



CASE STUDY

How iVision Simplifies and Scales Identity Security with BeyondTrust

Harrison Gibbs
Team Lead for Platforms and Automations, iVision

iVision

Product: Identity Security Insights®, Entitle, Privileged Remote Access, Remote Support, Password Safe®, Endpoint Privilege Management for Windows & Mac, ServiceNow integrations

Industry: Professional Services

iVision is a technology integration and managed services firm helping organizations transform through secure, scalable solutions across cloud, security, digital workspace, and enterprise infrastructure.

iVision is a full-service technology integration and management firm specializing in digital transformation. We consult, resell products, and deliver managed services across nearly every possible area of IT. But as our client base expanded nationally and globally, we knew our support model needed to evolve.

When I first joined iVision as the new team lead for platforms and automations, my job was straightforward, in theory: support our growth while maintaining operational efficiency and airtight security. In practice, that actually meant reassessing whether the tools we relied on every day were actually capable of scaling with us.

Managing a collection of disjointed tools was hindering our growth. Moving to a unified ecosystem meant we could stop fighting our internal tooling and start focusing on client outcomes. The first real friction point we needed to address was remote access.

Scaling Support, Without Installing Agents Everywhere

Our remote access process used to involve installing agents on client endpoints. Each new device required a fresh setup, and every environment needed manual coordination. It worked, but led to increased overhead as our footprint grew.

Apart from inefficiencies, agent deployments introduced friction at exactly the moment when our clients most needed quick, seamless support.

Responsiveness is foundational for a managed services provider (MSP), so we knew we needed a secure remote access solution that could eliminate friction without compromising security. BeyondTrust Privileged Remote Access provided the flexibility to connect to systems without requiring traditional agent deployments to make that happen.

Growth Demands a Holistic Identity Strategy

While we initially chose BeyondTrust Privileged Remote Access for secure remote access, it became clear that identity management itself was another one of our pain points. Between provisioning accounts, tracking standing privileges, and wrangling credentials across various client environments, the complexity multiplied quickly. Our internal workforce was nearing 200 employees, and continuing to address these issues manually stood in the way of achieving our operational efficiency goals. Once we hit that size, manually managing access wasn't realistic anymore. We needed something more holistic.

“Once we hit 200 employees, manually managing access wasn't realistic anymore. We needed something more holistic.”



Entrenching BeyondTrust Into Our Business

Over time, we have decided to explore the BeyondTrust portfolio to create something much more comprehensive. Today, we use BeyondTrust products to support every part of our business, both in managed services and internally, starting with remote access and then adding identity management.

Secure Remote Access, Privileged Credentials, and Endpoints Supercharged with ServiceNow

Since its initial implementation, Privileged Remote Access has become the backbone of how we access our large ecosystem of client environments. Almost all of our standard remote sessions currently flow through Privileged Remote Access. Our managed services clients operate across different geographies, networks, and configurations, and Privileged Remote Access provides us with the consistent, secure access we need across all of them.

For ad-hoc end-user support, we turn to BeyondTrust Remote Support, which helps maintain the agent simplicity we love, while adapting to diverse support scenarios.

Additionally, we introduced BeyondTrust Password Safe, which allows ivision to centralize our shared password storage and automate credential rotations in the cloud. For example, we replaced fragmented password management processes, while also reducing overall reliance on manual workflows. Password Safe also makes it possible to know who accessed what and when—without any operational drag.

In addition, we're maximizing impact with integrations like ServiceNow. We've integrated Privileged Remote Access, Remote Support, Password Safe, and to some extent, Entitle, with our ServiceNow instance. The ServiceNow integration with Remote Support has saved us time and money by reducing administrative overhead of our Remote Support landscape. The most impactful aspect of that partnership has been syncing up our Configuration Management Database (CMDB) from ServiceNow to Privileged Remote Access. Before having that integration, our service desk team members had to manually create jump items, verify device records, and cross-reference multiple tools before they could initiate support sessions. Again, administrative overhead added up quickly. Now, technicians can initiate remote access sessions directly from a ServiceNow ticket. Our CMDB syncs automatically, and as a result, reporting is easier and filtering across different client environments is simpler.

We further improved our internal security posture by implementing BeyondTrust Endpoint Privilege Management (EPM). The solution removes standing local administrative rights across our workforce. Instead of granting broad administrative access, we now enforce least privilege at the endpoint and allow controlled, policy-based elevation only when needed.

This shift reduced unnecessary privilege exposure while giving us clear visibility into elevation activity across our environment. Compared to relying on device management tools alone, EPM gives us meaningful insight into who is requesting elevated access, for what applications, and how often—allowing us to continuously refine policy without disrupting productivity.

As a managed services provider, enforcing least privilege internally is critical, not just for our own protection but to ensure we operate with the same discipline we expect from our clients.



"By increasing visibility into gaps and hidden identities, Identity Security Insights shines a light on True Privilege™. We discovered multiple over-provisioned identities and service accounts that we might not have been aware of or that have been over-provisioned for a long time."

Increased Visibility into Humans, Machines, and AI Agents

Adopting Identity Security Insights® was a particularly eye-opening experience for us. By increasing visibility into gaps and hidden identities, it shines a light on True Privilege™: inherited or indirect access paths that weren't immediately obvious. We discovered multiple over-provisioned identities and service accounts that we might not have been aware of or that have been over-provisioned for a long time.

This level of visibility is important as we enter the new world of agentic AI. Identity Security Insights gives us the ability to prioritize and reduce the most critical risks in our environment—for both human and machine identities.

Identity Security Insights also provides us with dashboards that align with additional recognized frameworks, like MITRE ATT&CK and NIST, so we can proactively address risk in a well-established, structured manner. Any security tool is going to give you a thousand suggestions, and there are a number of different ways to prioritize those, but I can trust that when I log into Identity Security Insights, the critical recommendations really are critical.

“Any security tool is going to give you a thousand suggestions, and there are a number of different ways to prioritize those, but I can trust that when I log into Identity Security Insights, the critical recommendations really are critical.”

Operationalized Just-in-Time Access, Everywhere

Entitle also helped us by enabling temporary, just-in-time access for high-privilege accounts. We use Entitle internally and within our client environments where standing high-level privileges might introduce unacceptable levels of risk. It gives us just-in-time management for our engineers, so we can grant access based on the context of how users need to access each resource in their daily workflows. With Entitle, we no longer use risky standing access by default, such as leaving a “master key” somewhere in Azure or other cloud contexts.

Throughout our implementation of Entitle, we've seen a drastic reduction in the number of users who have standing high-elevation privileges, like domain admin or global administrator.

“Throughout our implementation of Entitle, we've seen a drastic reduction in the number of users who have standing high-elevation privileges, like domain admin or global administrator.”

The biggest piece of feedback that I've seen around Entitle has been that, compared to other just-in-time tools, the ability to bundle entitlements together has significantly simplified elevation when someone needs multiple roles at the same time. It's not just about managing elevation, but also about privilege management on the whole.

A Single-Platform Approach to Managing the Identity Landscape

The single biggest benefit of working with BeyondTrust is the ability to manage our identity landscape across environments—not just our own, but within DR and client environments.

Having BeyondTrust products for so many aspects of our business has allowed us to simplify identity security. It's been great for us to have one provider for almost anything we want to do privilege-wise. Additionally, the Pathfinder platform has enabled us to set up a single entry point and one method of authentication, simplifying our user access to the entire portfolio.

“The Pathfinder platform has enabled us to set up a single entry point and one method of authentication, simplifying our user access to the entire portfolio.”

A Valued Partnership Leads to Continued Investment

For an MSP like our company, the partnership matters just as much as the technology. One of the reasons we continue to expand our use of BeyondTrust products is because of the trust we've established with their team.

Having complete transparency between our teams and BeyondTrust means we can plan realistically. We don't have to spend time and energy guessing which solutions will suit our use cases or working through vague answers from our account management team. Instead, we rely on the BeyondTrust team for honest, direct answers that help us make informed decisions about what will work best for our business.

This is important because, in addition to being BeyondTrust customers, we are an indirect reseller. We use these tools to protect our own assets, which gives us complete confidence when we recommend them to our clients.

What began as a search for efficiency led to something much bigger. With BeyondTrust, we gained a unified security framework that supports our growth without having to sacrifice control.



“Standardization is the value here. For seamless authentication, session logging, and consistent audit trails across every environment, our answer has been BeyondTrust. Together, we gained a unified security framework that supports our growth without having to sacrifice control.”

Secure Every Identity, Across Every Environment



Identity Security Insights®

Gain one holistic view of identities and access across your IT estate



Endpoint Privilege Management

Enforce least privilege across Windows, macOS, and Linux



Entitle

Enable just-in-time access with automated provisioning workflows



Remote Support

Securely access and support any device or system



Password Safe®

Gain visibility and control of privileged credentials and secrets



Active Directory Bridge

Extend and manage Unix / Linux authentication and group policies



Privileged Remote Access

Create identity-secure, just-in-time access to all your environments

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