

Privilege Creep: Access Gone Wild

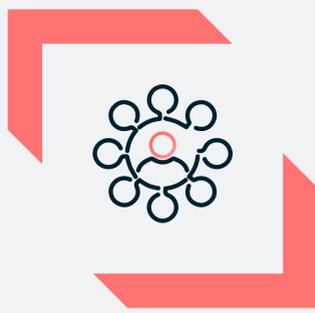
When excessive access goes from convenience to security threat

Privilege creep is the slow buildup of access rights that no one notices—until it's a problem. When users accumulate access they don't need, it creates hidden security risks. A forgotten account here, a shared password there, and suddenly, outside threats have more entry points than they could have imagined. The more unnecessary access floating around, the bigger the risk.

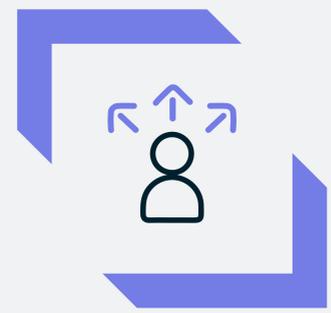
What are the risks of too much access?



Outside security breaches



Malicious insider threats



Negligent employee mishaps

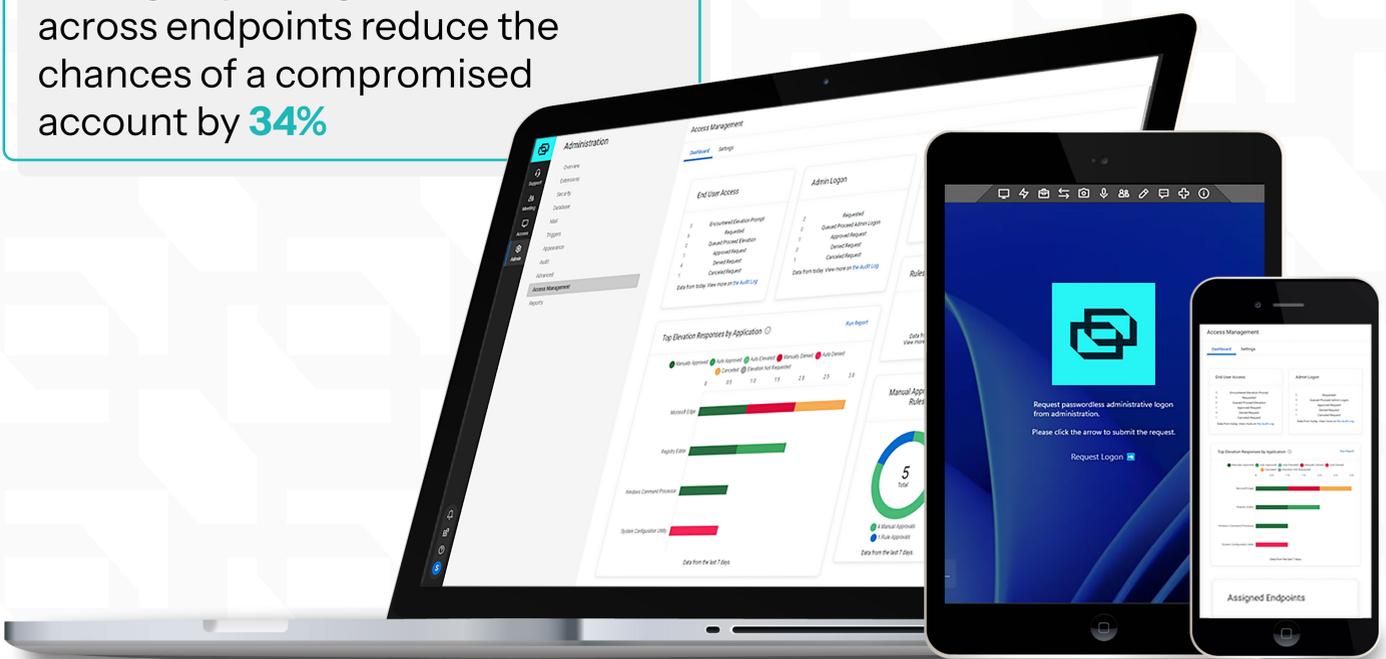
87% of security breaches are due to privileged credential misuse—accidental or otherwise

80% of breaches involve compromised privileged credentials

PAM platforms with centrally managed privileged access across endpoints reduce the chances of a compromised account by **34%**

57% of data breaches involving an insider are caused by inadvertent or accidental employee behavior

Organizations using policy-based controls to define privileged users were **33%** less likely to experience a policy breach



Too much access
= too much risk.
Let's fix that.

Try ScreenConnect Privileged Access for free for 14 days and see how easy it can be to keep access in check. No hassle, no risk—just better security.

screenconnect.com/pam-software/trial