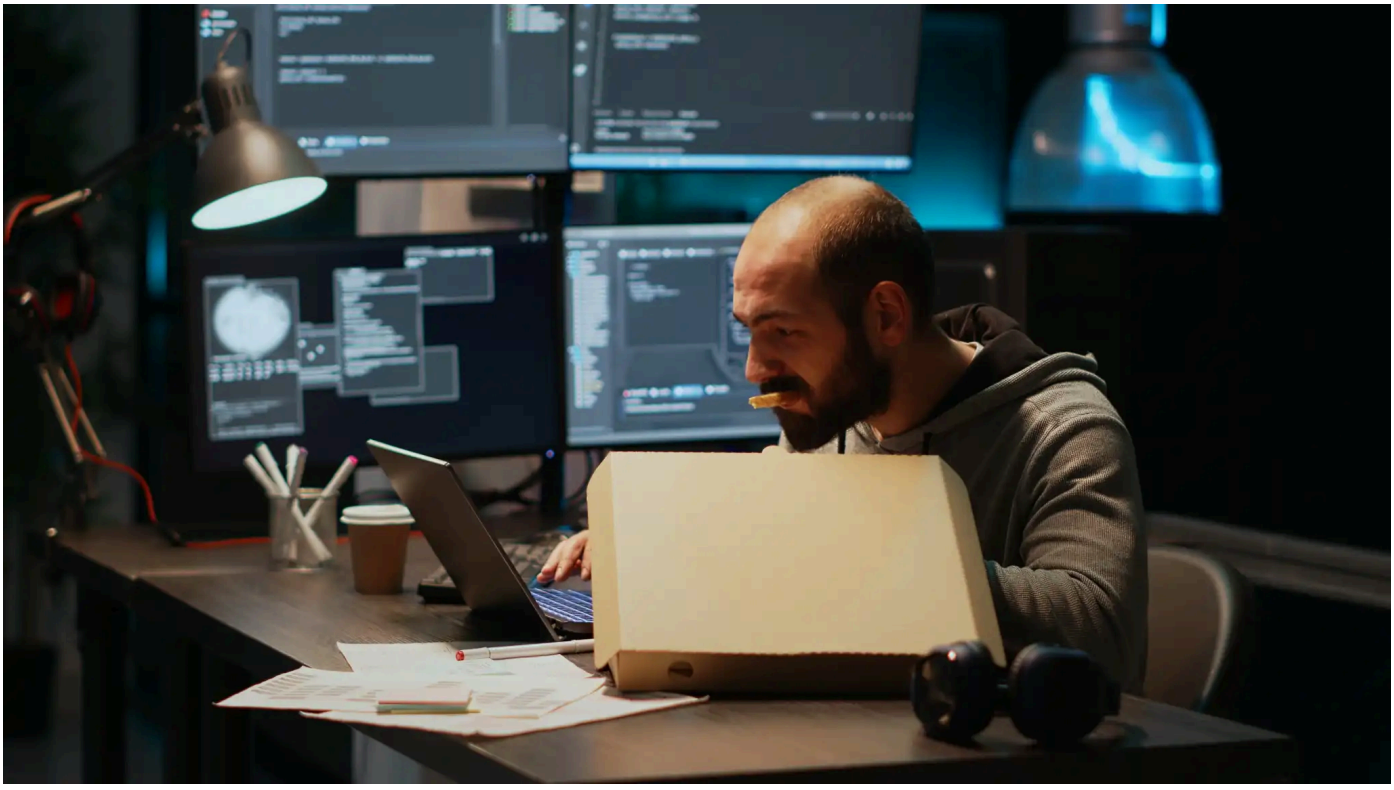
by **Evan Schuman**
Contributor

Always-on privileged access is pervasive — and fraught with risks

News Analysis

Jan 28, 2026 • 7 mins

91% of users log in at their highest level of privilege, which cyber experts see as a symptom of lax IT governance, laziness, and increasingly complex IT environments — and the harbinger of a PAM paradigm shift as NHIs rise.



Credit: DC Studio / Shutterstock

Privileged access management (PAM) has always been about ensuring least privilege. But the nature of enterprise cybersecurity — on top of the complexity of system operations — has prompted far too many users to log in at the highest possible privilege and stay there, even when most of their tasks do not require it.

One recent study [https://www.csoonline.com/article/4114758/enterprises-still-arent-getting-iam-right-2.html] put the percentage of end-users logging in at their highest level of privilege at 91%.

Sanchit Vir Gogia [https://greyhoundresearch.com/svg/], chief analyst at Greyhound Research, sees the widespread use of unnecessarily high privileges as the result of years of enterprise tech governance neglect.
"Enterprises are running complex, interdependent technology estates where privileged access underpins stability, recovery, and continuity," he says. "In many environments, privileged access was granted years ago to support systems that no longer have clear owners, clean documentation, or modern authentication paths. That access now props up integrations, batch jobs, recovery scripts, vendor tooling, and fragile automation chains."

Moreover, Gogia sees enterprises maintaining this status quo on privileges because reining it in "feels less like tightening security and more like introducing existential operational risk."

"They are choosing predictability over disruption," he explains. "Always-on privilege becomes the safest option in environments where architectural certainty no longer exists. It accumulates quietly over time as systems evolve faster than governance models. Mergers, cloud migrations, outsourcing, platform layering, and emergency fixes all leave behind privileged identities that nobody revisits. Over years, this creates an estate where privilege is deeply embedded into how work gets done."

Because of that complexity, Gogia says, always-on becomes not just the easiest tactic, but the default one.

"Enterprises often fall back to permanent privilege because it works," he says. "It keeps pipelines running, integrations stable, and systems responsive. Vaulting credentials does not solve the problem if those credentials never expire. Zero trust principles are sound, but their implementation frequently assumes a cleanliness that enterprise estates simply do not have. This mismatch explains why many organizations buy **PAM tools** [https://www.csoonline.com/article/572787/7-top-privileged-access-management-tools.html], deploy them partially, and quietly allow exceptions to proliferate until the exception becomes the norm."

As a result, PAM — and **identity access management (IAM)** [https://www.csoonline.com/article/518296/what-is-iam-identity-and-access-management-explained.html] — has become misaligned with how modern enterprise systems operate, Gogia says.
"Many tools still assume relatively static infrastructure, limited identity volumes, and manual intervention points," he notes. "Modern enterprises operate dynamic, ephemeral environments where workloads spin up and down constantly, identities are created programmatically, and access requirements change in real-time."

The perils of persistent privilege

Robert Kramer [https://moorinsightsstrategy.com/team/robert-kramer/], vice president and principal analyst for Moor Insights & Strategy, agrees that excessive credentials are caused by decades of lax IT governance.

"They are stuck in legacy habits, stuck in their legacy operational ways," Kramer says. "There should be a shift to more of a just-in-time model. Barely 1% of organizations have implemented that."

The executive overseeing the 91% report — **Charles Chu** [https://www.linkedin.com/in/charleshchu/], general manager for IT and developer products at CyberArk — said staying logged in at the highest level certainly has a cybersecurity risk, but it also introduces the IT risk of massive system damage.

An accidental typo, for example, could cause massive damage if the typist is logged in at the highest level, Chu contends. "I could fat finger something and delete it by accident. Is it really so onerous to log in or out of something?"

That last question is not rhetorical. Chu suggests that some PAM packages are indeed too difficult to use, therefore causing user friction. "If the PAM tool itself is onerous to use, [end-users] will find ways to bypass it."
JR Kunkle [http://kunkleconsulting.net/owner], president of Kunkle Consulting and former risk consultant with Deloitte & Touche, agrees about the typo risk. "Most interruptions in computers are due to errors or mistakes," he says. "IT staff using an admin-level [privilege] can cause a production outage."

But Kunkle, who also worked as an IT manager with Limited Brands and Honda, says defaulting to high privilege access can also undermine legal, compliance, and privacy efforts. "If the admin looks at sensitive data [that the admin was not supposed to see], it's pretty easy for them to cover their tracks by erasing the access logs."

Most observers, however, put the blame of excessive credentials on IT pros themselves. "It is negating the controls that they have put in place. You could take down an entire company through carelessness or fat-fingering," says **Justin Greis** [https://acceligence.com/talent/profiles/justin-greis/], CEO of consulting firm Acceligence and former head of the North American cybersecurity practice at McKinsey. "It's just human nature to take the easy road" and cut corners when it comes to privileged access.

Jason Sabin [https://www.digicert.com/blog/author/jason-sabin], CTO at DigiCert, is more blunt: "If an enterprise [IT worker] uses root, they are an idiot. You can screw up your world. You should never use root. Embrace least privilege. You should never use elevated privileges for ordinary mundane tasks."

Paradigm shift ahead

Forrester analyst **Geoff Cairns** [https://www.forrester.com/analyst-bio/geoff-cairns/BIO20052] **stresses the cybersecurity risks at play** [https://www.csoonline.com/article/3952041/malicious-actors-increasingly-put-privileged-identity-access-to-work-across-attack-chains.html] when organizations do not rein in excessive credential use.
"Persistent standing privilege, yes, I think that is rampant," he says. "It is something that attackers can target and then leverage to move laterally through systems and create havoc. The elevated privilege makes that all the more impactful."

Yet Cairns sees the hard road ahead in tackling this issue in modern enterprise environments.

"It is a challenging problem to solve in a very complex IT landscape, with on-prem, cloud, SaaS" and it is going to get exponentially worse with "the explosion of non-human identities," including autonomous agents, Cairns says.
Greyhound Research's Gogia agrees that non-human identities (NHIs) are going to make the problem of excess credential use far worse.

"The center of gravity has shifted away from human administrators. The most dangerous and least governed privilege now sits with non-human identities. Service accounts, APIs, cloud roles, CI/CD pipelines, SaaS connectors, automation frameworks, and autonomous systems operate continuously with standing access," he says. "These identities authenticate programmatically, at machine speed, often across environments, and frequently with broader permissions than any individual would ever be granted."

And the increasing proliferation of NHIs engaging with enterprise systems is pushing PAM and IAM toward a paradigm shift.

“Traditional PAM and IAM models were designed for humans who log in, perform tasks, and log out. They struggle when identities never log out,” Gogia says.

“Machine privilege is not an edge case,” he adds. “It is the majority case in modern environments. Enterprises attempting to apply human-style access reviews and approval workflows to these identities quickly discover that governance collapses under scale. This is where always-on privilege stops being a failure of discipline and becomes a failure of design assumptions.”

Identity and Access Management[https://www.csoonline.com/identity-and-access-management/]

Security[https://www.csoonline.com/security/]

Risk Management[https://www.csoonline.com/risk-management/]