Cybersecurity resilience in an era of identity sprawl

How unified identity security can help close critical exposure gaps and support Zero Trust initiatives

ONE IDENTITY by Quest

As a CISO, your concerns expressed to the board of directors about cybersecurity have been largely drowned out by macroeconomic challenges, pipeline complexity and a need to enable a drastic increase in remote access.

Now it's Saturday morning and your work mobile phone is buzzing in your home office.

Why is your director of IT security simultaneously texting and calling you?

"This isn't good news," you think.

It isn't.

There's been a cyberattack. The extent of it is unknown, but your director of IT security tells you that the team is assessing the situation.

Questions race through your head:

- How did they get in?
- Was an internal user part of the attack?
- How much privileged information did they access?
- How am I going to communicate this to the board of directors?
- Will this help or hurt my proposed cybersecurity budget for the next fiscal year?
- Do I need to update my resume?

There's been a cyberattack. The extent of it is unknown, but your director of IT security tells you that the team is assessing the situation.

The risk of identity sprawl

Your organization has been victimized by its own identity sprawl. It's a security risk of insidious creation that incrementally takes shape behind the guise of productivity and innovation intended to help the organization to operate faster and more effectively.

It seemed like the right thing to do to support the business with resources that enhanced the execution of its daily tasks. The problem is that each new system, app or database that your users connect to has a unique credential-handling process and requirements. Some less stringent than others. Some less secure that others. Some better. Many worse. Often, there's no visibility into who has access and what they are doing with it.

Layer on top of those issues, the ongoing need to provide privileged remote access to your admins; manage an increasing number of external users connecting with an even greater number of devices, operating systems and browsers; and attempts to control a roiling expanse of accounts, IDs and passwords.

You've got identity sprawl.

What are you going to do to control it, manage it and balance productivity against security?

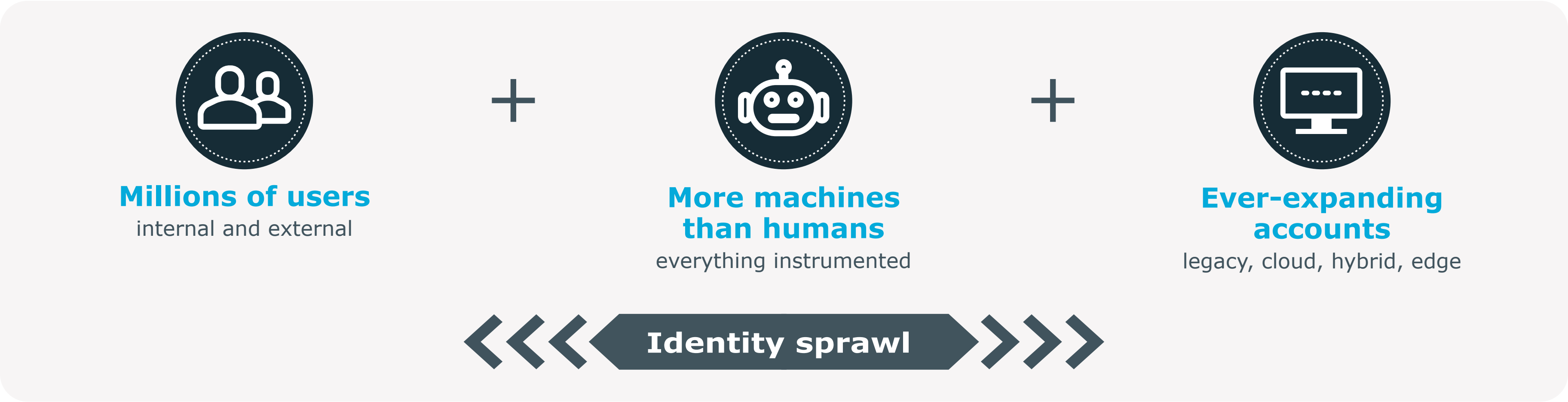
The following is a high-level, eight-step overview of identity sprawl. This ebook discusses the disappearance of the traditional security perimeter, acheiving cybersecurity resilience and the Zero Trust model. You will learn how to take a holistic approach and how a unified identity security platform can protect your organization — and your reputation.

Trends that drive identity sprawl

As described above, the IT landscape is evolving before our eyes, which is having significant implications on how organizations must protect themselves to ensure cybersecurity resilience. It's tough to keep up. Some examples of changes with which security professionals must quickly adapt include:

- The rapid disappearance of the traditional office and infrastructure
- Dispersed organizations are here to stay – employees are increasingly working from home and from remote locations
- A reliance on contractors and external partners to scale and expand value
- The push to adopt new platforms and technologies to accommodate remote access and non-traditional work environments
- The rise of cloud-first computing and the distribution of cloud services to different physical locations
- The constant desire to optimize for efficiency, accessibility and cost savings
- Increased IT complexity due to adapting to privacy regulations, such as, GDPR, HIPAA and CCPA) and data-sharing processes that help to maintain privacy or security
- Automation Robotic Process Automation (RPA) is progressively being used to streamline formerly manual and time-consuming processes.

Each of these trends creates new opportunities for efficiency and increased cybersecurity resilience, but each can create new challenges as well. Why? A common thread among each is the explosion of identities. Simply put, more people (internal and external), robots, machines and devices need to access company assets. On top of that, user accounts proliferate as organizations support a multi-generational IT landscape. All of this contributes to perhaps the biggest cybersecurity challenge yet: Identity Sprawl.



Millions of users
internal and external

+

More machines than humans
everything instrumented

+

Ever-expanding accounts
legacy, cloud, hybrid, edge

Identity sprawl

Why taming the sprawl matters

We all know that bad actors exploit cybersecurity gaps wherever the gaps exist and often at scale. This is playing out in real time with identity sprawl, as we've seen a massive increase in identity and credential theft attacks recently.

For example, Verizon's 2021 Data Breach Investigations Report (DBIR) found 63 percent of all breaches involved credentials, and CensusWide found that nearly half of organizations surveyed were hit with privileged credential theft in the previous year.

You see the devastating impact of these identity-related gaps featured on the front page of news sites virtually every day. The SolarWinds hack, the Colonial Pipeline cyberattack and an Exchange Server vulnerability are just a few examples of highly visible incidents. These breaches not only impacted the average person's safety, livelihood, and security, but also resulted in negative repercussions for the organizations.

What's more, the success of some attacks could have been easily thwarted. Cybersecurity Insiders noted in a recent report that almost half of all users have more privilege than they need to do their job. That's why you not only see enterprises prioritizing identity and privilege, but you even have governments calling out their relative importance. In a September 2021 draft memo, the U.S. Office of Management and Budget (OMB) highlighted a set of deliverables due by the close of fiscal year 2024, including for government agencies to adopt multifactor authentication and to set up enterprise-wide identity management processes.

For organizations to close this cybersecurity exposure gap, they will need to tame identity sprawl — or face fines, lawsuits, and lost customer confidence and revenue.

63%

Of all breaches involve credentials.

The rise of identity as the new perimeter

With identity-related challenges becoming more prevalent and impactful, it stands to reason that the importance of identity security is increasing.

The traditional perimeter remains an important defense for a cyberattack, but in many ways, it was born for another era. This infrastructure-centric approach, which has been a cornerstone of cybersecurity strategies for many years, is based on the belief that it is possible to protect everything inside the enterprise. Naturally, the only way to achieve this lofty goal is to optimize your defense at the outer-most points where preventing compromise at all points might be possible.

With the security perimeter rapidly becoming IT lore, relying on this approach is simply not practical and antiquated. Senior IT security executives now recognize that compromise is inevitable. And as such, a more pragmatic strategy is to take measures to keep bad actors out, but also to prevent exploitation once they get inside the network. With this identity-centric approach, forward-looking organizations are prioritizing what's most critical, and then taking steps to verify everything before ever granting access in the first place — e.g., who is this user? what should they have access to? what are they doing with that authorization? and when should their rights change?

In short, the traditional perimeter is eroding, and identity is emerging as the new edge.

Infrastructure-centric
PROTECT everything

Identity-centric
VERIFY everything

25

different systems to manage access rights at a typical large enterprise.

Key roadblocks to cybersecurity resilience

While identity security is a key emerging trend, success in this endeavor isn't always straightforward. This is largely due to how identities are evolving. In the past, organizations were primarily concerned with internal employees who were hired to do a single job, who were office bound, and who accessed resources from a single point. Most identities were users.

Contrast that with today, and it's an entirely different dynamic. Not only do security professionals have to worry about internal employees, but they also need to consider identities of contractors, suppliers and partners. Instead of doing one job, employees tend to change roles frequently, they are not office bound and they access what they need often from multiple points. And security professionals need to consider not just users, but also applications and machines as well. Users now can have multiple identities across even more accounts, users can be machines and robots, human users can have multiple devices that connect with different versions or generations of applications and they can all be moving about hitting resources from different physical access points and systems.

Moreover, most organizations today manage access rights in silos. According to the Third Annual Global Password Security Report, the average large enterprise identities in 25 different systems. This broad and varied environment can prevent the IT security team from attaining complete visibility into user activities. It also prevents the team from applying analytics in an end-to-end fashion. These challenges ultimately cause gaps and inconsistencies, and they can become a barrier to verifying everything before granting user access, which is a critical part of to implementing a modern security approach.

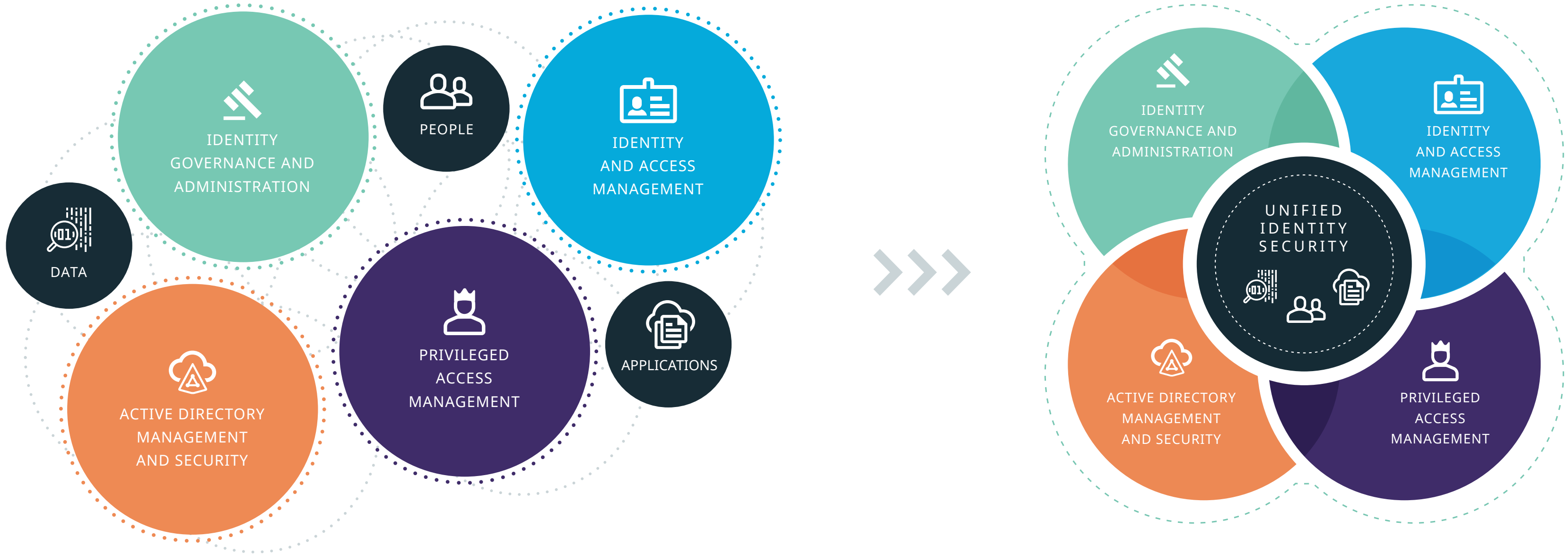
A failure to bridge these gaps could prevent your organization from adapting to changes in user roles/responsibilities, changes IT infrastructure, and to new and developing threats. Properly addressing the gap will contribute to your organization's cybersecurity resilience.

The case for a holistic approach to identity security

Identity security is flexible and can take very different forms depending on user populations and needs, and what resources are connected to and the make up an enterprise. The key to success is to shift from a fragmented to a unified identity-security state.

Many organizations address the key forms of identity security — Identity Governance and Administration (IGA), Identity Access Management (IAM), Privileged Access Management (PAM) and Active Directory Management and Security (ADMS) — in a separate manner. Within each there are often multiple silos to consider and people, applications and data are all distinctly managed. This fragmented state creates a good deal of friction, prevents automation and forces organizations to make best guesses on when and how to manage access rights.

The emerging model is much more holistic with the key forms of identity security addressed together. This means that applications overlap, data silos are emancipated — and people, applications and data are all aligned as one. This unified identity security approach you can correlate all identities, remove friction with better integration, reduce your attack surface, and strengthen your cybersecurity resilience.


IDENTITY GOVERNANCE AND ADMINISTRATION
PEOPLE
IDENTITY AND ACCESS MANAGEMENT
DATA
ACTIVE DIRECTORY MANAGEMENT AND SECURITY
PRIVILEGED ACCESS MANAGEMENT
APPLICATIONS
IDENTITY GOVERNANCE AND ADMINISTRATION
IDENTITY AND ACCESS MANAGEMENT
UNIFIED IDENTITY SECURITY
ACTIVE DIRECTORY MANAGEMENT AND SECURITY
PRIVILEGED ACCESS MANAGEMENT

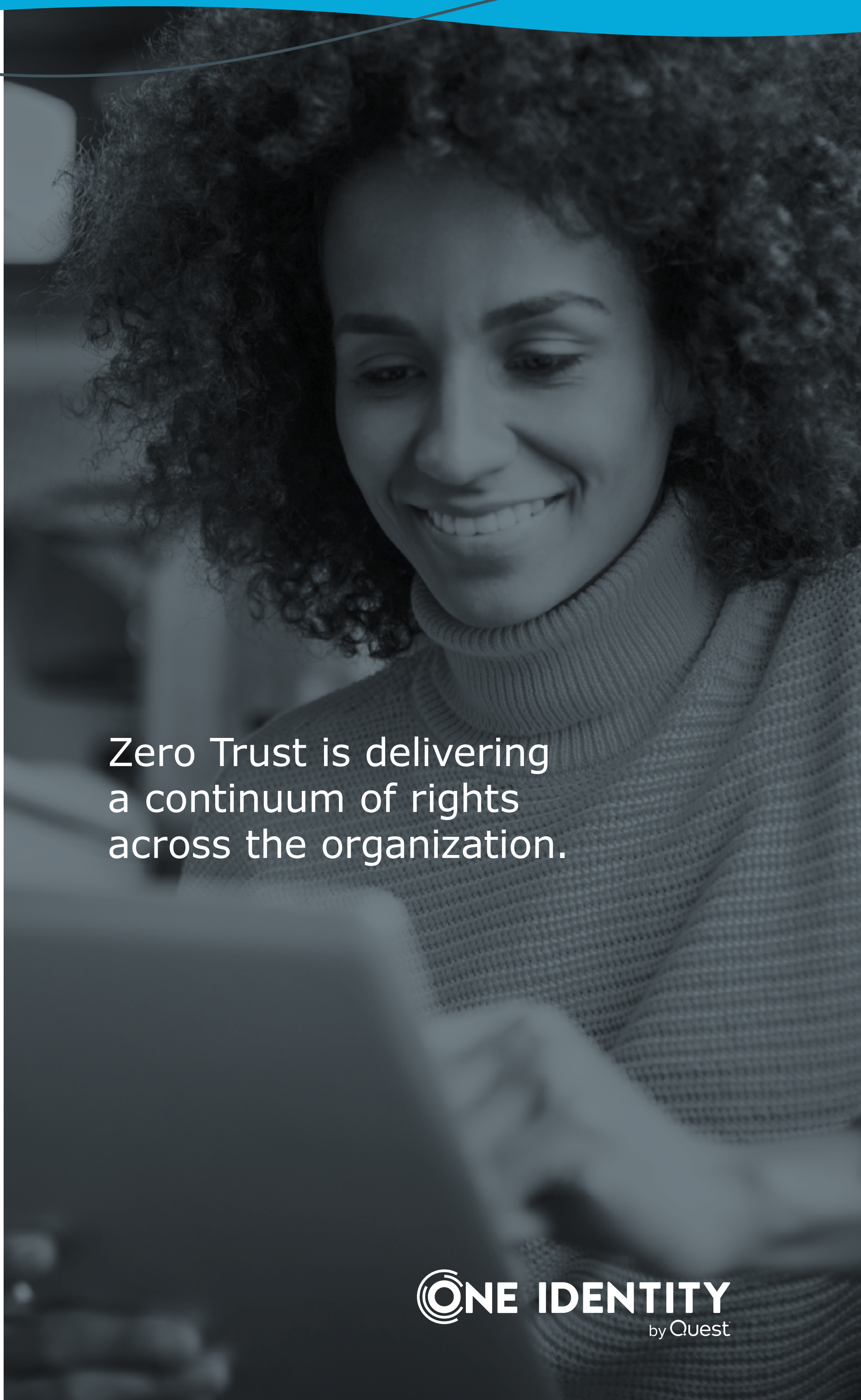
Unified identity security as a core building block for Zero Trust

By now, it’s largely understood that Zero Trust is proven model for implementing robust and selective security. It eliminates vulnerable permissions, unnecessary and excessive access in favor of specific-rights delegation and provisioning with granularity. Shifting from a fragmented to a unified state for identity security allows organizations to take a giant leap forward in delivering on this promise.

Zero Trust success starts with casting the net wide enough. This means focusing not just on people but also on machine identities and ever-expanding accounts as organizations move to a multigenerational, hybrid and edge, IT landscape. If you draw the circle too small, you stand to leave the side door open to bad actors. Unifying your identity security strategy helps ensure you avoid this issue.

A second key element of Zero Trust is delivering a continuum of rights across the organization. With added visibility and insights available, security professionals can more quickly and efficiently add, remove and adjust privilege just in time. In doing so, they can control user access to only what’s needed for his or her job, and only at the right moment – while eliminating error-prone manual processes and heavy IT involvement.

Finally, a key element of Zero Trust is adaptability, which is enabled with a unified identity security strategy. By leveraging holistic approach that includes contextual awareness and behavior analytics, organizations can more quickly and efficiently anticipate, detect and take corrective actions that address emerging threats.



Zero Trust is delivering a continuum of rights across the organization.

ONE IDENTITY by Quest

Best practices for unifying your approach to identity security

Technology can dramatically improve an organization’s chances of success in unifying identity security, but what should security professionals look for in a solutions provider to optimize their outcomes? Below are five must-haves as you consider alternatives:

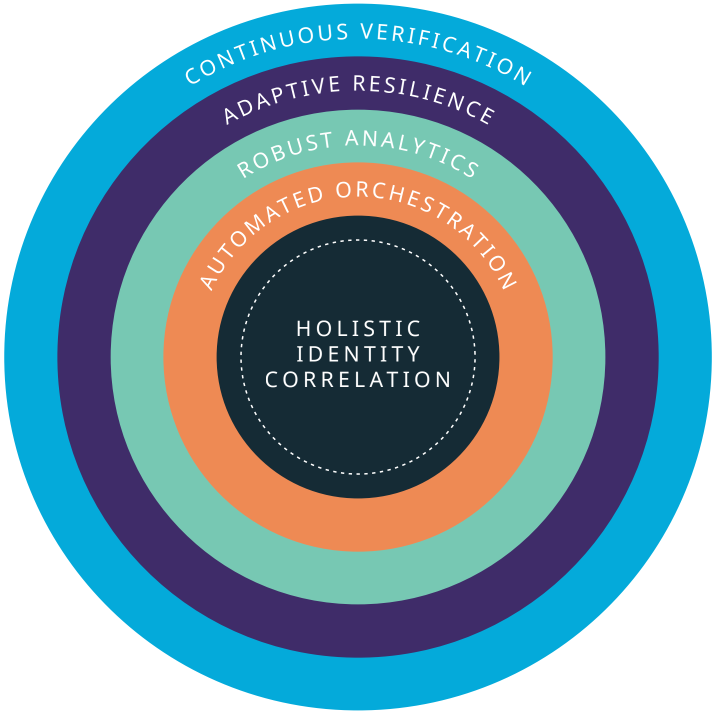
1. **Holistic correlation:** First and foremost, organizations will need end-to-end unification of all identities and accounts to optimize visibility and to make optimally informed decisions.

2. **Automated orchestration:** A second core element of a unified identity security strategy is frictionless governance, across identity and privilege. This allows you to drive efficiencies at scale.

3. **Robust analytics:** Given the breadth and evolving nature of identity security, organizations need solutions that deliver the level of insights necessary to anticipate, detect and take corrective actions on emerging threats at scale.

4. **Adaptive cybersecurity resilience:** With a recognition that the threat landscape and the enterprise are no longer static, cybersecurity professionals should have the ability to quickly pivot as needed and future proof their investments.

5. **Continuous verification:** Unified identity security is most successful when you can verify everything before access is granted. Technology enriched with situational awareness, session monitoring, and behavior analytics will help deliver.



Key problems solved with unified identity security

So far, we have outlined the high-level challenges and benefits of pursuing a unified approach to identity security. But what are specific uses cases cybersecurity leaders can expect with such a strategy? Below is a sampling of common outcomes:

Key Problems	Use Cases	Outcomes
Secure the organization: **Protect your people, applications and data**	• Zero Trust: Protect at scale and reduce risk of breaches by building an adaptive Zero Trust framework • Privileged Remote Access: Ensure remote workers and contractors can securely access critical information, without VPN friction • Endpoint Privilege Management: Unify endpoint security for AD/Azure AD, Unix/Linux, and Windows and macOS desktops • Privileged Analytics and Session Termination: Detect risk in your privileged users and prevent damage to your organization • Hybrid AD Management and Security: Reduce IT involvement in provisioning tasks and eliminate manual errors • Privileged Security for AD/Azure AD: Secure your internal environment as tightly as the perimeter to protect your critical and often-targeted assets • Password Vaulting: Simplify password management and protect privileged credentials	• Eliminate vulnerabilities and risk • Implement Zero Trust • Prevent breaches • Unify identities across cloud and on-prem environments • Secure privileged access
Drive operational efficiencies: **Centralize security processes**	• Privileged Access Governance: Close the policy and security gaps between privileged access and standard-user identities • Active Directory Management and Security: Secure and manage users and groups, and control administrator access via delegation • Active Directory Bridging: Unify policy-based management across all your operating systems and platforms • Mergers and acquisitions: Smoothly adapt to changes, such as workforce actions and pandemics, that typically require significant manual intervention	• Unify identity management policies and processes • Drastically improve efficiency • Control access to all resources, systems and platforms • Automate common tasks to optimize IT-staff work focus • Enjoy effortless joiners/movers/leavers processes

Key Problems	Use Cases	Outcomes
Address compliance and audit requirements: **Manage your identity sprawl and prove policy adherence**	• Identity governance: Ensure policies are enforced, user access is managed in accordance with requirements, and be able to show proof • Agentless session auditing: Protect your most critical resources and users with automated recording and analysis. Plus, support forensic investigations and satisfy compliance requirements for privileged access • Immediate compliance reporting: Get real-time reporting capabilities on compliance measures for all users and resources across your enterprise to satisfy auditors and compliance requirements	• Satisfy auditor demands for permission-related information • Minimize and eliminate risk from identity centric policy violations • Create reliable audit trails for all privileged-session activity • Enable security teams to search for specific events and replay privileged sessions • Meet compliance needs for monitoring privileged access
Secure your digital transformation: **Protect identities while you increase functionality and access**	• DevOps security orchestration: Secure DevOps pipelines with identity-centric security • Application governance: Streamline application-access decisions and enable line-of-business managers to make informed decisions • RPA security optimization: Manage risks associated with sprawling RPA identities • Complex environment management: Reduce administration overhead of heterogenous environments to drive security, speed and decision making	• Seamlessly manage your hybrid environment • Securely adopt RPA practices • Make DevOps secrets easy to use • Increase accountability for employees and contractors • Reduce errors, increase security, optimize efficiency and minimize complexity

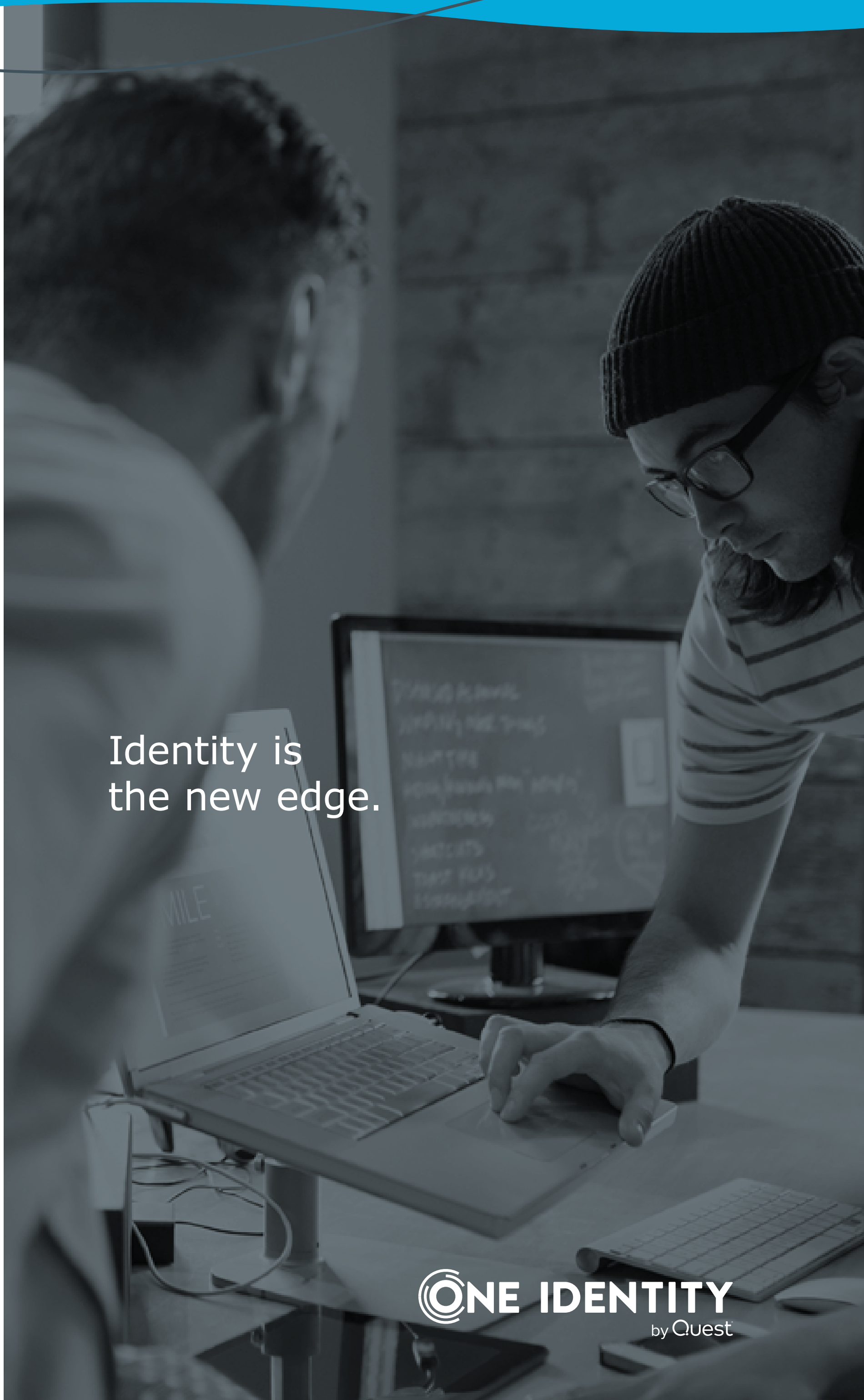
Conclusion

Powerful forces are at work, and a rapidly evolving business and IT landscape contribute to a proliferation of identities. This identity sprawl is compounding daily. It creates a very real set of risks that cybersecurity professionals must take seriously. It is time to stop managing cybersecurity in a fragmented manner.

By taking a holistic approach to managing access rights, CISOs can close a critical cybersecurity exposure gap, foster increased cybersecurity resilience for their organization, and take an important step in delivering on the promise of Zero Trust that is quickly becoming an enterprise imperative.

Identity is the new edge. A unified identity security strategy is the way to combat modern attack methods and take your organization into the future.

Now, when your director of IT security calls, you'll be confident that you have the information to immediately assess the status of your identity security and what actions have been taken on your network.



Identity is
the new edge.

ONE IDENTITY
by Quest

About One Identity

One Identity delivers unified identity security solutions that help customers strengthen their overall cybersecurity posture and protect the people, applications and data essential to business. Our Unified Identity Security Platform brings together best-in-class Identity Governance and Administration (IGA), Identity and Access Management (IAM), Privileged Access Management (PAM) and Active Directory Management and Security (ADMS) capabilities to enable organizations to shift from a fragmented to a holistic approach to identity security. One Identity is trusted and proven on a global scale – managing more than 250 million identities for more than 5,000 organizations worldwide. For more information, visit www.oneidentity.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

ONE IDENTITY by Quest