avanade Quest

Do what matters

Hybrid AD Cyber Resilience & Recovery

Active Directory Security Assessment & Proof of Concept

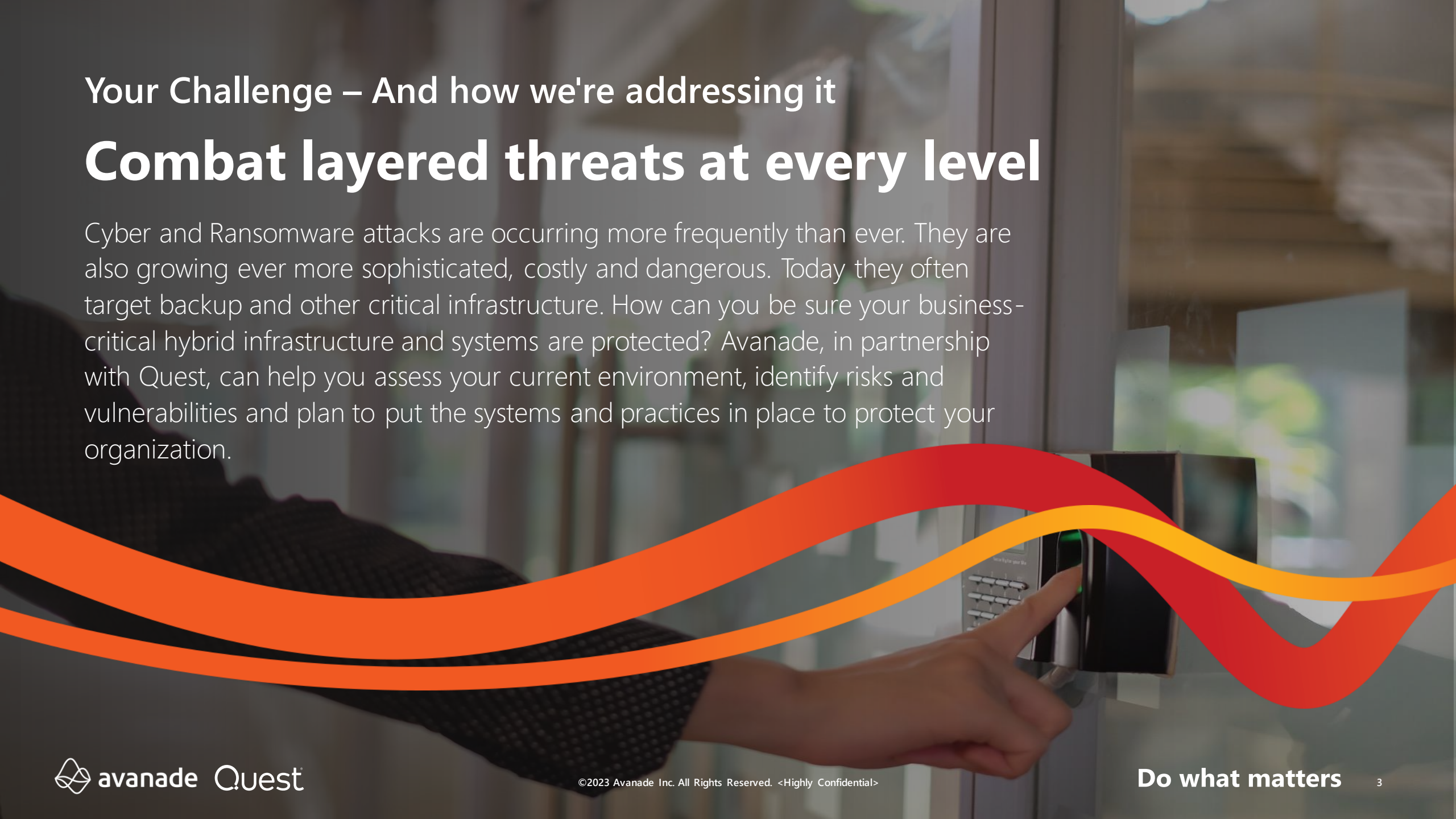
Contents

avanade Quest

Your Challenge – And how we're addressing it

Combat layered threats at every level

Cyber and Ransomware attacks are occurring more frequently than ever. They are also growing ever more sophisticated, costly and dangerous. Today they often target backup and other critical infrastructure. How can you be sure your business-critical hybrid infrastructure and systems are protected? Avanade, in partnership with Quest, can help you assess your current environment, identify risks and vulnerabilities and plan to put the systems and practices in place to protect your organization.



The cybersecurity landscape is ever changing

95 million attempted AD attacks every day

Source: Microsoft

25.6 billion Azure AD attacks in 2021

Source: Microsoft

23 days average downtime, yet **73% of orgs** unable to tolerate more than 2 hours (ESG)

Source: ESG

$42 million lost by LockBit victim

Source: Attento

Microsoft provides strong protection out-of-the-box . . . but there are still vulnerabilities

1. Easy-to-miss abnormal behavior
2. Configuration drift leaves openings
3. Every user poses a potential threat
4. Attack landscape constantly changing
5. Lack of visibility between on-prem and cloud
6. Misunderstood recovery options

avanade Quest

Do what matters

Our Offering

Hybrid AD Resilience & Recovery Assessment

In partnership with Quest, Avanade's Hybrid AD Resilience and Recovery Assessment provides a review/analysis of your current environment(s) and security processes, and a set of recommendations to improve visibility to threats, abnormal behavior and configuration anomalies across hybrid systems. The assessment provides recommendations on specific actions that will help you accelerate recovery from attacks by implementing a dedicated suite of tools for backup and recovery of Microsoft Active Directory.

The NIST Framework

We leverage the NIST Framework in our assessment, which provides five principles to cover all the bases of your cyber resilience strategy

Identify
Assets, policies, vulnerabilities & risk

Protect
Limit the impact of a cybersecurity event

Detect
Continually monitor for anomalies

Respond
Take appropriate action

Recover
Restore impaired services or capabilities

Hybrid AD cyber resilience lifecycle

Avanade - Quest Hybrid AD Resilience & Recovery Assessment - Identify Risks and Vulnerabilities

Identify

Identify indicators of exposure (IOEs) and prioritize the attack paths an attacker could use to own your environment

(Quadrotech Nova / Enterprise Reporter)

Protect

Prevent attackers from making changes to critical groups, GPO settings or link, exfiltrate your AD database to steal credentials

(Change Auditor / GPOADmin / Active Roles / Quadrotech Nova / Safeguard On Demand)

Detect

Detect indicators of compromise (IOCs) with real-time auditing, anomaly detection and alerting.

(On Demand Audit Hybrid Suite)

Respond

Respond quickly and speed investigations with automated information gathering on indicators of compromise (IOCs), as well as additional indicators of exposure (IOEs).

(Change Auditor / IT Security Search / Enterprise Reporter Suite / InTrust)

Recover

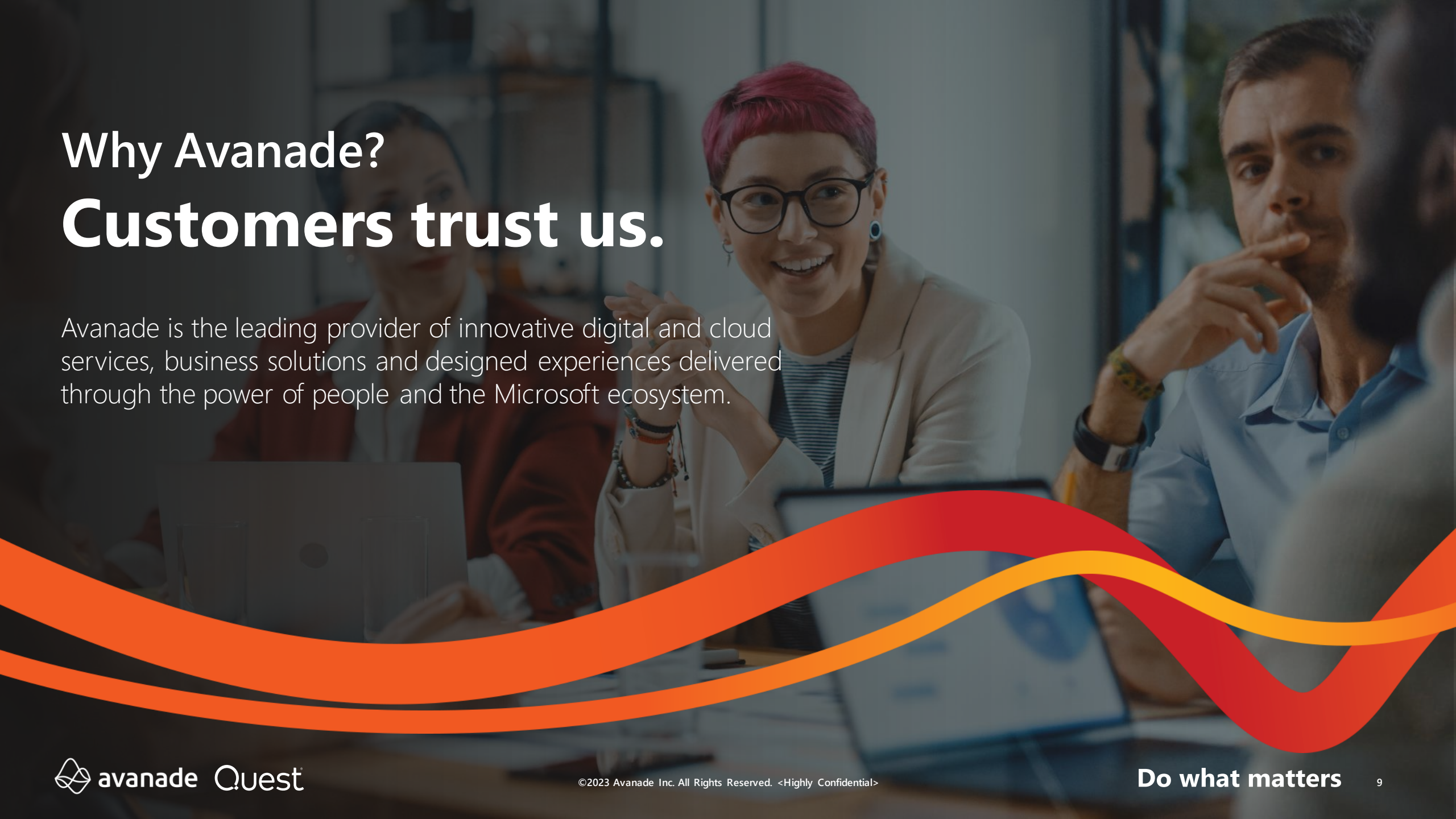
Recover AD from a scorched earth scenario and restore business operations, data integrity and customer trust in minutes or hours instead of days, weeks or months.

(Recovery Manager DRE / On Demand Recovery)

Why Avanade?

Customers trust us.

Avanade is the leading provider of innovative digital and cloud services, business solutions and designed experiences delivered through the power of people and the Microsoft ecosystem.



avanade Quest

Do what matters

Avanade by the numbers

60,000+

professionals in 26 countries

4,000+

client partners served worldwide since 2000 — typically mid- to large-scale enterprises and government agencies

46%

of Global 500 companies as clients

100+

Microsoft Partner of the Year awards, including Microsoft Global Alliance SI Partner of the Year for the 17th time

#1

Microsoft Security certified Partner – 2x the next Global SI

2-time

Winner of Microsoft's Zero Trust Champion Award

avanade Quest

Why Microsoft Technology?

Microsoft is leading the way

Microsoft, one of the most valuable companies in the world, is on a mission: To empower every person and every organisation on the planet to achieve more.

avanade Quest

Powered by a unique partnership

Microsoft has the largest addressable market in our clients

Microsoft has decades of relationship with every client. Microsoft is typically one of the Top 5 partners in terms of spend with many of our clients.

Microsoft's commitment to Innovation & Customer Success

Microsoft has invested millions into tools to evaluate and accelerate the path for converting their estate.

Microsoft's platform is much broader than Azure

All platforms are not equal; Microsoft is much broader than Azure in terms of cloud offerings and extends into M365 (Teams, Office, Etc.) and D365 (Dynamics, Power Apps, Etc.).

Microsoft is the #1 Industry Solution Leader

Microsoft is aligned with industries and more Industry Solutions are developed on Microsoft platforms than the competition, expediting time to value for clients.

Value

+ Partnership:
Avanade and Microsoft is a joint venture for 20+ years.

+ Industry scale:
Bring industry depth and breadth to differentiate the transformation journey

+ Scale, capability & compatibility:
Incumbent in all our clients, ability to leverage Avanade to drive & deliver

avanade Quest

Why Quest?

Around the globe, more than 95% of the Fortune 500 and more than 130,000 customers count on Quest to help them manage, modernize and secure their IT environments.

avanade Quest

Why Quest?

Customer Success

184M	166M	95M	90%
AD ACCOUNTS MANAGED	ACCOUNTS AUDITED	AD ACCOUNTS MIGRATED	SECURITY & COMPLIANCE GOALS MET

Source: Quest Solution Brief MPM

- 99% — Avera Health – "If we had a 90% success rate, that would have been good, but we achieved 99%! That's just outstanding and really hard to believe…it's almost mind-blowing"
- 95% — of customers believe that Metalogix helped them successfully migrate their complex SharePoint environments
- 94% — of MPM customers are likely to recommend Quest PSO
- 67% — of Change Auditor customers report ROI in < 9 months
- 50% — of Fortune 500 companies have used / are using Recovery Manager

Industry Validation

40/40 Quest is the only vendor that supports all features and functionality listed in the Gartner Market Guide for Cloud Office Migrations.

Source: Gartner Market Guide for Cloud Office Migration Tools

Microsoft MSUS Partner Award Winner 2020

Microsoft Content Services Partner Program Charter Member

Microsoft Partner — 2019 Partner of the Year Finalist — Health Award

https://www.gartner.com/en/documents/3997341

Quest Award-Winning SaaS

On Demand Recovery
June 2018

On Demand Audit
August 2020

On Demand Migration
November 2020

On Demand Audit
March 2021

On Demand Recovery
March 2021

Getting Started – Active Directory Recovery Assessment & POC

When a disaster like ransomware or a cyberattack strikes a customer's Active Directory and wipes out the Domain Controller's operating system every minute of downtime will have major impacts. If the customer does not have a plan to quickly recover, an Active Directory disaster can stop the business in its tracks.

The Active Directory Recovery Proof of Concept offering will showcase how Quest recovery solutions can provide customers a method of quickly recovering from Active Directory and Azure AD disasters. Additionally, an experienced architect will provide analysis of a comprehensive set of data relating to AD including Domain Groups\Members, Domain Users, Domain Summary and AD Permissions.

Solution

Software:

- Quest Recovery Manager for Active Directory – Disaster Recovery Edition
- Quest On Demand Recovery (Optional)
- Quest Enterprise Reporter

System Requirements: (must update next)

- High-end or server-class machine
- Intel® or AMD 2 GHz multiprocessor
- 4 GB RAM
- 64-bit MS Windows Server 2012 or higher
- Microsoft SQL Server 2012 or greater
- PowerShell 5.0 or later
- Microsoft .NET Framework 4.8 or higher
- An account with AD read permissions
- Optional: Secure Storage Server, Windows Server 2016 or higher stand-alone workgroup server

Activities

- Deploy \ Configure Quest solutions
- AD recovery scenarios:
  - Granular Object\Attribute recovery
  - GPO recovery
  - Forest Recovery (bare metal, clean OS, VM)
  - Perform Forest Health Check
- Azure AD recovery scenarios (Optional):
  - Perform Cloud Backup
  - Review Difference Reports
  - Perform Azure AD recovery of hybrid and cloud objects
- Generate Assessment Reports
  - AD Summary
  - AD Account Assessment (User, Service Accounts, Group Accounts)
  - AD Access Summary (# of Domain Admin, elevated rights, etc.)

Outcomes

- AD Security Assessment Report & Executive Summary
- Recommendations and Roadmap
- Active Directory Recovery
  - Automated Backups Scheduled
  - Granular Object\Attribute\GPO Recovery Validated
  - Restore Comparison Reporting Validated
  - Forest Recovery Methods Validated
  - Forest Health Check Validated
  - Restore from Secure Storage Server validated (Optional)
  - Recovery Plan Document Generated
- Azure AD Recovery (Optional)
  - Automated Backups Scheduled
  - Granular Object\Attribute Recovery
  - Restore to the cloud

Typical Engagement Duration: 2 – 4 Weeks

avanade Quest

Do what matters

Let’s get started

This journey begins with an assessment which will provide analysis and reports that will help identify vulnerabilities. We will also provide a set of recommendations that can be actioned to strengthen your defenses against attack. To get started, contact:

MicrosoftOfferings@avanade.com

avanade Quest