EBOOK

BeyondTrust | FOR PUBLIC SECTOR

Leave No Privilege Behind

Discovering, Understanding, & Managing Every Privilege

BeyondTrust | FOR PUBLIC SECTOR

Leave No Privilege Behind

Discovering, Understanding, & Managing Every Privilege

Table of Contents

FOR PUBLIC SECTOR

Identity is the New Battleground for Cyberattacks

Identity is the new battleground for cyberattacks, with fewer attackers "breaking in" via hacking or other offensive tactics.

Instead, many of today's threat actors are logging in with identity and account information harvested from prior identity compromises and cyberattacks. From that initial foothold, threat actors pivot to privileged access to fuel their campaigns and cyber operations.

In almost every modern cyberattack, from ransomware, insider threats, supply chain compromise, to nation-state intrusions, one thing is consistently common:

privileged access is needed to move laterally, maintain persistence, and/or gain a deeper foothold into environments—ultimately increasing the blast radius of their attacks.

Every unmanaged, excessive, or risky privilege can become a means for threat actors to launch or expand their attacks.

That is why organizations, especially in the public sector, must adopt "Leave No Privilege Behind" as part of their cyber defense strategy. It embraces foundational Zero Trust principles that focus on least privilege to reduce the entire identity attack surface.

This approach also involves eliminating every unnecessary privilege pathway that threat actors could exploit to escalate access, move laterally, or maintain persistence inside critical environments. Common examples of these privilege pathways include privileged accounts with always-on access, service accounts without oversight, exposed secrets such as passwords or API keys, misconfigured identity infrastructure, users with local admin privileges on their work devices, and many others.

Defining
"Leave No Privilege Behind"

At its core, "Leave No Privilege Behind" means ensuring no privileged account, entitlement, or privilege pathway is left unmanaged.

This includes:

- Standing or temporary accounts
- Active or dormant entitlements
- Shadow identities (unregistered SaaS accounts, self-service cloud access)
- Shared accounts (admin, root, superuser)
- Service accounts (domain-joined, database, application / web services)
- Cloud service principals (AWS IAM roles, Azure, GCP)
- AI agents (AI assistance, agentic, and model to model)
- Machine-to-machine communications (Kubernetes, message brokers)

If unmanaged, each of these examples represents an opportunity for threat actors to bypass defenses and compromise mission-critical systems. When privileges are not properly managed, they effectively become attack paths for threat actors to gain unauthorized access. The goal is to disrupt attackers' capabilities by leveraging a prevention-first approach. The only way to do so is to ensure that every privilege is accounted for, secured, and managed.

Leave No Privilege Behind is a strategic approach to identity security that CISOs, infrastructure, and security teams can take to ensure every privilege—human, machine, or AI agent—is discovered, governed, minimized, and continuously validated so threat actors cannot use them to escalate, move laterally, or gain persistence.

It operationalizes and elevates Zero Trust by eliminating hidden, excessive, and dormant privileges across the entire identity estate.

Putting "Leave No Privilege Behind" Into Practice

In practice, "Leave No Privilege Behind" (LNPB) focuses on implementing identity governance models that eliminate all unmanaged, excessive, inherited, transitive, and standing privileges across users, service accounts, secrets, workloads, and AI agents.

To do so, organizations must leverage continuous visibility and actionable telemetry to first see the True Privilege™ of every identity—what it can do and why—along with any hidden or indirect privileged pathways associated with each identity. With this level of visibility, organizations can then operationalize key Zero Trust policies and enforce least privilege in all its forms, including just enough privilege (JEP), just enough access (JEA), and just-in-time (JIT) access. When these policies are operationalized across the organization, they help ensure no privilege exists beyond what is required for a specific task or timeframe.

Zero Trust / Least Privilege Controls	What It Does	How It Supports LNPB	Identity Risk Reduced
JEP (Just Enough Privilege)	Tasks only get the privileges needed to do a task or activity	Eliminates excessive permissions	Privilege sprawl, lateral movement
JEA (Just Enough Access)	Restricts what actions an identity can take	Prevents privilege overreach; restricts attacker capabilities	Reduces and disrupts lateral movement
JIT (Just-In-Time) Access	Elevation only exists for a short, approved window	Removes standing & dormant privileges	Persistence, privilege escalation, and minimizes window of exposure

The "Leave No Privilege Behind" approach aligns with Zero Trust policies for the following controls:

- JEP ensures privileges are always scoped, intentional, and tightly controlled—never excessive or left unmanaged.
- JEA constrains what identities can do, closing privilege overreach and reducing pathways to privilege escalation.
- JIT eliminates standing privileges—ensuring elevated access only exists for an approved, timed duration or window.

You Can't See What I See - Illuminating Privileged Access

To operationalize the LNPB principle, organizations must formalize these questions into their overall cyber defense strategy:

1. **Do you have complete visibility into all privileged accounts and entitlements—across users, machines, and cloud services?**

   Organizations cannot secure what they cannot see. Illuminating the full identity estate is the first step in reducing and regaining control of the identity attack surface.

2. **Are you eliminating standing privileges with JIT / JEA / JEP and enforcing least privilege across all identities?**

   Zero Trust cannot exist without least privilege. JIT / JEA / JEP further reduce risk by ensuring elevated privileges only exist when necessary, and are tightly controlled and time-bound to reduce opportunities for privilege abuse or misuse.

3. **How are you continuously monitoring and validating privilege use to detect abuse or drift before it becomes a breach?**

   Proactive monitoring enables organizations to catch anomalies and poor identity practices early, stopping privilege abuse before it escalates into a full-blown cyberattack.

Understanding True Privilege™ and Paths to Privilege™

Managing privileges across your identity estate requires going beyond surface-level account inventories.

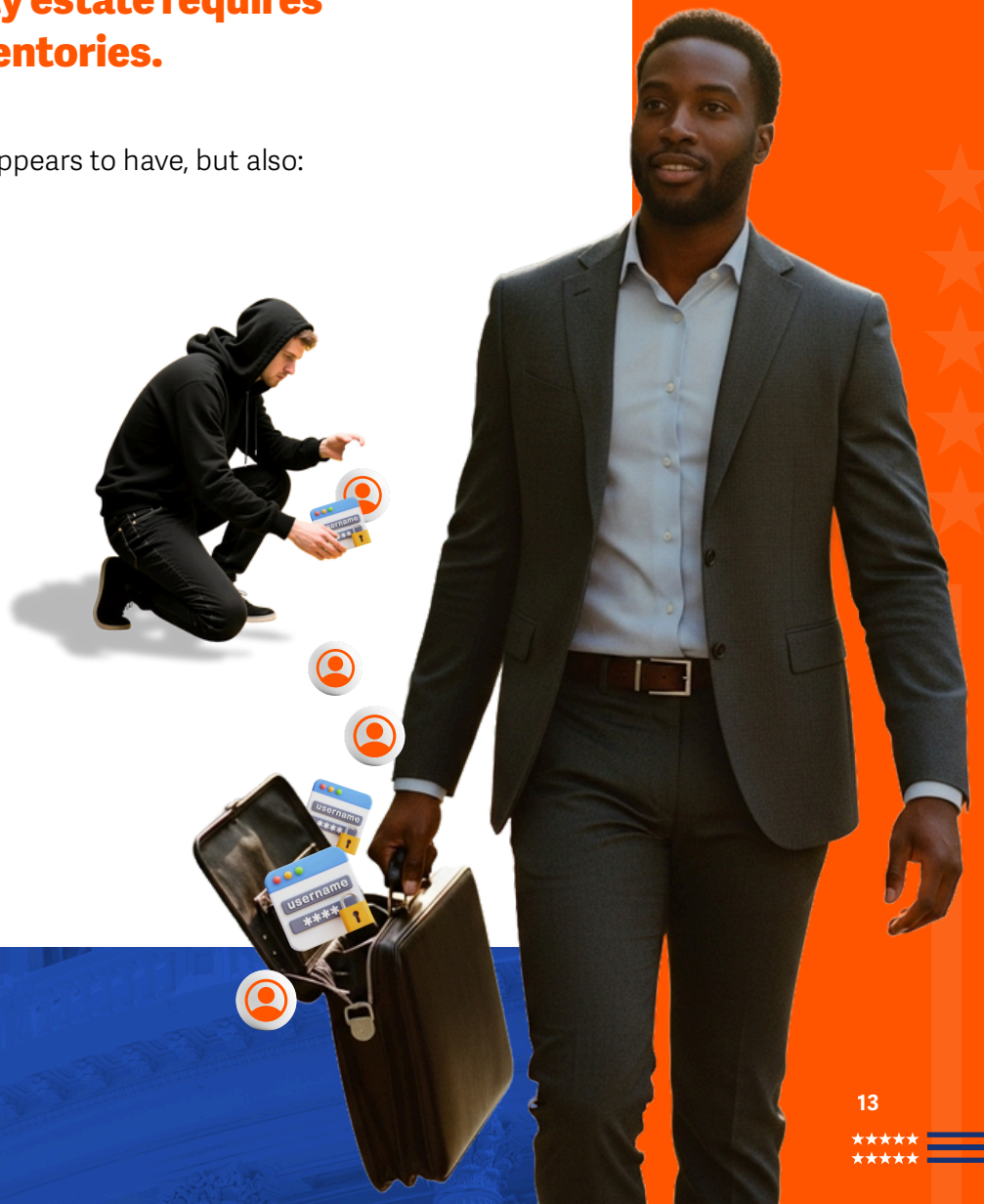
Agencies must ask not only which privileges each identity appears to have, but also:

What an identity can ultimately do?

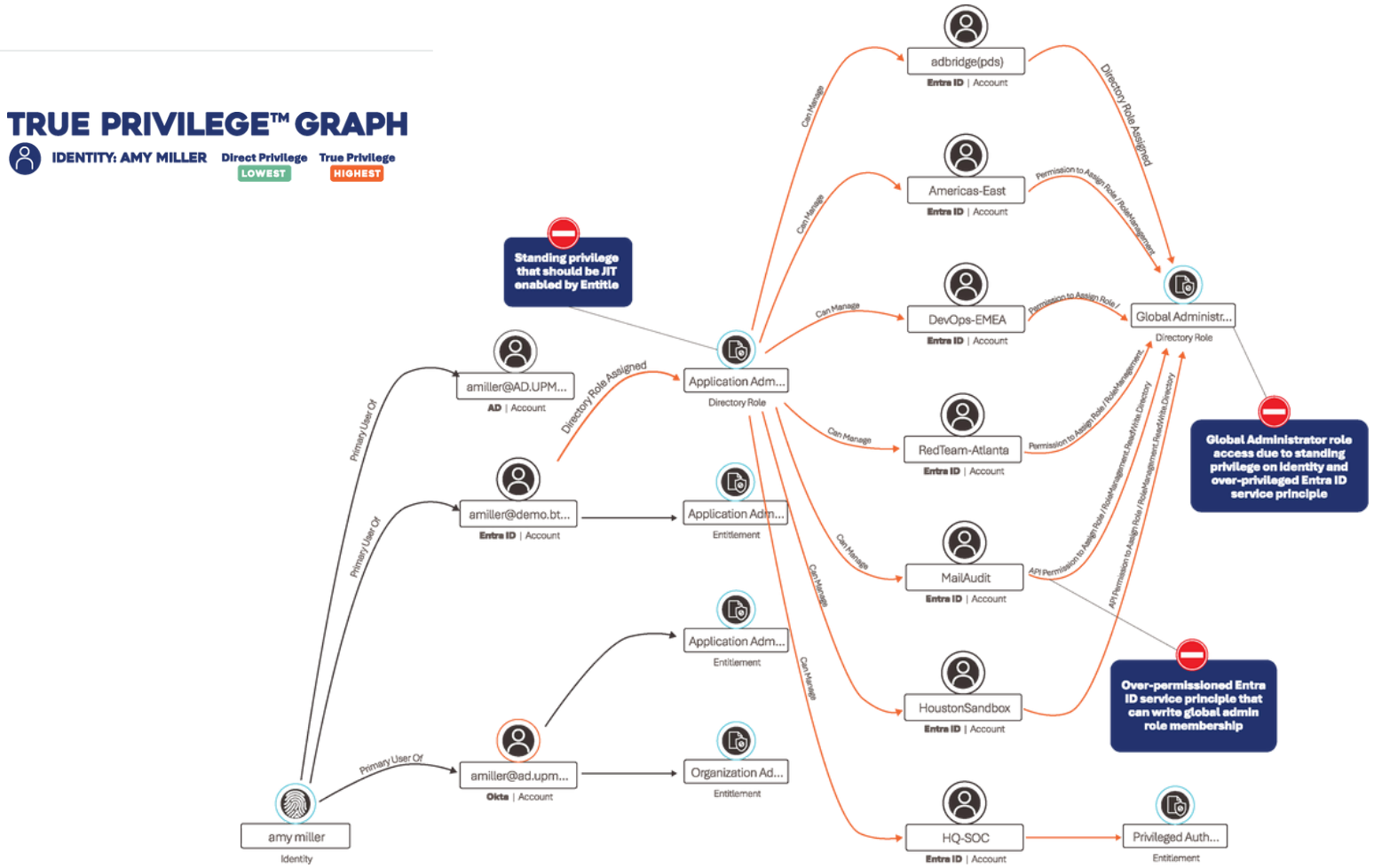
This is the actual, effective access an identity holds in the environment, often far greater than expected due to overlapping entitlements or group memberships. BeyondTrust calls this True Privilege™.

How an identity gets to do what it can ultimately do?

These are the exploitable pathways that allow identities to escalate privileges or inherit rights indirectly. BeyondTrust refers to this mapping of connections, entitlements, and configurations as Paths to Privilege™.



By understanding both True Privilege and Paths to Privilege, agencies can see their identity estate as threat actors do, exposing hidden risks and lateral movement opportunities before they are exploited. This ensures privileges aren't exposed or left behind.



Shining a Light on Shadow AI

Shadow AI is a growing threat that organizations must account for in their overall risk management and governance frameworks.

It happens when people in organizations adopt and use AI tools without governance, oversight, or formal approval.

For example, shadow AI could happen if a salesperson created an AI agent on their own, without approval, to assist them with market research on a competitive solution. Another example could be a developer installing a Model Context Protocol (MCP) server locally on their machine or on the network, linking to sensitive data sources like a database server or identity sources that could give these AI agents privileges across the environment.

Establishing visibility into AI agents, including their intentional or unintentional access and privilege, is important to ensuring that privileges are not left behind. Reducing unmanaged or excessive privileges across the identity attack surface for AI should be a top priority for leaders in both government agencies and corporate organizations.

AI Security Outcomes by BeyondTrust

AI Agent Inventory & Normalization

Discover and map agent-level identities including AWS, Microsoft, Salesforce, and more

Privilege and Access Risk Analysis

Identify overprivileged and dangerous deployment configurations

Secrets Discovery & Integration Hygiene

Uncover secrets that tie agents to sensitive services and detect shadow IT AI usage

Findings & Enforcement Hooks

Surface findings like Copilot Studio agent with excessive data and no delegation model

Managing AI identities requires the following:

- Maintaining a complete inventory and classification of AI identities (service principals, agent backends, API keys, SaaS connectors, service accounts).
- Building a "True Privilege" graph to see what AI identities can ultimately do (effective and actual access across tools, applications, cloud roles).
- Using ephemeral roles and short-lived credentials for agent tool use and enforcing least privilege.

Continuous Visibility & Actionable Telemetry for Identity Intelligence

Gaining complete control of your entire identity estate requires the right identity intelligence, comprised of continuous visibility and actionable telemetry that accounts for every identity, access, and privilege used in the environment.

It doesn't matter if identities are human or non-human (machine, application, AI, etc.), nor if they are on-prem or across multiple cloud / SaaS environments. The goal is to harness identity intelligence from across your entire IT estate to secure identities, access, and privileges everywhere. This capability is foundational to appropriately hardening your environment and preventing threat actors from taking advantage of unmanaged or unknown privileges.

Ultimately, effective identity intelligence enables you to uncover the weaknesses and gaps in your identity security posture before threat actors do.

The following elements facilitate the continuous visibility and telemetry needed for actionable identity intelligence:

Identity Hygiene

Identity attack surface telemetry

Paths to Privilege

Visualize identity attack surface path exposures

AI/ML Threat Detection

Threats targeting identity infrastructure

Identity Hygiene plays a critical role in reducing the identity attack surface across privilege control planes.

Identity hygiene pinpoints such issues as:

- Misconfigurations in your identity infrastructure
- Excessive privileges and standing privileges
- Exposed secrets (hardcoded, etc.) and passwords
- Shadow AI
- Vulnerable human and non-human accounts

Privilege Pathway Visualization illuminates the ways in which your identity security posture is vulnerable to exploits by threat actors.

This starts with understanding the True Privilege of an identity—uncovering what it can actually do.

As an example:

A user's Entra ID is assigned to directory role in Application Admin, which allows for the impersonation of a service principal and abuse of API permissions.

The user can now add privileged roles to users and change passwords, MFA factors, and more.

AI / ML-Based Threat Detection uses behavior analytics to identify suspicious activity and threats targeting an organization, including via its identity security posture.

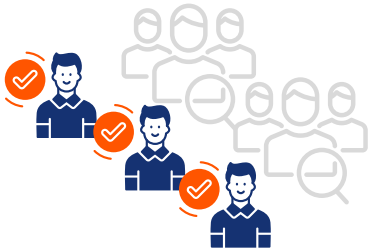
Such capabilities can be used to detect anomalous behaviors such as:

- Session hijacking
- Kerberos-based attacks and password spray attempts
- Anomalous entitlement behavior across multiple domains and multi-cloud environments
- Suspicious IP addresses targeting identity providers
- Anomalous activity associated with privilege sessions and accounts

This level of identity intelligence is also critical for formalizing and maturing Zero Trust capabilities.

It helps organizations ensure Zero Trust principles are enforced for least privilege, explicit trust, and identity threats. Identity intelligence should help inform organizations about where and how to harden their Zero Trust architecture. It also provides concrete data for making investment decisions about what protection capabilities are needed to mature Zero Trust and boost resiliency against cyberattacks.

Least Privilege



Grant only the minimum access necessary, for the shortest time necessary.

Explicit Trust

Access must be based on verified identity, device, risk, behavior, and policy.

Assume Compromise

Continuous monitoring and visibility for real-time identity intelligence.

With identity intelligence, organizations can see where their security controls succeed, where they fall short, and where investments should be focused to elevate cyber defense.

Quantifies Privilege Risks
Shows where excessive or unused entitlements create the highest risk of concentration.

Correlates to Security Control Effectiveness
Demonstrates Zero Trust capabilities and use cases to reduce risk across the privilege lifecycle.

Enables Continuous Maturity and Improvements
Uncovers security gaps over time and illuminates next steps for improving identity security controls.

6 Keys to Preventing Privilege Gaps

The 6 Keys to Preventing Privilege Gaps

There are six essential actions for ensuring that no privileges are left behind.
While the details vary by agency or environment, the guiding principles include:

1. Achieve full visibility into privileged accounts, including their credentials and entitlements.
2. Apply least privilege consistently across human and machine identities.
3. Eliminate standing privileges through just-in-time access.
4. Continuously monitor and validate privilege usage.
5. Map effective privileges to uncover hidden risks.
6. Visualize pathways to privilege escalation to disrupt potential attack routes.

Together, these steps strengthen identity hygiene and form a foundation for Zero Trust.

Conclusion:
A Mindset for Zero Trust Success

"Leave No Privilege Behind" is more than a catchy phrase.

It is a holistic approach to securing the modern digital world.

By reducing identity attack surfaces, improving identity hygiene, and embedding least privilege and just-in-time principles into operations, agencies can elevate their cyber defense posture.

1 RULE

The path to Zero Trust maturity begins with one uncompromising rule:
Every privilege must be discovered, managed, and monitored. No exception.

When agencies commit to this principle, they close critical gaps that threat actors rely on and take a decisive step toward resilience in the face of evolving cyber threats.

10 Key Takeaways

FOR PUBLIC SECTOR

"Leave No Privilege Behind"

10 Key Takeaways

1 Identity is the new battleground for cyberattacks.

The threat landscape has evolved, and all roads lead to identity security. Threat actors don't break in—they log in. Unmanaged, excessive, or dormant privileges ultimately fuel cyberattacks.

2 There is no Zero Trust when privileges are left behind.

Without good privilege management and enforcement, Zero Trust will fail. Identity is foundational for Zero Trust, and managing all privileges is what makes protection capabilities resilient against identity-related attacks.

3 AI identities demand the same rigor as human and traditional non-human identities (if not more).

AI agents introduce a new privilege frontier, and in many cases, these agents wield more privilege than humans or traditional NHIs. Removing the shadows of AI with comprehensive visibility and actionable telemetry will enhance awareness of unmanaged and excessive privileges.

4 Visibility is how you (re)gain control of your identity estate.

Informed threat prevention and cyber defenses start with visibility into every privileged account, entitlement, machine identity, and AI agent. You can't secure a growing attack surface if you don't have comprehensive visibility across your privilege planes.

5 Assume compromise—disrupt lateral movement and persistence.

As privilege attacks continue to scale, organizations must assume compromise and leverage early warning telemetry to take a prevention-first approach and disrupt threat actors from moving laterally and establishing persistence.

6 Effective privilege management levels up your cyber defense.

Privilege management across all privilege planes is the most effective way to disrupt threat actors and elevate cyber defense. It's the cornerstone of a successful Zero Trust strategy and architecture.

FOR PUBLIC SECTOR

"Leave No Privilege Behind"

10 Key Takeaways

7 Privilege is the common denominator in almost all cyberattacks and breaches.

When privilege is managed effectively, it reduces cyberattacks. In almost all cyberattacks, threat actors need privilege (the fuel) to move laterally, maintain persistence, and pre-position for large scale cyber operations. Cut off the fuel that drives cyberattacks.

8 Cyber defense must shift toward an identity-centric approach.

With the shift from network to identity attacks, identity security has become a critical component to cyber defense. It's the nexus and control point for Zero Trust maturity, building out visibility, least privilege, and continuous validation for disrupting and preventing cyberattacks.

9 Privilege management accelerates the shifts from detection to prevention.

While detection is needed, it's often too late. Focusing on reducing the attack surface for privileged access is proactive cybersecurity that accelerates the shift toward a prevention-first approach.

10 Unmanaged and excessive privilege is a form of technical debt.

Like technical debt, excessive privileges can silently accumulate over a period of time and pose significant risks to organizations. Eliminate that debt with comprehensive visibility to drive awareness of unmanaged privileges across your entire identity estate.

BeyondTrust for "Leave No Privilege Behind"

BeyondTrust for Enforcing Leave No Privilege Behind

BeyondTrust is trusted by 20,000 organizations, with many in highly regulated industries. We support 2,400+ government customers in protecting against modern identity threats and achieving compliance.

BeyondTrust empowers organizations to enforce Leave No Privilege Behind in the following ways:

- Gaining continuous visibility and actionable telemetry to illuminate all privileges and Paths to Privilege. Identity Security Insights® also flags anomalous identity behaviors and helps drive alignment to NIST and MITRE frameworks.
- Eliminating local admin rights, enforcing least privilege for application control, and providing just-enough privilege for all endpoints with Endpoint Privilege Management.
- Enabling just-in-time access and enforcing least privilege for internal and external access to cloud infrastructure, on-premises environments, and critical infrastructure with Privileged Remote Access.
- Bringing all privileged credentials, keys, and secrets under management and enforcing just-in-time access controls with Password Safe®.
- Automating self-service workflows for JIT and least privilege access across cloud infrastructure and SaaS with Entitle.

Additional Resources

Learn more about managing privileges and enabling Zero Trust for public sector agencies:

GUIDE

Mapping BeyondTrust Capabilities to NIST Zero Trust (SP 800-207)

GUIDE

A PAM Maturity Model

GUIDE

The Guide to Identity Security Defense-in-Depth

CASE STUDY

Town of Truckee: Enhancing Security and Efficiency with BeyondTrust

CASE STUDY

Large State Entity Adopts Identity Security Insights to Reveal Data Across Domains and Reduce Risk

CASE STUDY

Los Angeles Department of Water and Power Boosts Productivity with Endpoint Privilege Management

BeyondTrust | FOR PUBLIC SECTOR