HOW MERGERS AND ACQUISITIONS IMPACT DATA SECURITY

As illustrated by the Equifax and Marriott data breaches

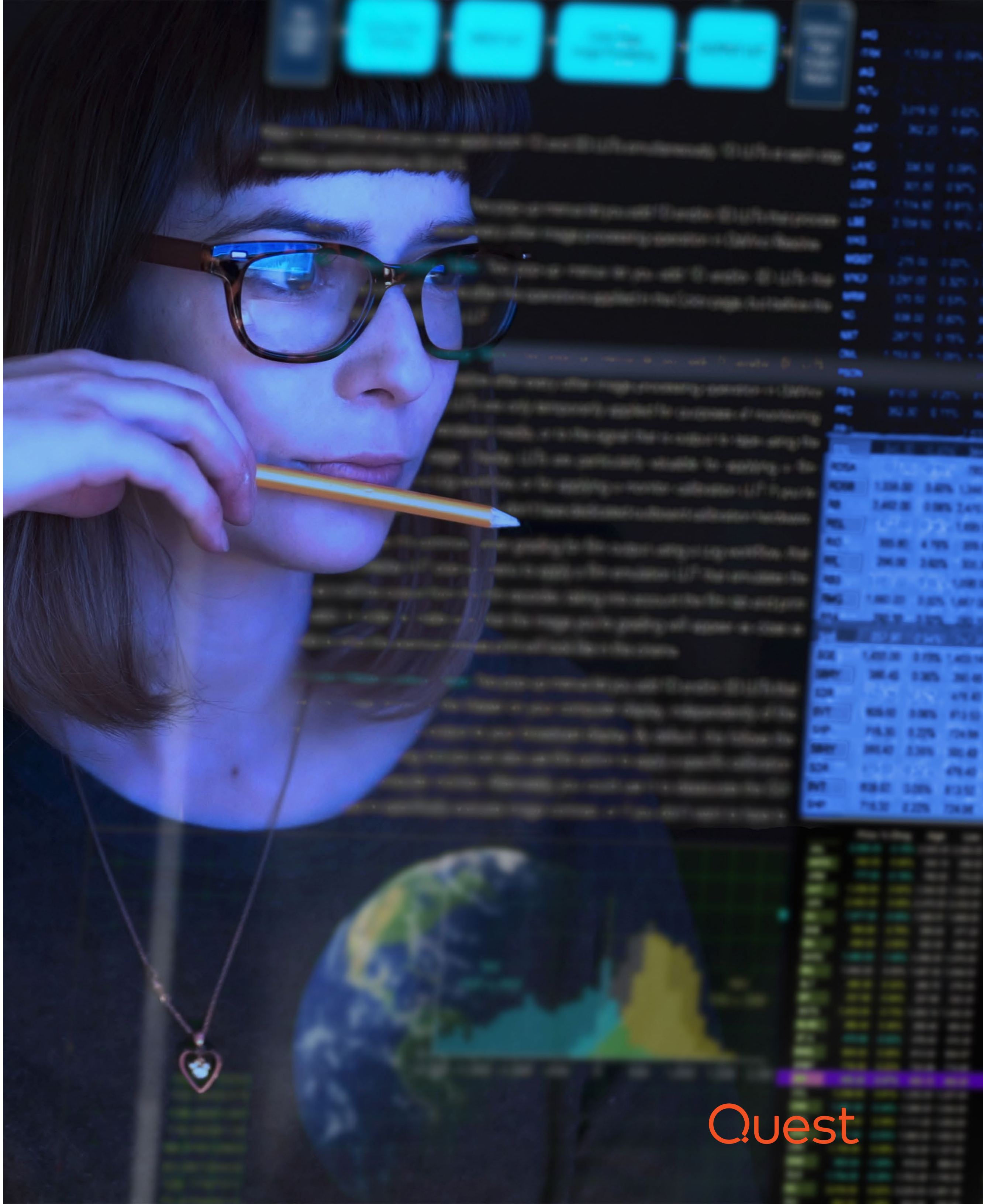
Quest®

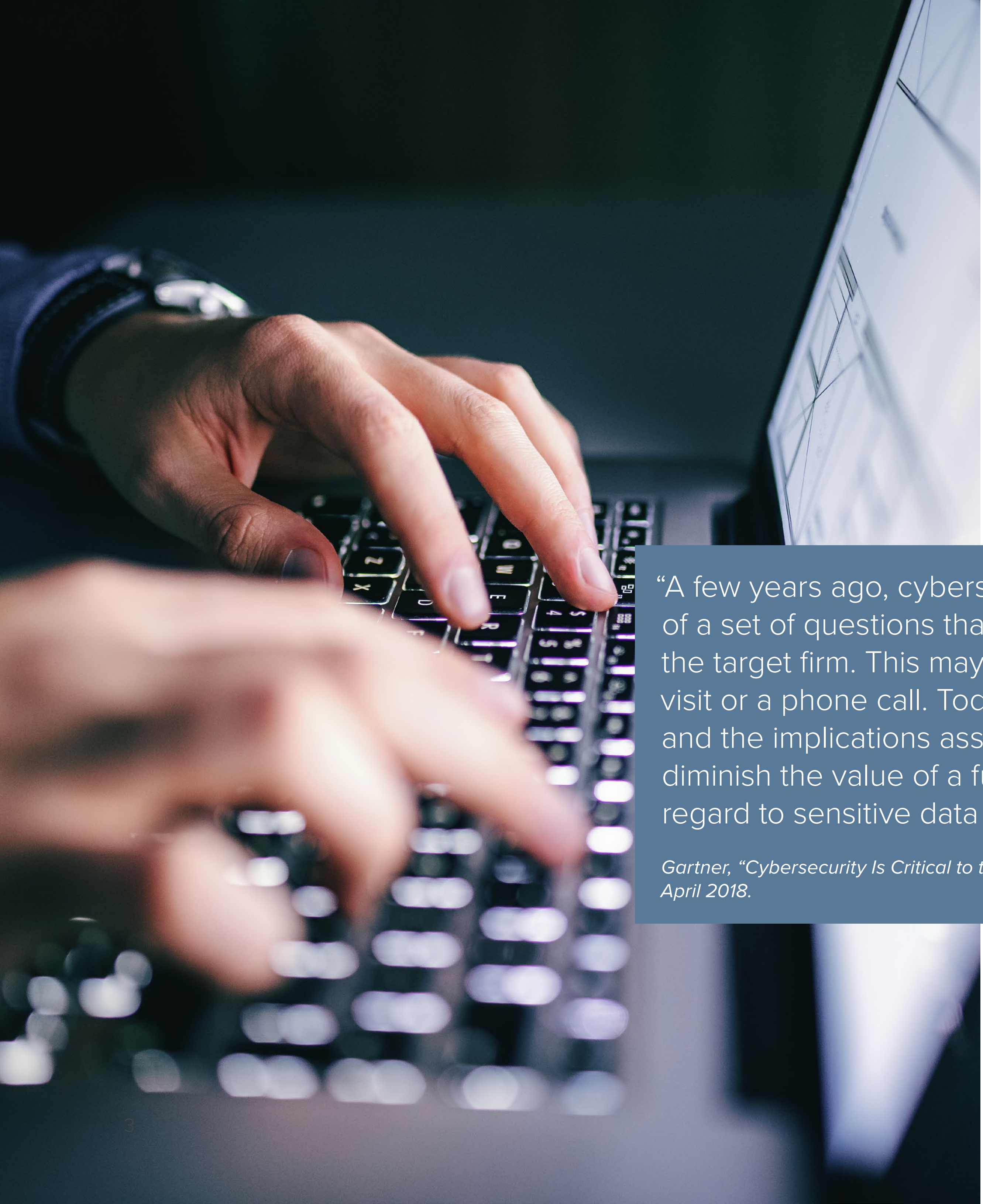
Introduction

GETTING IT INTEGRATION RIGHT IS CRUCIAL TO ACHIEVING M&A SYNERGIES

2018 was a banner year for large, complex mergers and acquisitions, and this year is expected to be even bigger. According to Deloitte's 2019 M&A Trends Report, 76 percent of M&A executives at US-headquartered corporations and 87 percent of M&A leaders at domestic private equity firms expect the number of deals their organizations will close over the next year to increase. Moreover, 70 percent of respondents anticipate that those deals will be larger than the ones in 2018.

The primary goal of M&As is synergy — ensuring that the value and performance of the new combined company is greater than the total of each of them individually. The sooner the combined entity can achieve synergy, the sooner it will realize improved financial performance. And the most important factor in achieving those benefits is a successful IT integration. In fact, Gartner reports that "25% of typical M&A-related integration efforts are coming from IT, and more than half of all synergy-relevant integration activities heavily depend on IT, meaning that CIOs





have a significant opportunity to accelerate M&A execution."[1]

Unfortunately, in the glow of anticipated synergies, companies often make crucial mistakes and fail to get the IT integration done right. As a result, they suffer serious security problems that put the newly created company at risk. This ebook reveals how to avoid those missteps and achieve the security required to reap the benefits you expect from your merger or acquisition.

> "A few years ago, cybersecurity due diligence consisted of a set of questions that the acquiring firm presents to the target firm. This may be supplemented by an on-site visit or a phone call. Today, security is a boardroom issue, and the implications associated with it can seriously diminish the value of a future organization, especially with regard to sensitive data and intellectual property."
>
> *Gartner, "Cybersecurity Is Critical to the M&A Due Diligence Process," Sam Olyaei, 30 April 2018.*

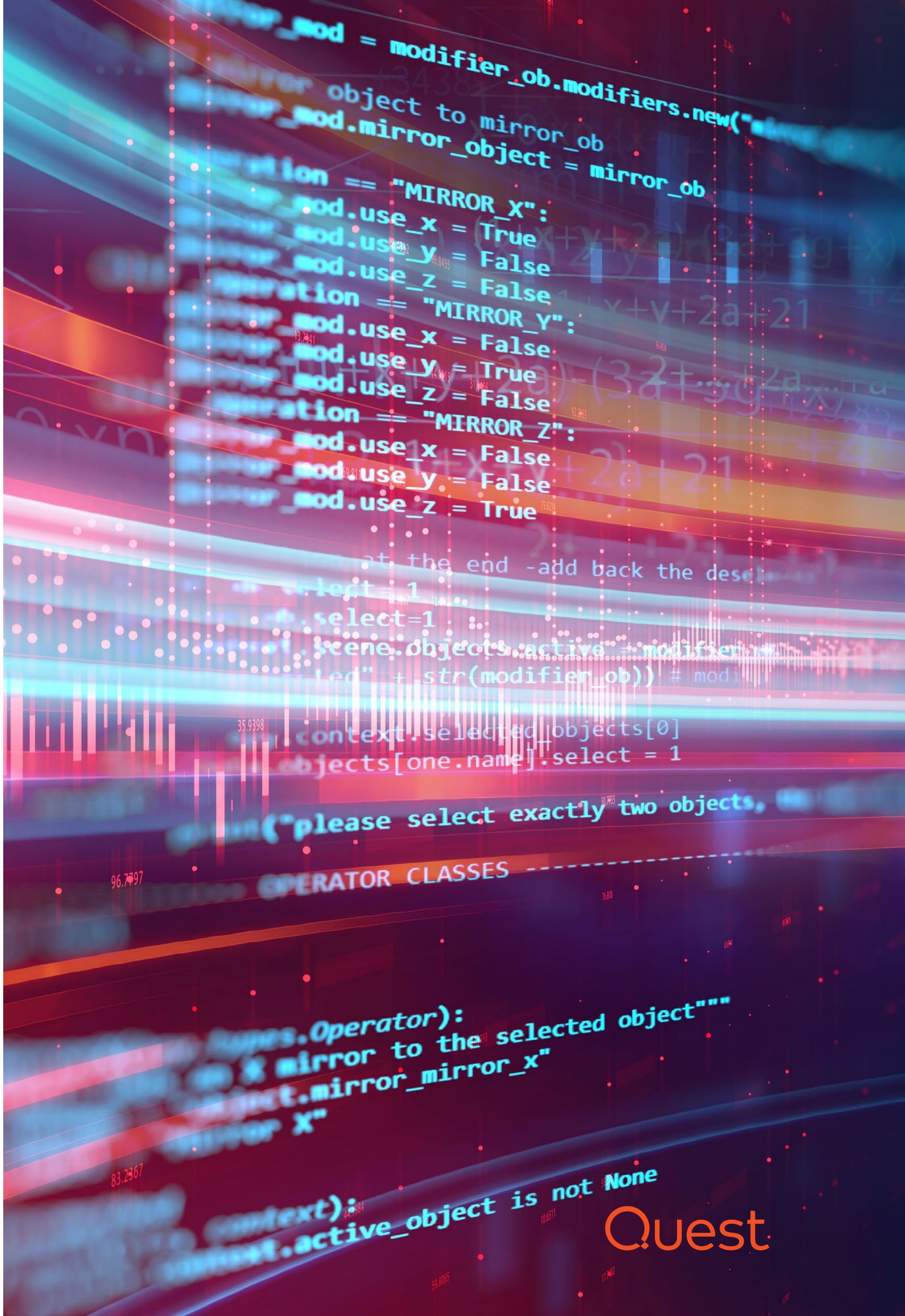
[1] Gartner, "The CIO's Role in Making Mergers and Acquisitions Faster" (ID G00226390), Ansgar Schulte, refreshed December 5, 2018, published February 1, 2012.

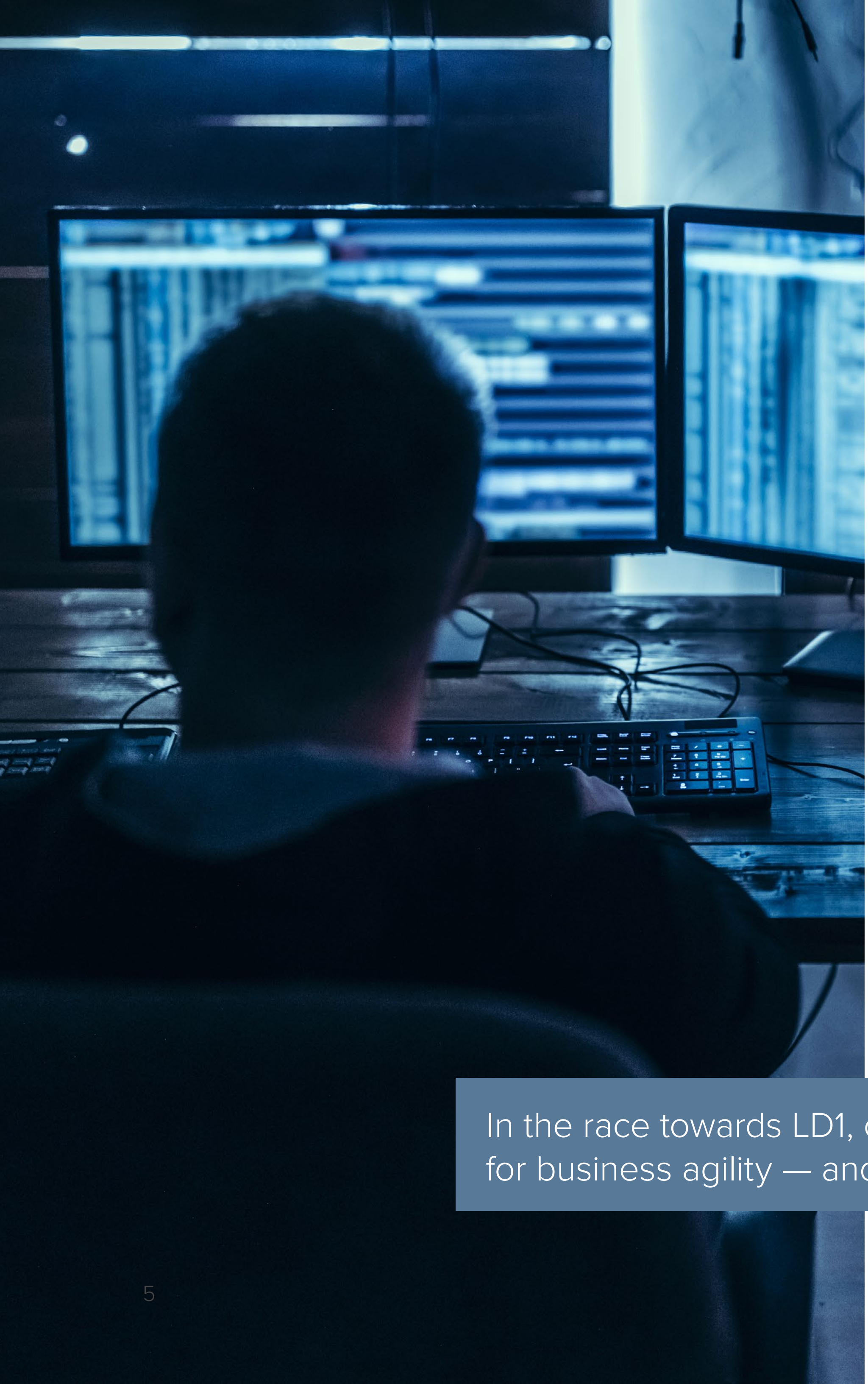
How M&As impact security

PRE-LD1

Once a merger or acquisition is announced, the race towards Legal Day 1 (LD1) begins. Pressure mounts on IT teams to complete the IT integration quickly, and proper IT due diligence is sacrificed for business agility. Here are some of the common mistakes that can lead to dangerous security issues down the road:

- **Not establishing the scope of the migration —** The goal of LD1 is not a complete integration between the organizations involved in the M&A; it's to have some minimum level of interoperability and communication, along with the appearance of unification to the outside world. Failure to scope the migration carefully can have serious implications for security. Under-scoping, such as forgetting about all those B2C accounts in the cloud that need to be migrated, can leave users without the access permissions they need to be productive on LD1. Over-scoping is arguably worse; for example, if you migrate user accounts for employees who are part of HR's workforce reduction, you create opportunities for those employees or others to misuse those accounts for malicious purposes.
- **Establishing an Active Directory trust before performing a cybersecurity analysis —** Active Directory is the core authentication and authorization mechanism in any Windows environment. In order for resources to be shared between





two AD domains, an AD trust is established between them, so there can be tremendous pressure to establish trusts between the AD domains of the IT environments being integrated in a merger or acquisition. However, creating a trust with another domain creates a pathway for anyone in that domain — including a malicious insider or a compromised account — to traverse laterally into your environment. Before you take that risk, you need to thoroughly review the security policies and procedures in place in the other AD domain.

- **Using dirty data —** Any AD infrastructure that is more than a few years old is likely to have experienced significant growth and change, often without sufficient oversight and management — in other words, sprawl. As a result, just about every AD infrastructure involved in a merger or acquisition has some amount of duplicate, stale and unnecessary data. Failure to clean up all this dirty data adds cost and complexity to the IT integration project, leaving IT pros even shorter on time to attend to all the tasks required to reach LD1 on time. Moreover, giving short shrift to cleanup increases security risks in several ways. First, every unused computer and user account that does not get properly disabled and deleted is a ripe target for attackers to exploit. Second, IT teams often give into the temptation to rely too heavily on SID history, thereby giving users the same access in the new environment as the old one without stopping to consider whether those access rights are appropriate. It's the IT equivalent of not changing the locks on a house you just bought.

In the race towards LD1, companies often sacrifice proper IT due diligence for business agility — and suffer serious security consequences.

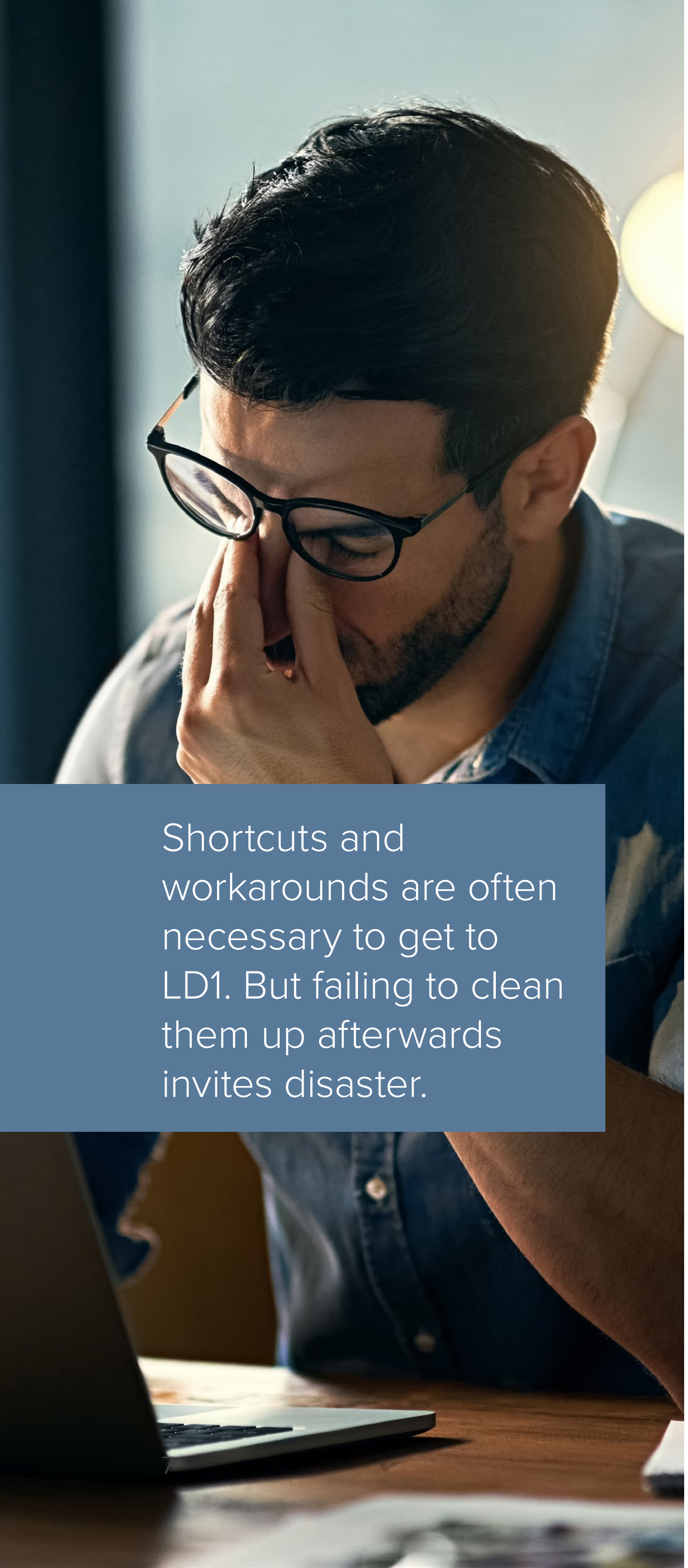
Case in point: Marriott's acquisition of Starwood

Back in 2015, the CEO of Marriott predicted the company's acquisition of Starwood Hotels would deliver $200 million in annual cost synergies by leveraging back-office and operational efficiencies. However, two years after the deal was completed, Marriott discovered that hackers had been merrily romping through Starwood's guest databases since 2014, accessing, encrypting and downloading the personal data of up to half a billion customers. Clearly, Marriott failed to perform proper cybersecurity due diligence during the M&A IT integration project or they would have discovered the massive issues with Starwood's security processes and perhaps even the breach itself.

Now, instead of basking in the glow of M&A synergies, Marriott is suffering storms of epic proportions. Estimates of the direct costs from the data breach range from $200 million and $600 million, but that's just the start of the total bill. Regulators could tack on a fine of as much as $915 million for failure to comply with the EU's General Data Protection Regulation (GDPR), and litigation costs will likely add millions of dollars more. In addition, the U.S. Securities and Exchange Commission could potentially prosecute Marriott for failing to disclose the breach promptly. Finally, there are the less tangible costs, including brand damage and loss of customer loyalty.

All in all, the damage could top 3.5 billion dollars — all of which Marriott could have avoided with a careful and thorough IT integration process.

Marriott's failure to perform proper IT due diligence during its M&A will cost it as much as $3.5 billion.



Shortcuts and workarounds are often necessary to get to LD1. But failing to clean them up afterwards invites disaster.

POST LD1

On your way to the LD1 goals of basic communication and interoperability, IT teams often have to make some compromises, such as leaving legacy systems in place and using workarounds to enable the associated workflows; all those shortcuts need to be cleaned up. And of course, there's still all the work that was beyond the scope of LD1, such as various server, application and workstation migrations.

Unfortunately, organizations often make mistakes during the post-LD1 phase that can lead to security issues, including the following:

- **Not migrating legacy apps —** Moving legacy applications, especially home-grown applications that are AD dependent, often seems not to be worth the effort. Because of the work and complexity involved, organizations opt to leave the old directory in place to work with the legacy environment and set up some sort of coexistence between the old AD and the primary AD. But it's almost inevitable that the old AD will get out of sync with the primary AD, or the old servers won't get patched properly — leaving you with security gaps that insiders and intruders can take advantage of.
- **Trying to get by with native tools —** While native tools are free, they have limited functionality and simply cannot scale to the size and complexity of most AD and Office 365 migrations. Moreover, there is no native tool for tenant-to-tenant migrations. Therefore, when you weigh the ROI of purpose-built migration tools and support from a trustworthy vendor, be sure you factor in the cost of forcing IT teams to struggle with manual processes and limited visibility, as well as the direct and indirect costs of a security incident that could result from relying on basic tools.
- **Not planning for the unexpected —** Even organizations that successfully avoid all the previous pitfalls are not home free. Things will go wrong. Ensure that you can quickly and easily roll back migration tasks that do not work as expected, or the business will suffer. A proper backup and recovery system must be in place before, during and after the migration to roll back mistakes in a timely manner and ensure information doesn't get lost.

Case in point: Equifax's multiple M&As

In 2005, credit reporting agency Equifax embarked on an aggressive growth strategy — by 2018, it had acquired 18 companies, making one of the largest private credit-tracking firms in the world. By one measure, this M&A approach was wildly successful: Equifax's market value more than quadrupled, from approximately $38 per share in December 2005 to $138 per share in September 2017.

However, the manner in which the IT integrations were performed during these acquisitions was a significant factor in the data breach the company suffered in 2017, which exposed the sensitive personal data of 148 million people. As the report from the U.S. House of Representatives Committee on Oversight and Government Reform put it, "While the acquisition strategy was successful for Equifax's bottom line and stock price, this growth brought increasing complexity to Equifax's IT systems, and expanded data security risks."[2]

The blistering report notes that the breach was "entirely preventable." Specific issues included failure to patch a version of Apache Struts that was used by an internet-facing consumer dispute portal custom built back in the 1970s, and expired certificates that allowed traffic flowing to and from the internet to not be analyzed by the intrusion detection or prevention systems for 19 months.

"It looks like this will be the most expensive data breach in history," commented Larry Ponemon, chairman of Ponemon Institute, a research group that tracks the costs of cyberattacks.[3] He estimated that the total cost of the breach could be "well over $600 million," which includes technology and security upgrades, legal fees, and free identity theft services to consumers whose data was stolen, as well as costs to resolve government investigations into the incident and civil lawsuits against the firm.

Equifax's failure to deal with the IT complexity resulting from its M&As led to one of the most expensive breaches in history.

[2] U.S. House of Representatives Committee on Oversight and Government Reform, Majority Staff Report, "The Equifax Data Breach," December 2018.

[3] Reuters, "Equifax breach could be most costly in corporate history," March 2, 2018.

How to protect yourself

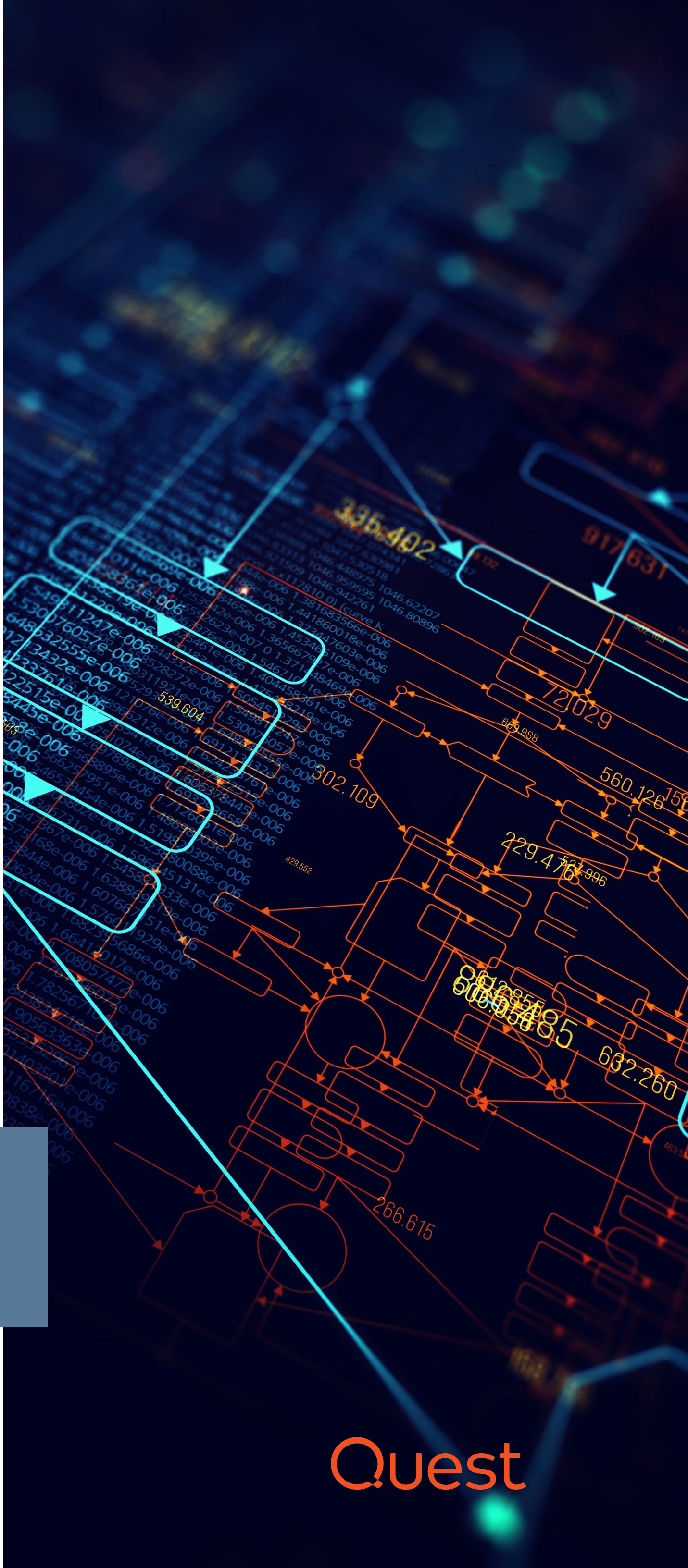
As you can see, there are many ways for the IT integration portion of an M&A to go sideways — and that wasn't even the complete list. You might be dismayed at this point. But there is good news on two fronts.

First, this is not untraveled territory by any means. Plenty of organizations have already undertaken AD migrations and consolidations and Office 365 or Azure AD tenant to-tenant migrations, and you can learn quite a bit from their experience. Second, while migrations differ in their specifics, such as the platforms involved and the volume of data being moved, the same basic best practices apply to nearly every migration. At a high level, you need to ensure that you can:

- **Perform discovery —** Make sure you get a thorough understanding of the users, applications, systems, permissions and other details of both the source and target environment, as well as their interactions and interdependencies. Then work with your business counterparts to identify unused mailboxes, accounts and services that do not need to be migrated, as well as content that should be archived. This process will simplify the migration and improve security and administration in the target environment.

- **Back up and recover data —** Before you begin any migration, you need to make thorough backups of the originating forests, mailbox repositories and collaboration sites in case in case something goes wrong during the move. Of course, a reliable backup and recovery solution will continue to deliver value long after the IT integration project is complete.
- **Ensure productivity —** The migration process will take time, and you need to ensure that users can organize meetings no matter which system the various participants are one, everyone retains uninterrupted access to all their email, and so on. Therefore, it's essential to make sure you can synchronize public folder content, free/busy information, mailboxes and critical data between the two systems. In addition, you should ensure that all users who are being moved to a new system will have their existing passwords moved with their accounts, and that you can update users' AD and Outlook profiles once they've been migrated.
- **Keep management informed —** Make sure you can report on how the migration is proceeding to the various stakeholders, or given them secure access to access that information themselves on demand.
- **Properly govern and secure the target environment —** Make sure your new combined IT environment is secure by establishing proper governance and tracking and alerting on abnormal or suspicious changes and user activity. Ideally, you want to be able to prevent changes to your most important objects, such as powerful administrative groups.

Following established security best practices during your IT integration will help your organization avoid being the next Marriott or Equifax.



Conquer the complexities of M&A IT integrations with proven solutions and first-class support from Quest.

Conclusion

M&As are increasing in both number and size, and their success depends to a great extent on proper execution of the IT integration. Unfortunately, many organizations fall prey to common mistakes, both in the rush to LD1 and in the months afterward, that can seriously compromise the security of the newly combined organization and lead to massive expenses rather than the savings the deal was intended to deliver.

However, by following the expert advice here, your organization can avoid being the next Marriott or Equifax. And you don't have to go it alone. Quest has developed a comprehensive framework for the effective integration, consolidation and management of on-premises, cloud and hybrid Microsoft environments — software and services you can count on, again and again. Even better, it's repeatable: You become familiar with one set of solutions, one support team and one services team, so when the next M&A falls into your lap, you'll be prepared.

To learn more about the security impact of M&A IT integrations, discover best practices and see how Quest solutions enable you to conquer the complexities involved, read our whitepaper, "IT Integration Best Practices in Mergers & Acquisitions (M&A)."

ABOUT QUEST

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats and regulatory requirements. We're a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we've built a portfolio of solutions which now includes database management, data protection, identity and access management, Microsoft platform management and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. 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.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at www.quest.com/legal

Trademarks