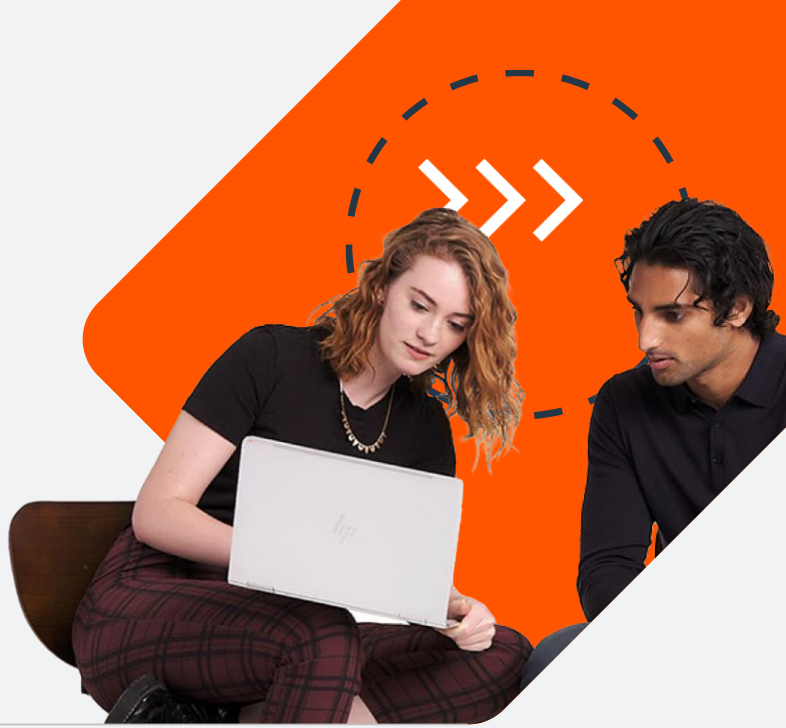




Do you know who has access to your cloud infrastructure?

Overprivilege, data breaches, and noncompliance—it's a lot to manage.



Onboarding users. Offboarding users. Managing vendor access. Remaining compliant. With constant change in your dynamic cloud environment, it's easy for employees and third parties to have privileged access beyond their needs, expanding your attack surface.

Risks of overprivilege

74% of IT decision makers say their company breach involved privileged access credential abuse.¹

Define and control who can access remote systems to reduce overprivilege and potential security breaches.

Forgotten vendor access

58% of companies think it's likely they have suffered a breach due to vendor access.²

Leverage just-in-time and just-enough privilege access to increase security and reduce administrative burden.

Costs of noncompliance

Noncompliant companies receive penalties upwards of \$3.945 billion.³

Track audit data to reduce risk of noncompliance, saving time, resources, and money.

Access all your cloud infrastructure— anywhere— with BeyondTrust and Amazon Web Services (AWS).

[BeyondTrust demo](#)

Sign up for a demo now to see BeyondTrust's Privileged Access Management solution in action.

Do more. Stay secure.

Let BeyondTrust save you time, money, and peace of mind.

¹ Columbus L, *CIOs Guide to Stopping Privileged Access Abuse*, Forbes, 2019.

² BeyondTrust, *Privileged Access Threat Report*, 2019.

³ SumTotal Systems blog, *The Ultimate Cost of Noncompliance on Your Business*, 2021.

