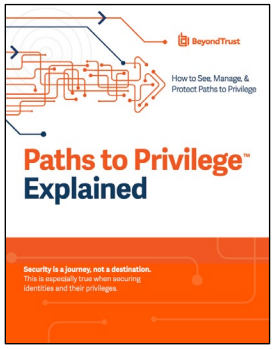


Whitepaper: Paths to Privilege Explained

Thank you for downloading this BeyondTrust Whitepaper. Carahsoft is the Distributor for BeyondTrust solutions available via GSA 2GIT, NASA SEWP V, ITES-SW2, and other contract vehicles.

To learn how to take the next step toward acquiring BeyondTrust's solutions, please check out the following resources and information:

For additional resources:
carah.io/beyondtrustresources

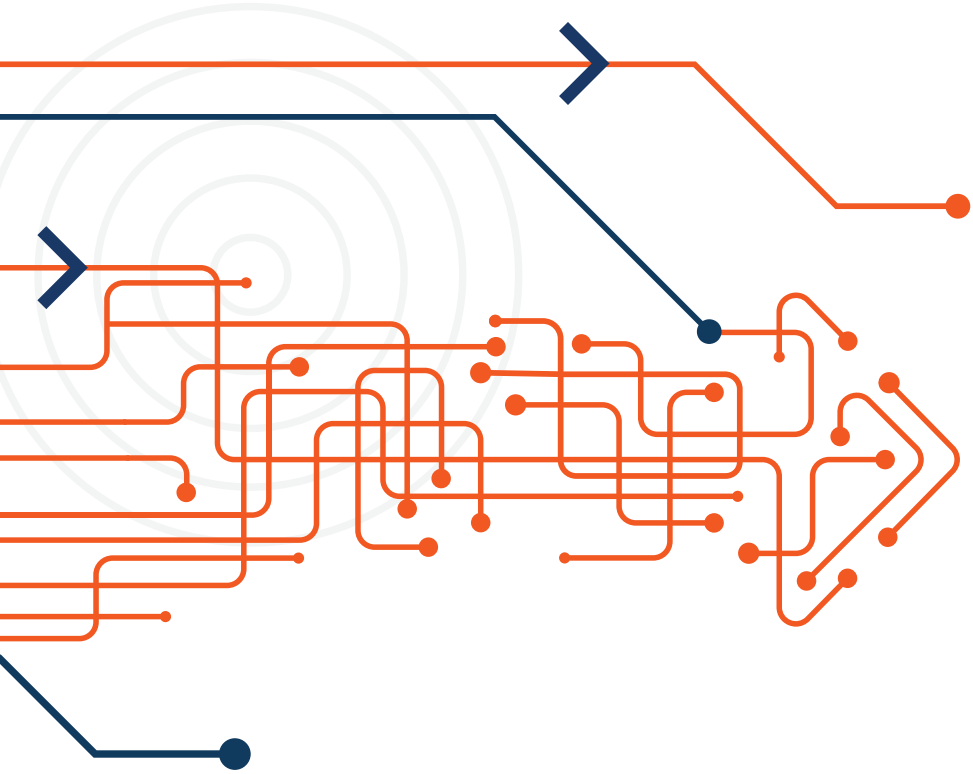
For upcoming events:
carah.io/beyondtrustevents

For additional BeyondTrust solutions:
carah.io/beyondtrustsolutions

For additional Cyber solutions:
carah.io/cybersolutions

To set up a meeting:
beyondtrust@carahsoft.com
(866)-421-4683

To purchase, check out the contract vehicles available for procurement:
carah.io/beyondtrustcontracts



BeyondTrust

How to See, Manage, & Protect Paths to Privilege

Paths to Privilege™ Explained

Security is a journey, not a destination.
This is especially true when securing identities and their privileges.

BeyondTrust

TABLE OF CONTENTS

Microsoft, Internet Explorer, Edge, Windows, Microsoft Office, Windows Server, Azure, Dynamics 365 are trademarks of the Microsoft group of companies.

Introduction

The principle of least privilege and the discipline of Privileged Access Management (PAM) have long stood as IT security cornerstones. Everyone knows privileges are the main target and it's essential to protect them. However, the modern technology and threat landscapes have evolved significantly, and most organizations are approaching the identity security and privilege challenge incompletely because they are overlooking the paths to privilege. **But attackers aren't.**

> To effectively protect identities, you need to go beyond just directly managing privileged accounts to protect how human and non-human identities access privilege.

This means you need to be looking at the identity infrastructure that grants privilege, the policies and groups used to manage privilege, and the connections between identities and accounts that open up paths across different domains (for example, providing paths from on-prem into the cloud). These are all paths to privilege that, if unaccounted for and unprotected, can undermine your organization's identity security—including the identity infrastructure itself.

Read this paper to learn what paths to privilege are, how and why attackers seek them out, and how to look at your environment from the lens of an attacker to better understand and defend your identity landscape. Also learn how the BeyondTrust Platform takes you beyond PAM with the most comprehensive approach to discovering, managing, and protecting paths to privilege.

What is privilege?

Before defining paths to privilege, we need to define what privilege is in the context of identity security.

Privilege is a right granted to an identity that can be used to perform security-relevant operations.

While we often think of privilege in terms of human identities with admin and non-admin user accounts, it's important to highlight that privilege is not binary, and not every privilege is an administrative one.

There are multiple planes of privilege that grant identities access to systems, resources, and data through traditional on-premises privilege models or through roles and entitlements in cloud and SaaS systems.

While organizations often focus on directly assigned administrative privileges, even the privileges assigned to a typical, non-admin user can cause significant harm.

There are multiple planes of privilege that grant identities access to systems, resources, and data.

An ostensibly low-privilege user has the ability to execute code and access data—which can be exploited by threats, such as ransomware, in the event the user is compromised. In the worst-case scenarios, a typical user might be unintentionally assigned a very high level of privilege indirectly as a result of group memberships, misconfigurations, or confusion over what privilege a role allows. Such scenarios might allow that user—or an attacker who has compromised the user—to easily assume a highly privileged role.

Beyond human identities, there is another important type of identity: non-human identities (NHIs). These can outnumber human identities many times over in some IT environments. NHIs (sometimes referred to as machine identities) can be service accounts, system accounts, machine accounts, or application accounts. In general, they are used to allow applications and services to interact with each other.

While NHIs may be granted significant privileges, they often lack the additional layers of protection (MFA, for example) used for human identities. In addition to regular username and password credentials, non-human identities might have API keys, SSH keys, and certificates used for authentication. These might have differing levels of controls applied to them when accessing privilege.

> Credentials comprised nearly 90% of cloud assets for sale on the dark web. And use of valid credentials was the most common initial access vector in cloud security incidents.

IBM Security, 2023 IBM Security X-Force Cloud Threat Landscape Report. Sept. 2023.

When thinking about identity security and privilege, we need to consider all identities, accounts, and privileges. This applies to humans, non-humans / machines, employees, vendors, and other third parties.

Most organizations find themselves managing disparate, siloed systems and having to make use of point solutions focused on specific use cases across the identity fabric. These challenges are further compounded by organizational structures where Identity Access Management (IAM) and security teams are completely separate.

The gaps between these identity silos creates blind spots that prevent the ability to holistically see identities and privilege. Because identity security crosses every domain, we need to view identity and privilege through a cross-domain lens to see the full picture.

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.

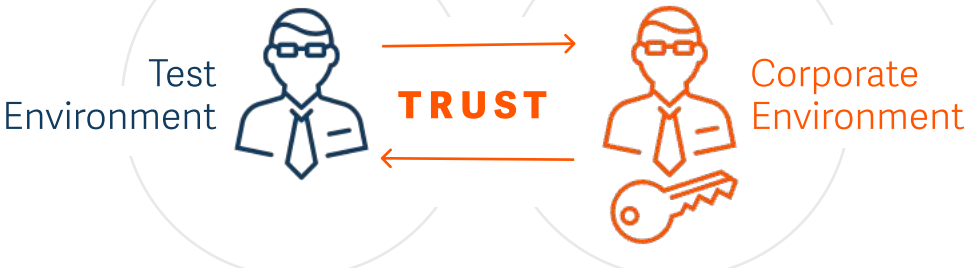
Once you have visibility of paths to privilege, you can begin to apply the principle of least privilege to remove paths that aren't absolutely necessary, and then apply mitigating controls and protections for the ones that are needed. Given the dynamic nature of modern IT environments, this needs to 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.



These connections highlight how attackers win—by looking for the paths to privilege instead of just looking at system boundaries. It's essential to consider all possible paths to privilege from the perspective of an attacker so you can adequately secure the privileged identities in your environment from complex cross-domain routes of attack.

Going Beyond PAM to Protect Privilege

When we think about protecting our organizations, Privilege Access Management (PAM) and the protection of traditional privileged accounts is often top of mind. PAM is an essential foundation of any security program. Organizations typically start by focusing on directly managing privileged human identities.

However, in any modern identity ecosystem, there are many different ways privilege is assigned, accessed, and authorized, and this presents a large identity attack surface.

> To protect privilege, you need to go beyond just managing privileged identities to also protect how identities can access elevated privilege.

Consider Domain Administrator accounts. In a traditional environment, you could follow best practices: limit the number of accounts, implement MFA, and use a PAM solution to provide just-in-time access and to automate credential rotation.

Today, we need to think like an attacker about alternative paths to Domain Administrator access. For example:

Misconfigured certificate templates in Active Directory Certificate Services (AD CS) could provide an attacker a path to authenticate as a Domain Administrator from any valid domain account.

Weak permissions on AD Groups could provide an attacker a path to add themselves to an administrator's group or a group with administrator-equivalent privileges.

Service accounts could have high levels of privilege and be vulnerable to exploitation, providing a path to create a new Domain Administrator account.

Legacy Azure AD (Entra ID) sync agent accounts with Global Administrator privileges could allow a user with access to the sync agent system to capture highly privileged credentials and pivot into the cloud, or change AD memberships.

These paths to privilege are all examples of common attack techniques threat actors leverage for lateral movement and escalation of privilege. While these techniques are commonly used because they exploit indirect paths to privilege, many organizations struggle to find, manage, and protect these paths due to the complexity of their environments and the siloed nature of systems and tooling.

Common Paths to Privilege

Human and Non-Human Accounts

Compromising a human identity is one of the better-known entry points to finding and exploiting privileged access and paths to privilege. An attacker might use compromised credentials to authenticate as the identity and exploit the privileges that account directly holds or can indirectly access. They might also use phishing, software exploits, or malware to execute code as an account to access the privileges. In some cases, an attacker might even use malware on an endpoint that allows them to capture a session token after the user has authenticated using MFA. Achieving such an exploit gives the attacker access to privileges without having to know what the password for the account is, or having to pass MFA.

When an identity has local admin privileges, it opens up a variety of paths to privilege. If a local administrator account is compromised, an attacker can use the account's privileges to capture the credentials of other users logged into the system using common tools, such as Mimikatz. Those credentials could then be used to move laterally, create new accounts locally, access the data of other local users, tamper with endpoint security controls, and elevate to SYSTEM level. This is why removal of local admin privilege is a critical mitigation.

Non-human identities, such as service accounts, present high-value targets because they are often highly privileged, yet lack the MFA controls enforced on human accounts. Using a compromised domain account, an attacker can utilize techniques, like Kerberoasting, to capture the credentials of a service account and access new paths for lateral movement.

These non-human identities can also be exposed in code, configuration files, and poorly secured development pipelines where account credentials are stored in plain text. Again, these are likely to be highly privileged accounts used to perform important tasks, so it is critical to manage and protect the paths to these privileges.

The ability to understand what privileges accounts can access, the risk exposure when accounts are dormant, and which accounts have poor password hygiene or lack adequate controls (such as MFA or conditional access policies), can help you see paths to privilege and the underlying risks an attacker might find and exploit. This is a critical capability for proactively hardening identity security posture, as well as for effectively detecting and responding to attacks.

Exposed Secrets

Many breaches start with an attacker gaining a low-privilege foothold in a network and then searching the environment for secrets that can open new paths to privilege. These paths could be credentials stored in plain text, API keys saved locally in scripts, or certificates stored on network shares. Exposed secrets can provide a variety of cross-domain paths to privilege, allowing an attacker to move from on-prem to cloud and escalate privileges.

For example, storing credentials for an unmanaged privileged service account in a script or configuration file represents a path to privilege that is easy for an attacker to exploit, especially when the credentials are not being rotated. Even if attackers only gain access to a low-privilege identity initially, that access could allow them to conduct reconnaissance in the environment and find exposed secrets that open up new paths to privilege for them.

In recent years, the international cyber-extortionist group LAPSUS$ compromised large enterprises, including Microsoft, Nvidia, Ubisoft, Okta, and Samsung (among others) without flexing any significant technical skillsets. They simply exploited identities and paths to privilege by leveraging off-the-shelf tools for reconnaissance and remote access.

Here are some techniques observed during LAPSUS$ breaches:

- Accessing and scraping corporate Microsoft SharePoint sites to identify secrets stored in technical documentation.
- Accessing local password stores and databases to obtain further secrets.
- Cloning Git repositories to extract API keys.
- Leveraging compromised credentials to access corporate VPNs.

Attackers may also utilize secrets exposed in third-party breaches. For instance, the compromised secrets could be put to use in a targeted attack or in broader password spray and credential stuffing-type attacks (where compromised credentials are tested against a range of popular cloud services).

Cisco and Duo Labs have issued warnings of a growing number of large-scale password spray attacks leveraging commonly used, or compromised, credentials. While these attack techniques are not new, the scale and sophistication have increased. The ever-increasing number of paths to privilege offers attackers a range of options they can leverage in the event they are able to compromise an identity.

Identity Infrastructure

The identity infrastructure provides authentication and authorization for paths to privilege, making it a very desirable target for threat actors. Despite this high level of risk, the monitoring and protection of identity infrastructure itself is often inadequate, and characterized by dangerous security blind spots and gaps.

Identity infrastructure misconfigurations can provide attackers with paths to privilege. For example, common misconfigurations in Active Directory Certificate Services can provide a path for any valid domain user to authenticate as a Domain Admin. Similarly, a privileged Entra Synchronization Account might not have a Conditional Access Policy applied, making it possible to authenticate to the cloud from outside of trusted locations and managed systems.

Identity infrastructure can also be directly exploited. For example, the Scattered Spider group and others have targeted Okta Super Administrator accounts by social engineering the help desk to reset passwords and MFA controls. After the attackers logged into Okta as the Super Administrator, they were able to add their own rogue IdP into the environment, enabling themselves to access applications within the compromised organization.

Identity Infrastructure paths to privilege are often hidden. Disparate identity systems may belong to different teams, the systems may require specialist knowledge to understand, and the system events may not be consumed or understood by the SIEM or security tools.

Having the ability to understand when high-risk misconfigurations exist, and when high-risk changes are made to identity infrastructure, is pivotal to finding, managing, and protecting paths to privilege.

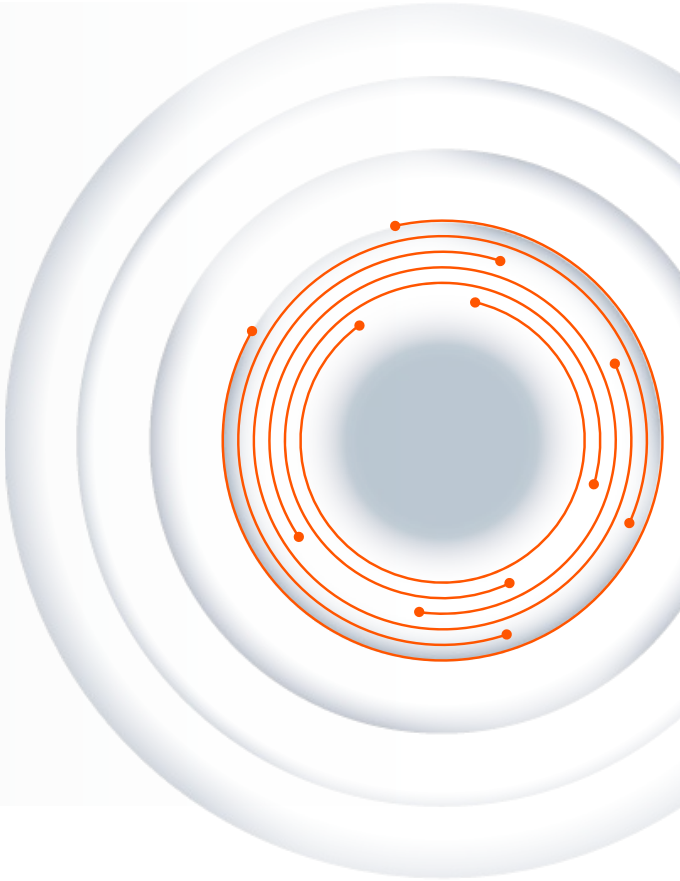
Remote Access

Commonly used remote access solutions, such as VPNs and RDP, can present many paths to privilege because they can open up access to an entire network when all the user needed was access to one system or endpoint. This is particularly true of privileged identities, where the same credentials used to authenticate to the VPN might also be used to authenticate to systems within the network and to perform administrative actions.

This was the case in the 2022 Cisco breach, where the Yanluowang ransomware group compromised corporate credentials within a user's personal Chrome password store and used them to not only connect to the VPN, but also to access systems within the network, create new local administrator groups, and then install further remote access software.

When thinking about paths to privilege for remote access, prioritize least privilege and just-in-time (JIT) access controls.

By providing just the right amount of access and privilege required, and only for the finite moments needed, you can reduce standing privilege, thereby reducing the **"blast radius"** of a potential compromise.



Threat actors, such as LAPSUS$, advertise that they will pay employees to hand over credentials for remote access solutions so they can gain access to systems and the network. This highlights how valuable these paths to privilege are to an attacker.

Even if the compromised identity only has limited privileges, the broad access provided by a VPN offers threat actors the ability to potentially discover vulnerable systems, uncover secrets stored on network shares, and find further privileges and paths to privilege they can exploit to achieve their objectives.

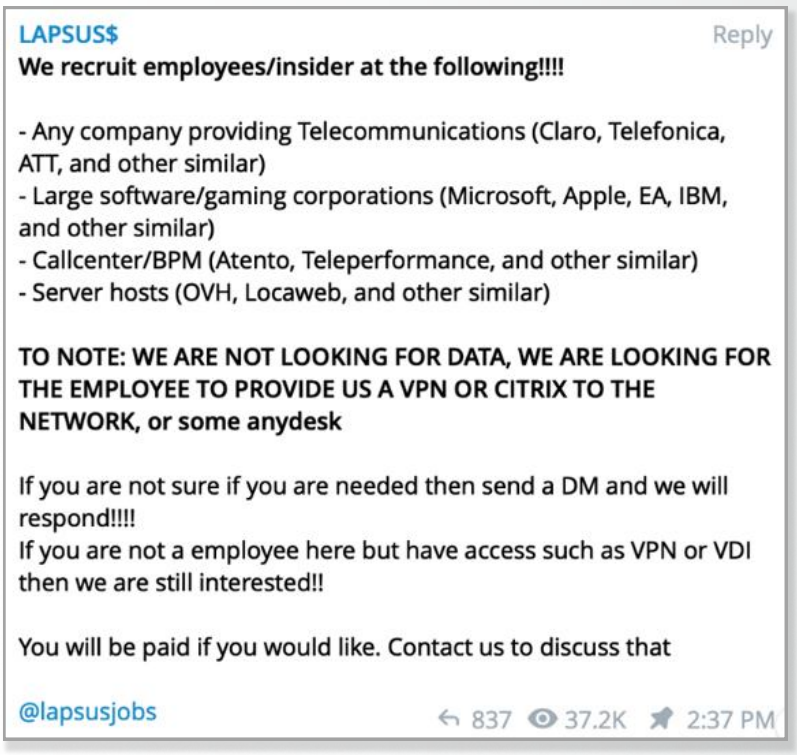


FIGURE 1
LAPSUS$ post on Telegram channel recruiting employees

Excessive Privileges

Privilege creep is all too common. Privileges are often granted on a permanent basis (standing privileges), even if they are only needed once. As users change roles or take on new projects, their identities can continue to collect privileges that are never removed. In extreme cases, the highly privileged identities of former employees can exist in a dormant state. These offer no value to the business because they are no longer (legitimately) used, but they create plenty of risk in the event of compromise.

In the race to the cloud, we see an abundance of privilege granted through roles and entitlements, often with little knowledge or consideration of the extent of their reach. This problem is further complicated by the thousands of different, granular privileges that can be granted in the major cloud platforms.

Number of IAM Permissions & Actions
BY CLOUD PLATFORM

*AWS, Azure, and Google Cloud data is updated regularly. These numbers were captured July 31, 2024.

The adoption of more cloud applications was the **#1 factor driving an increase** in the number of identities.

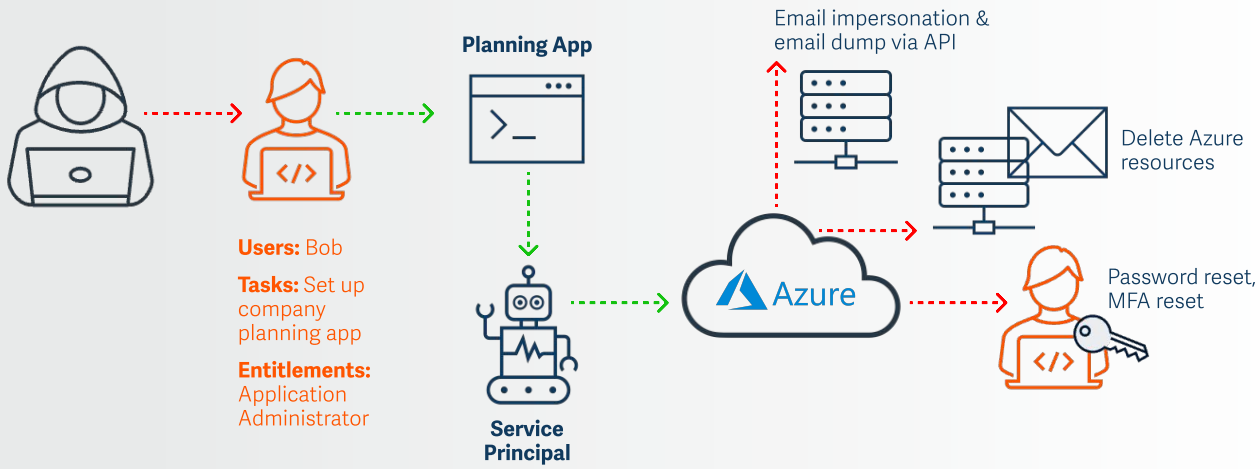
- IDSA. 2023 Trends in Securing Digital Identities. June 2023.

1. https://aws.permissions.cloud/
2. https://azure.permissions.cloud/
3. https://gcp.permissions.cloud/

Several high-profile attacks, including the infamous Midnight Blizzard attacks against Microsoft, have succeeded because of the hidden connections and excessive paths to privilege that arise from creating and managing human and non-human identities in the cloud.

A common example of paths to privilege in Entra is an identity with control over an OAuth application. Even if the identity isn't directly privileged, it has a path to the privileges that are granted to the application they control. In many cases, applications are granted high levels of cloud privilege, presenting a path from a seemingly low-privileged identity to Global Administrator in the cloud via an application and its service principal.

Paths to Privilege in Entra



In many cases, these applications were set up for legacy cloud migration projects, which required high levels of privilege at the time, but are no longer needed. In other cases, they were simply over-privileged due to a lack of understanding of what was required. In any case, these privileges provide a tempting target for attackers looking to pivot into the cloud. From the cloud, the attackers can use these paths to elevate their privileges to access mailboxes, data stores, and other identities through Entra ID.

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:

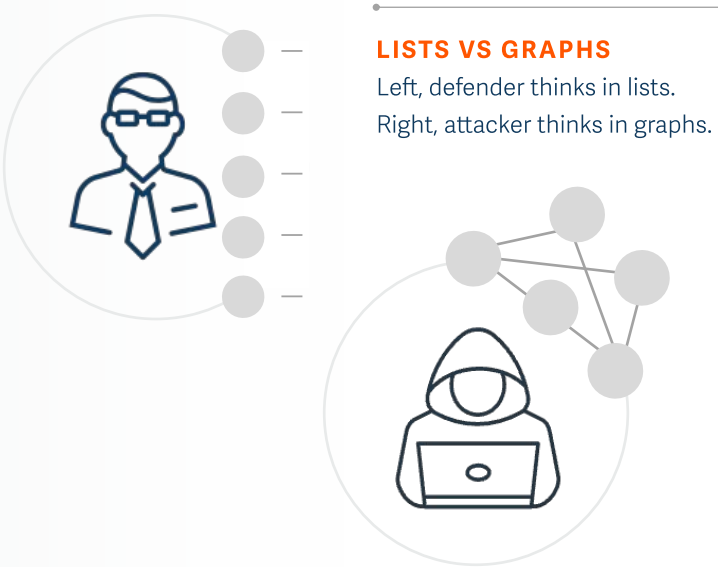
"...defenders think in lists. Attackers think in graphs. As long as this is true, attackers win."

– John Lambert

When we talk about attackers thinking in graphs, we are not describing malicious pie charts and bar graphs, but are rather applying the concepts of graph theory, which examines the structures used in mathematics to model relationships between objects to create a model of identity-threat behavior. In the case of identity, the graph contains nodes (circles) that represent endpoints (desktops, servers, IoT / OT, other internet-capable devices, etc.) and services, and then edges (lines) that represent the paths that connect the nodes—or as we've defined them, the paths to privilege.

By thinking in graphs, we can conceptualize how attackers could pivot from the initial compromise of an identity and move across your environment by exploiting the privileges and paths to privilege within your systems.

Compromising an identity or endpoint gives you access to one or more nodes, and privilege gives you control of them. The more paths to privilege in the environment, the more opportunities for an attacker to access and control endpoints and services.



LISTS VS GRAPHS

Left, defender thinks in lists.
Right, attacker thinks in graphs.

Attackers look for the cross-domain paths that connect systems by thinking in graphs. However, organizational silos and tooling often leave defenders thinking in lists (ie: checklists) isolated to one system or environment, and not going beyond the system boundaries. This limits their ability to see what the attacker sees, thus hindering their defense.

> For example, an attack might start by exploiting a vulnerable public-facing server on-prem, then move laterally to a system running a cloud sync agent. From there, the attacker could extract the highly privileged cloud account credentials from the agent, then use the credentials and privilege to pivot to the cloud and take over the entire cloud tenant. **The attacker could then use all the paths to privilege** they have uncovered to delete systems and data, both in the cloud and on-premises, in a knock-out blow (or "game over" event).

This example isn't threat actor fiction—it's just one of many real-world examples of how attackers think in graphs and exploit paths to privilege to move fluidly between different domains. The more paths to privilege in your environment, the more opportunities an attacker has to move laterally, escalate privilege, and cross domains.

On the defenders' side, we often think in lists and silos. This means we might have an Active Directory (AD) team, a cloud team, an endpoint team, and a server team. Or, we might think in terms of compliance checklists for individual systems and controls. Silos and list-thinking are often a result of a disparate identity infrastructure, niche tooling, and different team structures. The result: gaps in visibility as you cross domains, teams, and tools, leaving IAM and security blinded to the paths to privilege between systems that attackers can readily exploit.

Thinking in graphs and focusing on paths to privilege allow you to see your attack surface from the perspective of an attacker so you can proactively harden your environment. It also allows you to understand the blast radius in the event of a breach, so you can quickly detect and appropriately respond to an attack. This is why understanding paths to privilege is not only the crux of modern identity security, but is also essential for overall security.

What about existing security tools?

Many solutions available today are heavily focused on detecting malware, known exploits, and malicious code. While these are valuable defenses, **they aren't effective against modern identity threats**.

Evolution of Identity-First Security

Perimeter Security

Endpoint Security

Identity Security

Since it's now typically easier for an attacker to log in than hack in, it's vital to be able to see, manage, and protect the paths to privilege in your environment.

Because most current detection tools are generally reactive to events and lack the context of identity and paths to privilege, it's challenging to proactively reduce the attack surface and reduce risk. Without a clear understanding of paths to privilege, it's impossible to understand which identities present the greatest risk in your environment, or which controls will have the greatest impact on reducing your identity attack surface to protect against future attacks.

For example, an EDR or SIEM might detect that an endpoint has been compromised by malware and that an identity has been exposed to risk. However, without the context of what privilege that identity has—not only on that endpoint but also across the environment—you won't know what paths to privilege are available to the attacker.

> Is there a way for the attacker to elevate to Domain Administrator from that compromised endpoint? Could they use the identity to access data in AWS? Do they have control over OAuth applications in Azure that could be used to pivot into the cloud infrastructure? **Without the wider context, it becomes difficult (if not impossible) to respond appropriately and prevent further compromise.**

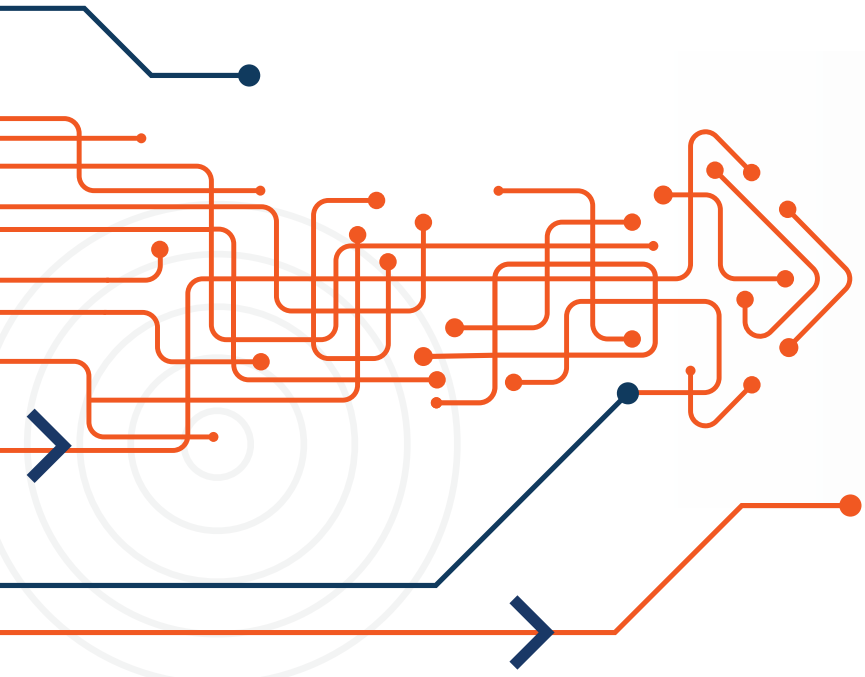
While a range of identity-centric controls exist—for example, MFA, conditional access, and SSO—these are not enough. Attackers can socially engineer users into providing MFA codes, phishing toolkits can capture credentials and proxy MFA requests, compromised devices can be used to hijack sessions, proxy networks can evade access restrictions, and, once the attacker has that initial access, SSO can open up access to a range of cloud apps and data.

By understanding the potential blast radius from a compromised identity, you can better prioritize, respond to, and mitigate the risks. This knowledge allows you to take a proactive approach to reducing your identity attack surface, and effectively remove, manage, and monitor paths to privilege. Eliminating the easy paths an attacker might use to access systems or disable security controls will also help ensure the rest of your security tooling can work effectively.

How BeyondTrust Protects Paths to Privilege

As the only analyst-recognized leader in both Privileged Access Management (PAM) and Identity Threat Detection and Response (ITDR), **BeyondTrust is uniquely poised to protect against identity threats, minimize your threat surface, and reduce the blast radius of attacks.**

We apply years of experience in managing privileges, a deep understanding of the ever-changing cybersecurity landscape, and an advanced platform of proven identity security solutions to protect our customers from today's identity-based threats.



Through our platform approach, BeyondTrust provides the broadest and deepest coverage for finding, managing, and protecting paths to privilege.

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

Identity Security Insights

BeyondTrust Identity Security Insights offers unified, continuous assessment of risks and paths to privilege across your identity landscape, playing a pivotal role in preventing and disrupting sophisticated identity attacks. Customers rely on Identity Security Insights to holistically assess and improve their identity security with radically reduced effort, regardless of where they are today.

The product leverages AI/ML to analyze vast amounts of identity data from diverse sources, including Active Directory, Entra ID, Ping, and Okta, as well as BeyondTrust products. This allows you to proactively identify and address your critical identity security issues with deep visibility and context from a single place.

Path to Privilege Protection:

Uncover Direct and Indirect Paths to Privilege

Uncover paths to privileges and identity risk pathways in interconnected IT environments, such as those arising from nested group memberships, over-privileged identities, dormant accounts, misconfigurations, unknown access paths between production and non-production environments, vulnerabilities in Active Directory Certificate Services (ADCS), unmanaged privileged accounts, accounts vulnerable to Kerberoasting, etc.

Proactively Harden Your Identity Security Posture

Stay ahead of attackers. Enhance your identity security hygiene with continuous risk assessments that provide detailed entitlement information and deep insights paired with contextually rich recommendations. Leverage BeyondTrust PAM and other integrations to rapidly address the findings to eliminate or protect privilege and paths to privilege.

Operationalize Identity Threat Detection and Response (ITDR)

Detect when privileges or paths to privilege are under attack. Alert on anomalies such as password sprays, malicious IP sign-in, excessive password read events, infrastructure changes following suspicious MFA events, unusual changes to Azure service principals, and access from known malicious IP ranges. Leverage prescriptive recommendations, and BeyondTrust PAM controls, to promptly prevent and remediate attempts to exploit paths to privileges. Integrate with your familiar SIEM, SOAR, ITSM, and ChatOps platforms to accelerate response and mitigation.

Identity Security Insights was crucial in detecting the Okta Support breach in October 2023, catching critical activities (like session hijacking and proxy-based administrative actions) weeks before Okta's public acknowledgement. One of our customers said that when the Okta Support breach was detected by BeyondTrust, their CIOs and CISOs were relieved to know about the **proactive capabilities of Identity Security Insights**. It allowed them to confidently assure their management that they were unaffected by the breach.

By mapping complex interconnections between human and non-human identities, accounts, privileges, and configurations across the identity fabric—including endpoints, servers, identity providers, IaaS, PaaS, SaaS, and DevOps tools—Identity Security Insights uniquely uncovers hidden paths to privilege that other solutions miss. With the product's prescriptive recommendations and detections, you can harden your identity security posture, remediate issues, and disrupt paths to privileges more proactively and effectively.

Password Safe

BeyondTrust Password Safe provides comprehensive visibility and control of privileged accounts, sessions, credentials, and secrets. The product streamlines Privileged Account and Session Management (PASM) and Secrets Management capabilities within one cohesive solution.

Password Safe is critical to protecting some of the most commonly targeted paths to privilege. The product helps organizations minimize the risks associated with privileged credential compromise by onboarding privileged accounts and credentials and safeguarding access to privileged account passwords and DevOps secrets, as well as certificates, API keys, tokens, and SSH keys.

Path to Privilege Protection:

Discover, Onboard, and Manage Privileged Accounts and Credentials

Leverage advanced discovery capabilities to streamline the process of bringing privileged accounts under management. Gain full visibility and control over privileged accounts to mitigate risks associated with unmonitored access.

Automate Credential Rotation

Secure paths to privilege by automatically rotating credentials to minimize risks like password reuse and account compromise, which can lead to footholds or lateral movement within your network.

Enable Just-in-Time Access

Provide just-in-time access to paths to privileges on critical resources to eliminate standing privileges and reduce the attack surface.

Manage Secrets

Secure paths to privilege in DevOps and other dynamic environments by efficiently managing and safeguarding secrets, and eliminating hardcoded credentials that threat actors seek out.

Manage Workforce Passwords

Eliminate unmanaged and shared employee application credentials by implementing robust password management practices, closing identity security gaps.

By implementing these features, Password Safe can prevent many attacks, such as password reuse threats and Pass-the-Hash (PtH) attacks where threat actors use stolen hashed credentials to access other networked systems. By auto-rotating credentials and removing standing privileges, Password Safe ensures that, even if an identity and its credentials are compromised, they cannot be reused, thus significantly reducing the risk of such lateral movement attacks. By extending enterprise security even to employee workforce passwords, Password Safe further expands path to privilege protection beyond those accounts traditionally treated as privileged.

Endpoint Privilege Management

BeyondTrust Endpoint Privilege Management helps organizations enforce least privilege and achieve compliance by controlling local admin rights and root access across Windows, macOS, and Linux desktops and servers.

Endpoint Privilege Management plays a vital role in defending paths to privilege by offering comprehensive control and visibility over local admin privileges and application access on endpoints. The product ensures endpoint security policies are enforced consistently across all devices, reducing the risk of unauthorized access and privilege escalation.

Path to Privilege Protection:

Remove Paths to Local Admin Privileges on Endpoints

Eliminate unnecessary local admin rights, reducing the risk of exploitation by malicious actors in the event the endpoint is compromised.

Unlock Productivity with Out-of-the-Box Quick Start Templates

Allow users to easily access the privilege needed for their role, through granular policy and controls.

Prevent Misuse with Advanced Anti-Tamper Mechanisms

Block the misuse of privilege, such as the creation of new local admin accounts and unauthorized privilege elevation.

Protect the Endpoint

Local admin rights and root access are commonly exploited paths to privilege that attackers use to disable security controls, capture credentials, and move laterally. Endpoint Privilege Management mitigates these risks and provides a powerful foundation upon which to build your endpoint security.

By protecting paths to privilege on endpoints, Endpoint Privilege Management can mitigate privilege escalation, where attackers exploit privilege to gain elevated access rights. By removing unnecessary local admin privileges and using advanced anti-tamper mechanisms, this solution significantly reduces the attack surface and mitigates the risk of lateral movement and privilege misuse. Even if an endpoint is compromised, Endpoint Privilege Management security controls help minimize the blast radius and risk.

Entitle

BeyondTrust Entitle automates cloud permissions management, enabling organizations to implement seamless just-in-time access to reduce the attack surface of critical cloud assets.

Entitle is a powerful solution for gaining control over the path to privilege explosion in the cloud. The product provides a hassle-free approach to robust access controls and security policies to protect identities, sensitive data, and systems. With Entitle, only grant privileged access for the moments necessary, and under strict oversight.

Path to Privilege Protection:

Orchestrate Just-in-Time Cloud Access

Control access to cloud resources by granting privileges only when needed, reducing the need for standing privileges and minimizing the threat windows during which privilege can be exploited.

Enable Self-Service Access

Empower users to request and approve access through automated workflows that enforce security policies, ensuring paths to privilege are protected.

Support Break-Glass Scenarios

Provide emergency access in critical situations, with full auditing and control. Ensure that such access is both secure and traceable.

Support Just-in-Time SSH Access for Non-Federated Identities and Legacy Environments

Offer secure and timely SSH access for users in non-federated and legacy systems, maintaining security across diverse environments.

By protecting paths to privilege in cloud environments, Entitle can mitigate privilege escalation attacks and permissions misuse to access sensitive data and systems. Entitle implements just-in-time access ensuring that, even if credentials are compromised, they cannot be used to gain unauthorized access. Additionally, Entitle's support for break-glass scenarios ensures emergency access is granted securely and is fully auditable, reducing the risk of misuse during critical times. This comprehensive approach secures paths to privilege across cloud environments and SaaS applications.

Privileged Remote Access

BeyondTrust Privileged Remote Access allows organizations to create identity-secure, just-in-time access for all cloud, on-premises, and OT environments.

The product provides essential identity security and control over remote connections, eliminating the need for traditional VPNs, and removing and protecting commons paths to privilege that attackers exploit. With Privileged Remote Access, ensure remote access is both secure and manageable for employees and vendors with comprehensive visibility and control over all privileged activities.

Path to Privilege Protection:

Control and Protect Vendor and Third-Party Paths to Privilege

Eliminate the need for VPNs and known privileged credentials. Gain full control and visibility over vendor access, ensuring secure and monitored remote connections.

Implement Just-in-Time Secure Remote Access for Employees

Create secure, least-privilege remote access only as needed, inject managed credentials directly into sessions, and eliminate standing privileges for employees.

Gain Full Visibility and Control of All Actions and Privileges in Every Session

Monitor, manage, and audit all actions and privileges in every remote session, ensuring activities are tracked and controlled.

Protect More Paths to Privilege with Support for Multiple Protocols

Securely manage remote access across various protocols, including RDP, VNC, HTTPS, SSH, and SQL, to ensure broad protection of paths to privilege.

By implementing these features, Privileged Remote Access can prevent unauthorized access and privilege escalation attacks. The product provides just the access required and injects credentials directly into the session from a secure vault without exposing them to the user. This reduces the risk of compromised credentials being used to gain unauthorized access.

Additionally, the comprehensive session management and auditing capabilities ensure all actions are monitored and controlled, preventing misuse of privileges. This robust approach maintains a high level of security across remote connections, while also protecting paths to privilege that a threat actor could otherwise leverage to gain a foothold or expand an attack.

Remote Support

BeyondTrust Remote Support allows organizations to securely access and support any device or system in the world. The product is crucial for securing remote access paths to privilege for service desks.

Remote Support eliminates the need for traditional VPNs and standing privileges, ensuring access is granted only when necessary and under strict monitoring. Also benefit from the product's robust controls and auditing to ensure security and oversight of remote sessions.

Path to Privilege Protection:

Secure and Control Remote Access Pathways to Privilege

Provide secure, VPN-less remote access to reduce the risk of compromised connections, and ensure all remote access paths are tightly controlled. Also gain the ability to define and enforce different policies for attended and unattended remote support sessions.

Implement Just-in-Time Access for Support Sessions

Grant granular permissions and access, only when needed, eliminating standing paths to privilege and reducing the potential for unauthorized access.

Integrate Password Security

Enable technicians to securely store, share, and track the use of privileged credentials by the IT service desk.

Audit Every Session

Monitor and audit every remote session to ensure identities are not misused, achieving full accountability and visibility into all remote activities.

By implementing these features, Remote Support can prevent unauthorized access and identity misuse. For instance, by removing standing paths to privilege and relying on just-in-time access, you can ensure that, even if credentials are compromised, they cannot be used to gain unwanted access. Additionally, the auditing of every session ensures all activities are monitored, preventing the misuse of identities and maintaining a high level of security and accountability in remote support scenarios.

Active Directory Bridge

BeyondTrust Active Directory Bridge (AD Bridge) extends Microsoft AD authentication, SSO capabilities, and Group Policy configuration management to Unix and Linux systems. The product simplifies policy and administration, streamlines security, and reduces the potential for errors.

By integrating non-Windows systems into Active Directory, AD Bridge ensures consistent policy enforcement and accelerates the path to zero trust security.

Path to Privilege Protection:

Simplify Policy and Administration

Unify management by extending AD capabilities to non-Windows systems, reducing administrative complexity and potential errors that could create paths to privilege.

Streamline Security

Benefit from centralized control over identity and access policies, ensuring uniform security standards across all platforms.

Reduce Potential for Errors

Automate policy enforcement and compliance, minimizing the risk of misconfigurations and human errors.

Accelerate your Path to Zero Trust

Monitor and audit every remote session to ensure identities are not misused, achieving full accountability and visibility into all remote activities.

By leveraging Active Directory Bridge, organizations can prevent configuration drift and security inconsistencies, which can open or expose paths to privilege. The product centralizes and automates policy management to ensure security policies are applied uniformly across heterogeneous infrastructure, reducing the likelihood of errors that could be exploited by attackers. This approach supports the zero trust model, where continuous verification is key to maintaining a secure environment.

Next Steps

Securing identities and their paths to privilege is an essential, ongoing journey that requires a strategic approach, and the right identity security toolset.

This paper has underscored the critical importance of understanding and protecting paths to privilege. By considering the broader identity infrastructure, policies, groups, and interconnections, organizations can enhance their security posture and effectively mitigate risks.

Interested in uncovering the paths to privilege across your own environment and gaining clear recommendations on how to proactively harden your security posture?

Take advantage of our complimentary **identity security assessment and 30 days of continuous threat monitoring,** powered by Identity Security Insights.

LEARN MORE
beyondtrust.com or contact us

Resources

WHITEPAPER
Buyer's Guide for Complete Privileged Access Management (PAM)

WHITEPAPER
Advancing Zero Trust with Privileged Access Management (PAM)

PODCAST
The Midnight Blizzard Breach on Microsoft and Other Identity Attacks

BLOG
AD CS 101: Introduction to Active Directory Certificate Services & How to Detect and Mitigate ESC1 Attacks

BLOG
Identity Attack & Defense: Lessons in Okta Security

About BeyondTrust

BeyondTrust is the global cybersecurity leader protecting paths to privilege with an identity-centric approach. We are leading the charge in transforming identity security and are trusted by 20,000 customers, including 75 of the Fortune 100, and our global ecosystem of partners.

Learn more at **www.beyondtrust.com.**