BeyondTrust

CASE STUDY

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

Products: Identity Security Insights, Remote Support, Privileged Remote Access, Password Safe, Endpoint Privilege Management
Company: A State-Level Agency with around 50,000 employees

Use Case — Gain a Complete View of the Entire Identity Landscape

A large state entity has focused on strengthening identity security for years, having adopted four solutions from the BeyondTrust portfolio:

- **Remote Support,** which enabled the team to move their thousands of employees to a work-from-home setup that was both convenient to use and compliant with stringent compliance regulations.
- **Privileged Remote Access,** which enabled the team to further secure their remote environments with just-in-time (JIT) remote access, privileged session management, and additional auditing capabilities.
- **Password Safe,** which enabled the team to better manage privileged passwords, accounts, keys, secrets, and sessions through automated discovery and credential rotation.
- **Endpoint Privilege Management,** which enabled the team to reduce the endpoint attack surface by removing local admin rights and enforcing least privilege.

As the team continued to mature their approach to identity security, they faced the growing need to gain more holistic visibility and control over all the parts of their expanding identity landscape, including toolsets such as Active Directory, Entra ID, and Okta.

Without a holistic view of their entire identity landscape, areas of their environment remained hidden and unmanaged—particularly accounts that were seemingly insignificant. However, many of these ostensibly low-privilege accounts posed risk to the organization, as they had indirect or hidden privilege pathways, which could also enable the ability to move laterally and gain deeper access.

Additionally, the environment contains over 5,000 non-human identities, many of which were unmanaged/unknown. Many of their service accounts and other machine identity credentials were static and hadn't been changed in over a decade. The lack of visibility across platforms also made it challenging to provide an audit trail that incorporated all identity data. The agency was using Splunk to manually correlate identity-related data from disparate solutions but got overwhelmed by the volume of reactive alerts coming from across their environment.

Why BeyondTrust Identity Security Insights

The agency's security team brought their concerns to the attention of their BeyondTrust customer success team, who had supported them for years. From there, the teams collaborated to develop a proof of concept for Identity Security Insights and implemented the platform with read-only access. After witnessing the platform's straightforward implementation process and fast time-to-value, the agency's security team chose to add it as the fifth BeyondTrust product within their environment.

Success with Identity Security Insights

Since initial installation, the BeyondTrust solution has automated the process of correlating all identity-related data into a single view.

Identity Security Insights provided enhanced visibility, enabling the team to understand which of their over 477K accounts and 60K human identities were not under the purview of existing solutions.

During the initial discovery phase, the solution identified critical privilege escalation paths within the client's Azure environment. Multiple applications were configured with excessive API permissions, creating direct escalation paths for Application Administrators to elevate their privileges to Global Administrator roles. These over-privileged app registrations bypassed normal role boundaries and presented significant security risks.

Once Identity Security Insights uncovered this escalation path, the agency's team was able to remediate it by implementing the principle of least privilege across all application API permissions. The BeyondTrust team worked with the client to audit permissions for each application, removing unnecessary elevated privileges and ensuring Application Admins could no longer leverage these permissions to gain Global Administrator access.

Additionally, the solution revealed the following data on other hidden risk within the agency's environment:

- 17,000 compromised passwords that were not considered directly privileged and, therefore, were not subject to controls such as frequent rotation because the accounts were not recognized as highly privileged
- 31,000 password collisions (multiple accounts with the same password)
- 9 logins from Tor nodes
- 124,000 dormant accounts
- 84 accounts that allowed blank passwords
- 45 accounts that were vulnerable to Kerberoasting

These discoveries revealed other significant privileged pathways connected to accounts that the agency did not consider as highly-privileged, and therefore weren't protected as such.

By adding a discovery and visibility dimension to the agency's overall identity security strategy, Identity Security Insights has enhanced the depth of existing solutions. It has enabled the team to understand the True Privilege™ of every account—including low-privilege accounts with hidden escalation paths. It also offers the team pertinent next steps for improving overall identity hygiene and shrinking the attack surface and enables them to ensure appropriate security controls are applied wherever needed.

Looking Ahead with BeyondTrust

After seeing the value of Identity Security Insights firsthand, the agency hopes to roll the solution out to more teams in different departments, further multiplying the value of the product across other security objectives.

"BeyondTrust Identity Security Insights has been a huge help for us in the SOC when it comes to consolidating all our different identity-based log sources into a single platform with prebuilt alerts and flags. Every day we spend in the platform leads to the discovery of more things we want to address. There is an almost endless amount of work to be done when it comes to securing our environment and Identity Security Insights has greatly helped us identify and prioritize what needs addressed first."

Security Operations Supervisor, Large State Agency

BeyondTrust is the global identity security leader protecting Paths to Privilege™. Our identity-centric approach goes beyond securing privileges and access, empowering organizations with the most effective solution to manage the entire identity attack surface and neutralize threats, whether from external attacks or insiders.

BeyondTrust is leading the charge in transforming identity security to prevent breaches and limit the blast radius of attacks, while creating a superior customer experience and operational efficiencies. We are trusted by 20,000 customers, including 75 of the Fortune 100, and our global ecosystem of partners.

Learn more at beyondtrust.com