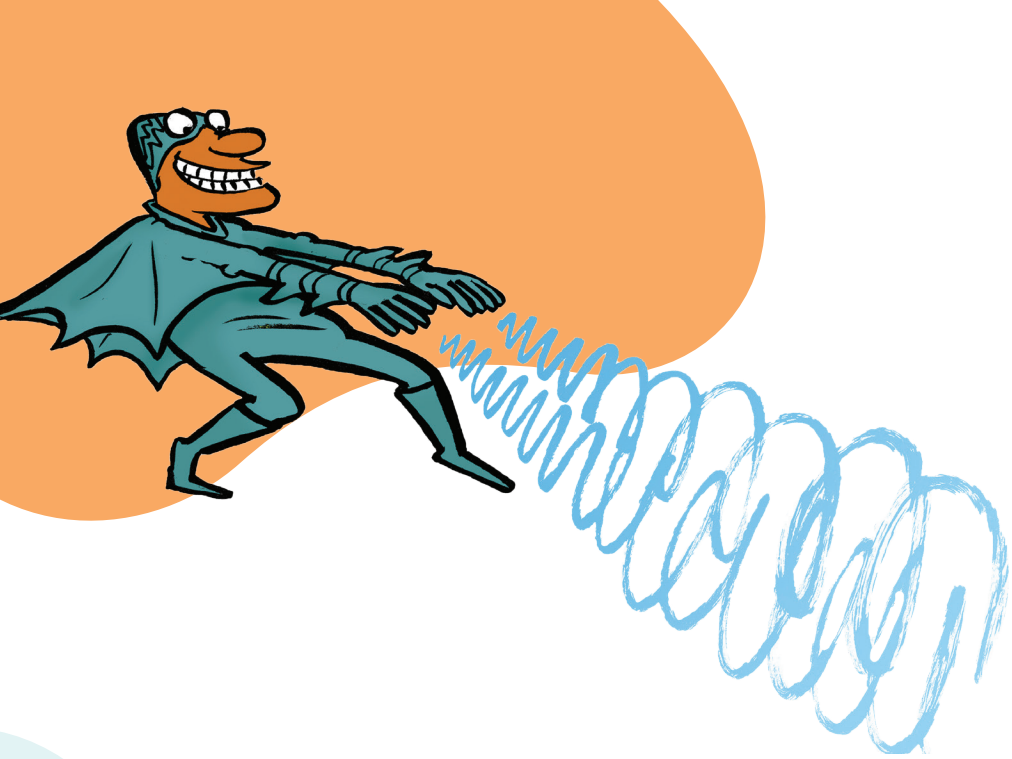
At Quest, we offer an approach to hybrid AD cyber resilience that provides defense in depth to reduce risk at every layer of the NIST Framework, so you can be ready before, during and after an attack.

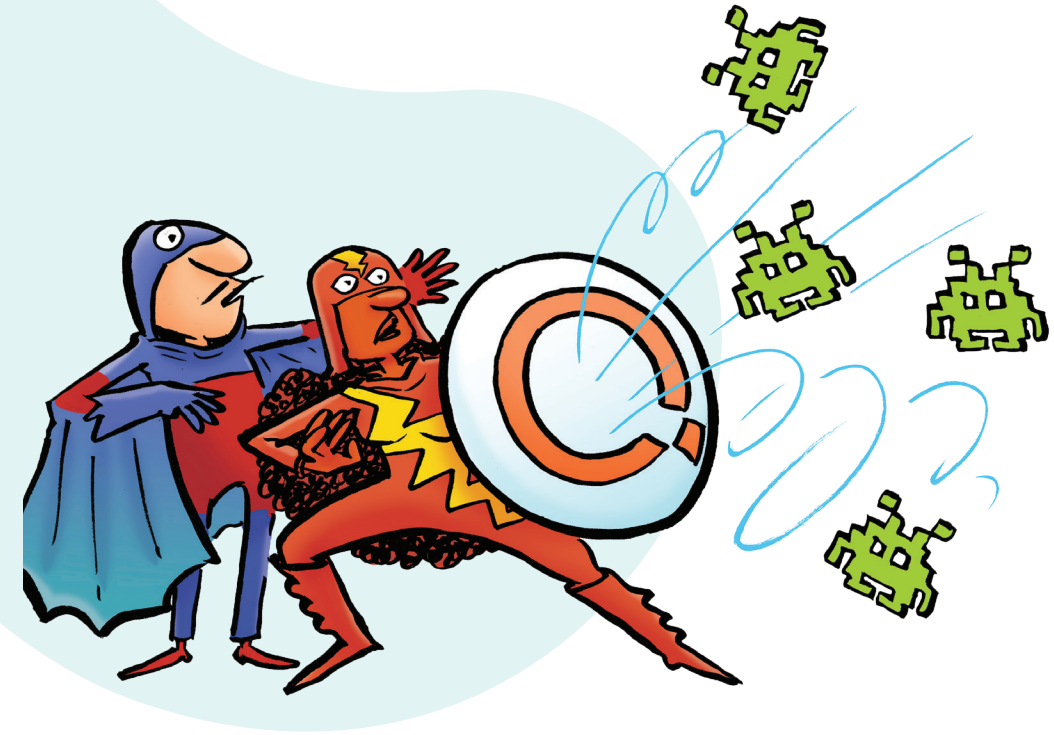
The solutions in our hybrid AD cyber resilience suite are complimentary solutions that team up for a dynamic, comprehensive defense, allowing you to:

- **Identify** indicators of exposure (IOEs) and prioritize the attack paths an adversary could take to own your environment.
- **Protect** your environment so attackers can't make changes to critical groups, GPO settings or exfiltrate your AD database to steal credentials.
- **Detect** indicators of compromise (IOCs) with real-time auditing, anomaly detection and alerting.
- **Respond** to threats and rapidly gather information to accelerate investigations.
- **Recover** AD from any attack, big or small, and restore business operations, data integrity and customer experience in minutes instead of days, weeks or even months.



But how does this team of powerful solutions exactly work together to defend your hybrid AD environment from the onslaught of threats? By putting them into their respective suites, we're able relay their capabilities and explain how they build on one another.





## Quest AD Risk Assessment Suite

The AD Risk Assessment Suite combines two of our flagship products: Change Auditor and the On Demand Audit Hybrid Suite, along with the powerful SpecterOps BloodHound Enterprise to give you the power to identify, protect against and detect potential threats in your environment. With the AD Risk Assessment Suite, you can:

- Audit all security changes across your AD and Azure AD environments, including user and group changes, as well as exploits such as exfiltration of the AD database via offline copy or unauthorized domain replication
- Detect threats early – including unauthorized domain replication, offline extraction of your AD database, and GPO linking – to mitigate and avoid costly ransomware attacks
- Block attackers from making changes in the first place to critical groups, GPOs or exfiltrating your AD database to steal credentials – regardless of the privileges they've hijacked

## Quest AD Risk Protection Suite

With the AD Risk Protection Suite, you get everything from the Risk Assessment Suite along with GPOADmin, our powerful solution for simplifying the management and governance of GPOs. The AD Risk Protection Suite helps you:

- Ensure changes adhere to change management best practices prior to deployment, a critical step in Active Directory group policy management
- Validate GPOs continually through automated attestation — a must for any third-party group policy management solution
- Improve GPO auditing and verify setting consistency quickly and easily with advanced, side-by-side GPO version comparisons at various intervals
- Revert back quickly to a working GPO in the event that a GPO change has an undesired effect. The environment can be running smoothly again in seconds.

Quest

## Quest Hybrid AD Cyber Resiliency Suite

While the first two suites cover more than half of the NIST Framework principles (identify, detect and protect), the final suite – the Hybrid AD Cyber Resiliency Suite – covers the rest of the Framework (respond and recover). With the Hybrid AD Cyber Resiliency Suite, you can rest assured that you've maximized security no matter what cyber events come your way. Along with the products included in the other suite, the Hybrid AD Cyber Resiliency Suite adds IT Security Search to respond to events as well as Recovery Manager Disaster Recovery Edition, and On Demand Recovery to handle all your recovery needs, both big and small, on premises and in the cloud. You'll be able to:

- Automate every step of the manual AD forest recovery process
- Protect AD backups from compromise and eliminate the risk of malware reinfection
- Restore cloud-only objects not synced by Azure AD Connect
- Demonstrate and validate your hybrid AD backup and disaster recovery plan

## Conclusion

With Quest, you receive a complete and continuous AD and Office 365 cyber resilience lifecycle that provides defense in depth across many layers that map to the NIST Cyber Security Framework. Our solutions work together and build on one another to ensure that your cyber-resiliency goals and business outcomes are achieved, without any gaps that might come and haunt you later.

Cyber-criminals of the world beware – the Quest cyber-resiliency story is only getting started.



Quest

## About Quest

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Microsoft 365 migration and management, and cybersecurity resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.



If you have any questions regarding your potential use of this material, contact:

**Quest Software Inc.**
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (www.quest.com) for regional and international office information.