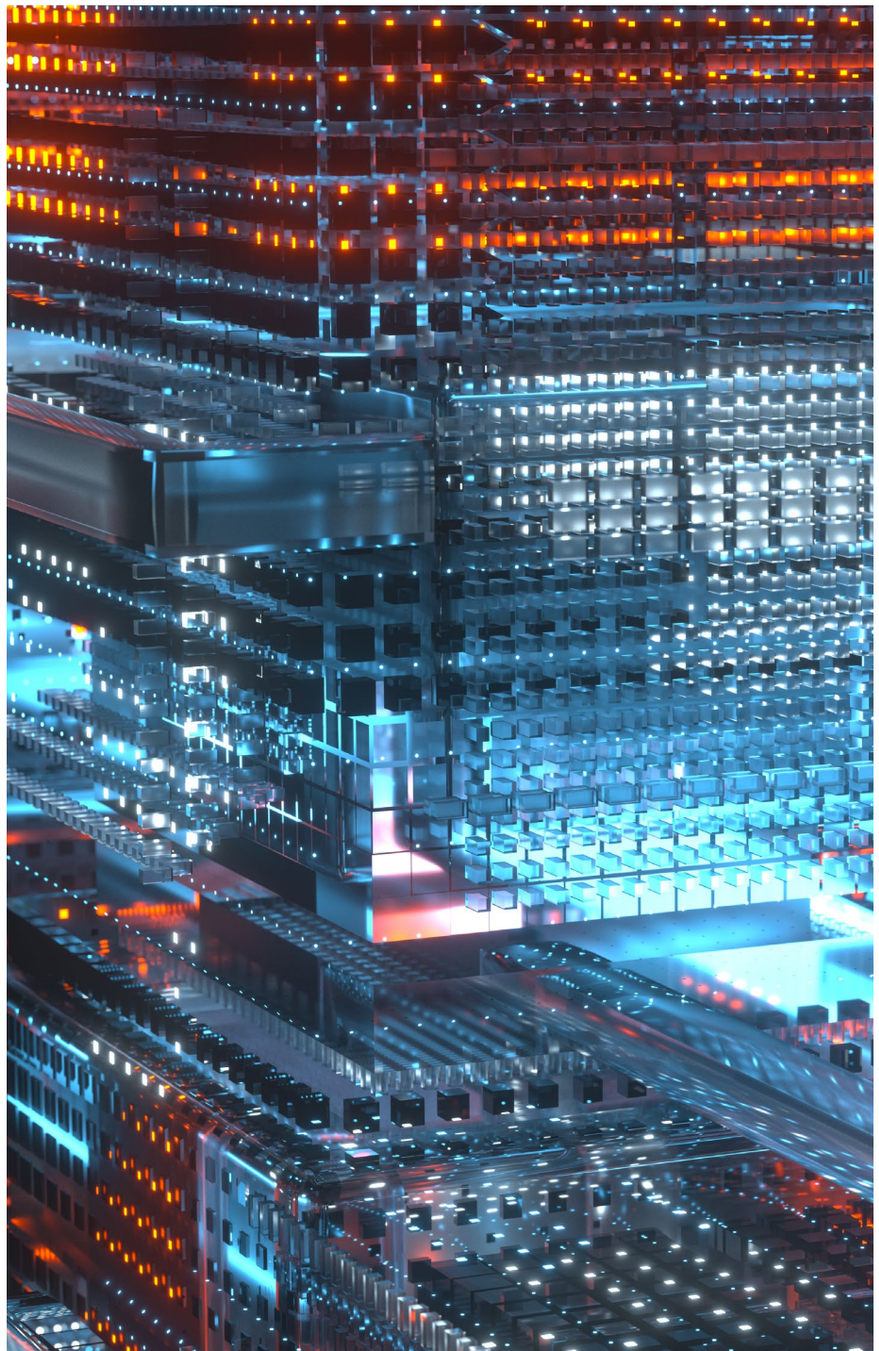
Remediant

PRIVILEGED ACCESS AT THE SPEED OF BUSINESS

Agility, Security and Optimizing the Principle of Least Privilege at Scale

"FORRESTER ESTIMATES THAT 80-PERCENT OF CYBER ATTACKS INVOLVE ABUSE OR MISUSE OF PRIVILEGED CREDENTIALS."



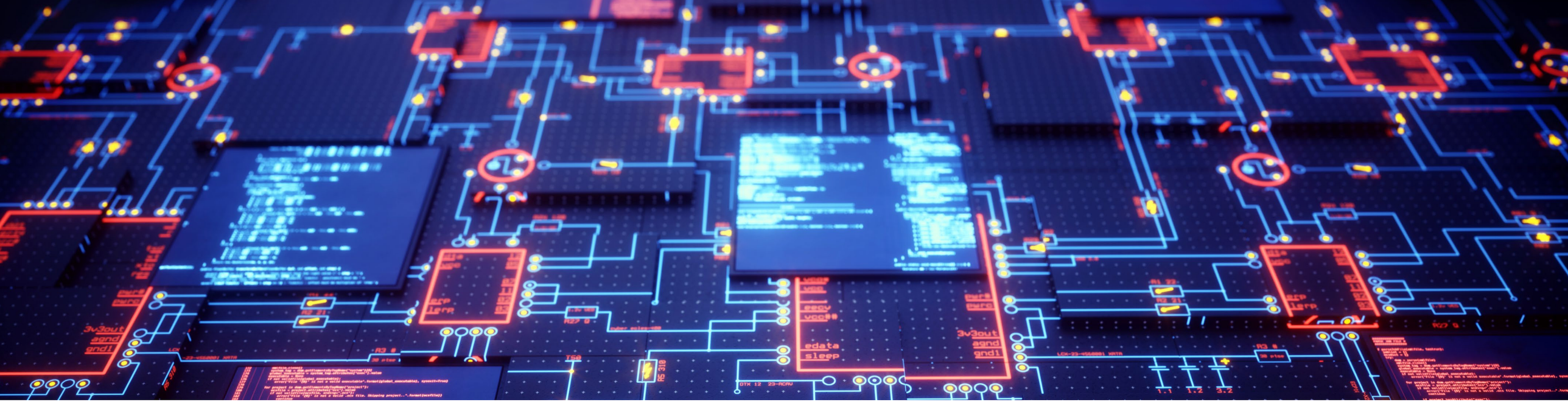
Keeping networks secure is never easy. But the task is especially hard for the modern enterprise operating at scale with a mix of cloud and on-premises solutions that expands attack surfaces and cyber risk. What's worse, many enterprises scale operations without fully evolving their access management systems to match this newly complex — and dangerous — digital landscape. 78% of organizations surveyed in the *2018 Enterprise Management Associates Privileged Access Management Research Report* indicated that they would be adopting a comprehensive PAM solution in the near term.

The result is an Achilles heel — a vulnerable blind spot at the heart of a growing company — that gives malicious actors the keys to your entire kingdom of otherwise impressive resources and capabilities. Indeed, Forrester estimates that 80-percent of cyber attacks involve abuse or misuse of privileged credentials.

In 2016, Uber was breached when hackers exploited employee credentials that had been published to GitHub in error. By accessing these privileged accounts, they were able to steal data from 57 million Uber users and drivers. The hackers then leveraged this personal data to hold Uber for ransom to the order of $100,000, which the company secretly paid out at the time.

More recently, Reddit was the victim of an August 2018 cyber attack — when hackers compromised multiple employee accounts through the company's cloud and source code hosting providers. While the hack itself wasn't devastating in nature, it highlighted once again the importance of safeguarding privileged accounts.

Organizations clearly need better privileged access management and protection at scale.



NEW CHALLENGES & OPPORTUNITIES AROUND ACCESS MANAGEMENT AT SCALE

THE BAD NEWS

THE RISK IS NOW MUCH GREATER

Due to expanded attack surfaces

THE GOOD NEWS

THE RISK IS NO LONGER NECESSARY

Provided you evolve your approach to privileged access into one of dynamic, real-time access management at scale

In a previous era, broad network access was written off as a *necessary risk* for innovators to easily collaborate on relatively sheltered systems. Today, it's a very different picture:

- The bad news is *the risk is now much greater* due to expanded attack surfaces.
- The good news is the *risk is no longer necessary* — provided you evolve your approach to privileged access into one of dynamic, real-time access management at scale.

The key to PAM today is to embrace highly-scalable solutions that leverage multi-factor authentication and dynamic privileged access to meet compliance requirements *and* minimize the impact to ongoing operations.

SCALING THE "PRINCIPLE OF LEAST PRIVILEGE"

Any successful approach to advanced PAM involves continually managing vulnerabilities by controlling administrative use, assignment and configuration, together with optimizing what's known as the Principle of Least Privilege (POLP). Excessive privileges are the malicious actor's playground and a dream come true — and the notion behind the POLP is to limit access only to what a user or developer really needs, and only for the specific period of time that need exists.

Unfortunately, while the POLP concept goes back decades, its application has not always been strategic — slowing down business and fraying the nerves of users in search of legitimate access. Because of this, many organizations consider the Principle to be a nice idea that — when put into practice — typically does more harm than good.

The answer is not to do away with POLP, but to do it right. Specifically, it should be applied in the modern enterprise as part of a fully dynamic approach that assigns privileged access solely to the endpoints the administrator needs, and only for a specific time. The approach should be so automatic, real-time and scalable that it becomes both secure and frictionless for developers and users. In short, we need to *apply the Principle of Least Privilege in the manner of most impact.*

"...LIMIT ACCESS ONLY TO WHAT A USER OR DEVELOPER REALLY NEEDS, AND ONLY FOR THE SPECIFIC PERIOD OF TIME THAT NEED EXISTS."

3 GUIDELINES FOR SUCCESS

Establishing strong and effective PAM is easier said than done. Considering stolen administrator accounts continue to be the #1 method attackers use to steal data, one could argue existing PAM solutions might not be rising to the challenge. But thankfully, we can look to a few key guidelines to shape our work in forging a new path in the world of privileged access:

- ***Utilize the user's own account for privileged access — not a generic or shared account that creates audit, traceability and compliance challenges.***
- ***Make the tool extremely easy to use, including a responsively-designed web interface and API-first architecture that is easy for administrators, DevSecOps, operations and information security teams to manage.***
- ***Without installing agents, continuously scan for changes in privileged access across the enterprise to bring a new level of insight and control over privileged access.***

By following these guidelines, we strengthen security in the "when, not if" world of modern cyber threats. Even in cases where administrator usernames or passwords are stolen, this zero-privilege baseline for protected endpoints ensures that compromised accounts cannot be used to access systems or move laterally through the network.

THE ROAD TO IMPLEMENTATION

There's no single way to go about implementing next generation privileged access management at scale. Much will depend on specific industries, business problems and enterprise architectures. That said, any successful approach will likely include several key characteristics:

AGENTLESS

Cloud workloads, in particular, are ever-changing and ephemeral — many go without protections because they're only designed to stay around for a few minutes. Amid this reality, any privileged access management that relies on installing software or tools will never keep up. Your PAM solution must rely on agentless, continuous monitoring for real-time adjustments to fast-changing circumstances.

DYNAMIC ACCESS MANAGEMENT ACROSS THE ENTIRE DEVOPS LIFECYCLE

The early stages of software or product development may require lots of collaboration and admin rights. But if loose privileges go into a production environment, security problems go there too. Your PAM solution should be dynamic across the entire DevOps journey — from the earliest stages of coding, to testing and delivery.

AUTOMATION

Many companies have 10,000 or more endpoints (servers, workstations, virtual machines, laptops, etc.). That means you need a PAM solution that includes automation and controls that operate at scale. Without such capabilities, your solution won't be able to run effectively and in real time. Ultimately, security gaps will continue to persist.

CAPACITY FOR MANAGING ACCESS ON NON-HUMAN ACCOUNTS

Not every request for access comes from a human being. Consider the admin rights your backup software and servers need in order to save and store data. Similarly, vulnerability scanners need admin rights to apply patches and updates throughout the enterprise. Your PAM solution should be able to address these non-human accounts with the same dynamic, real-time efficiency it applies to developers, users and other people in the enterprise.

ABILITY TO MANAGE ACCESS REGARDLESS OF AUTHENTICATION METHOD

Particularly as enterprises move away from passwords and other outdated, vulnerable methods of authentication, your PAM solution should work with any form of authentication — including newer, more secure, techniques like biometrics, facial recognition and security tokens. Not all PAM solutions have this flexibility. But in an era where the FIDO alliance is fueling new methods of authentication and enterprises are catching on to these new methods — you should make sure your PAM approach is agnostic on authentication.

“...ENSURE THAT YOUR PATH FORWARD IS GUIDED ... BY A DEEP UNDERSTANDING OF THE FUNCTIONAL AND SECURITY FACTORS IMPACTING THE ENTIRE DIGITAL LANDSCAPE...”

REALIZING THE GOAL OF BETTER PRIVILEGED ACCESS MANAGEMENT

Many of the insights shared in this eBook come from Remediant’s extensive experience innovating dynamic and scalable privileged access management across complex cloud and legacy environments — including very large workloads and mission-critical settings like Lockheed Martin, the Lansing Trade Group and other enterprise clients.

Ultimately, whether you take on the job yourself or look to a trusted partner, reevaluating your approach to distributing, using and protecting privileged access across your enterprise environments is critical to shrinking your organization’s attack surface area and closing compliance gaps. Ensure that your path forward is guided not just by leading practices in privileged access management, but also by a deep understanding of the functional and security factors impacting the entire digital landscape.

Particularly as businesses increasingly reach both across and outside the four walls of the organization, PAM should remain a central tenet to your information security strategy so you can confidently manage your ecosystem and speed business innovation - today and into the future.

Remediant

For more information, contact us at info@remediant.com

www.remediant.com (415) 854-8771

8/23/18