What are paths to privilege?

The security importance of privilege and privileged access is well established, but modern identity protection requires going beyond those basic notions of privilege to find and protect the paths to privilege.

Paths to privilege may be indirect, or otherwise well-hidden from the scans of typical security toolsets. Yet, if found and exploited by threat actors, these paths could fast-track the ability to compromise identities, undermine the integrity of identity infrastructure, and bring an organization to its knees.

Paths to privilege are anything that can be leveraged to gain access to a privilege—a privileged account that could be compromised, a secret that could be used to authenticate, a misconfiguration that allows for elevation of privilege, a VPN vulnerable to a password spray attack that provides access to the entire network, or identity infrastructure that is exploited to grant privilege.

> To prevent misuse of privilege in an environment, you need to understand all the paths to privilege an attacker could exploit.

Why finding paths to privilege is the key to modern identity security

Modern IT systems are complex and contain an ever-growing number of disparate systems, applications, and identities, all of which potentially create new paths to privilege—**paths that are actively being exploited by attackers.**

90%

In the past year, 90% of organizations experienced at least one identity-related security incident.

IDSA. 2024 Trends in Identity Security. May 2024

John Lambert, of the Microsoft Threat Intelligence Center, summed up the central challenge in identity security that is currently tipping the balance in favor of attackers.

His apt description gave rise to the now-popular expression:

"...defenders think in lists. Attackers think in graphs. As long as this is true, attackers win."

– John Lambert

Once you have visibility of paths to privilege, you can begin to apply the principle of least privilege to remove paths that aren't absolutely necessary, and then apply mitigating controls and protections for the ones that are needed. Given the dynamic nature of modern IT environments, this needs to be a continuous process. By focusing on paths to privilege as identities, apps, and systems are onboarded, offboarded, and updated, you can better ensure your identity security posture remains hardened, even as your environment changes.

Why Context Matters

When thinking about paths to privilege and risk, it's important to be aware of the business context. In one organization, having the privilege to access data on a given system might represent potentially business-ending risk due to the high sensitivity of that data. Whereas, in another organization, that same privilege might represent little-to-no risk. Similarly, an account in a test environment might be perceived as low risk, whereas a Domain Admin in the corporate environment is high risk.

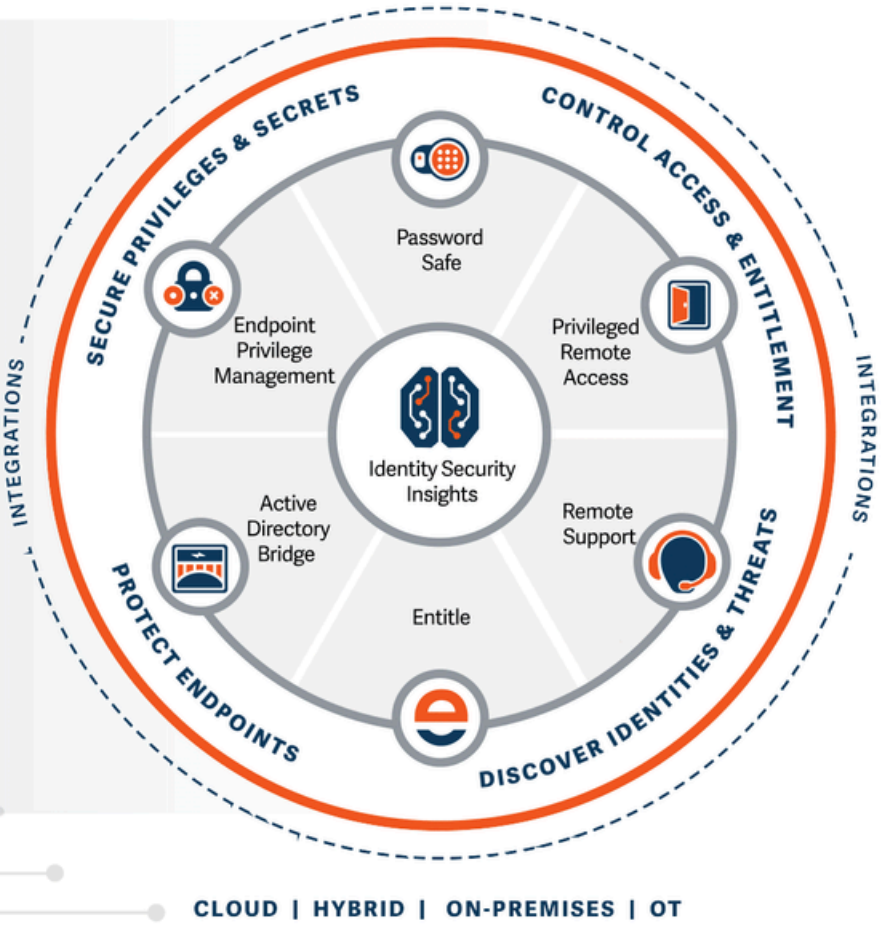
But what happens when a trust relationship exists between the two environments?

In this case, there is a path to privilege from the account in the test environment into the corporate environment. This allows a compromised test account to authenticate and access resources in the corporate environment. These connections and trust relationships have become very common as organizations seek out easy ways to test new systems and migrate them into production environments.

The BeyondTrust Platform

BeyondTrust products integrate with each to offer more protection and greater efficiencies. Rich integrations with third-party toolsets help your organization further maximize existing security investments.

For more information about the BeyondTrust Platform, visit our website.



BeyondTrust is uniquely positioned to protect your paths to privilege and improve your identity security posture.

Holistic Visibility

Illuminate your paths to privilege

Simplified Management

Accelerate least privilege and gain efficiencies

Intelligent Protection

Improve continuously using AI & ML insights