BeyondTrust + ServiceNow

Transforming the Service Desk Into Your Strongest Security Layer

The Service Desk Is Now the Frontline of Identity Security

Service desks sit at the heart of modern enterprise IT, tasked with keeping staff productive and systems running. Yet help functions are increasingly targeted and exploited by cyberattackers. Password resets, device enrollment, and access troubleshooting can all be manipulated to bypass cyber defenses.

The challenge extends beyond human identities. Non-human identities (NHIs)—including service accounts, machine identities, and AI agents—are proliferating across enterprises. Moreover, NHIs are typically far less governed than their human counterparts, making them attractive targets to attackers. In an era where identity is the new perimeter, a unified view of every identity and every privilege escalation path is critical.

Three Risks Every Organization Must Address

Social Engineering & Vishing
Attackers impersonate employees or contractors to convince service desk agents to reset credentials, enroll new MFA devices, or override standard controls. Exploiting internal phone systems, they appear as trusted internal callers, lending calls an air of legitimacy that enables them to bypass even well-trained staff.

Standing Privilege & Excessive Access
Service desk staff typically hold broad, continuous permissions across multiple systems. This standing privilege dramatically widens the blast radius of any compromise so that a single breached identity can, in some environments, provide a pathway to the entire organization.

Third-Party & Outsourced Support Risk
The risks multiply in organizations that outsource support functions. A breach involving a third-party provider can cascade across multiple clients simultaneously, with no reliable way to track who performed specific actions.

BeyondTrust + ServiceNow: The Ultimate Better Together Offering

BeyondTrust and ServiceNow are working jointly to close these gaps, transforming ITSM into your organization's strongest security layer.

- **Seamless Integration:** Ensure enhanced service levels, minimal disruption, and easy deployment by leveraging native ServiceNow integrations
- **Stronger Security:** Monitor privileged sessions, enforce least privilege, eliminate standing privileges, and enable just-in-time (JIT) access control from within ServiceNow.
- **Improved IT Productivity:** Automate workflows and secure remote access to enhance IT efficiency and improve incident response times.
- **AI Agent Governance:** Gain full visibility and control over autonomous AI agents (including ServiceNow AI agents) and the credentials, roles, and permissions they inherit.
- **Compliance & Audit Readiness:** Ensure audit readiness by capturing every access decision, session recording, and policy action within a ServiceNow record.

BeyondTrust | servicenow

Key Outcomes

- **Identity Security Insights® & ServiceNow SecOps**
  Gain a unified, graph-based view of every identity (human, machine, and AI) and map every privilege escalation path across your environment. Detections flow directly into ServiceNow Security Incident Response (SIR), enriched with risk scores, attack path data, and playbook recommendations. Benefit from end-to-end visibility, detections, and intelligent recommendations for any identity—including AI agents—across your environment.

- **Endpoint Privilege Management & ServiceNow**
  Enforce least privilege on all managed Windows and Mac endpoints by removing local admin rights while allowing users to request elevation through ServiceNow. The JIT integration is the first to support both application access and admin access. Leverage it to automatically create Incidents, Change Requests, or Service Catalog items, with approvers acting directly in ServiceNow and the full decision trail written to the ticket. Access is granted or denied instantly at the endpoint.

- **Remote Support & ServiceNow ITSM / CSM**
  Improve service desk efficiency with secure, audited remote support sessions initiated directly from ServiceNow tickets or CSM cases. Session transcripts, recordings, and system information are automatically written back to the originating record, ensuring compliance, reducing downtime, and improving end-user satisfaction with no manual data entry required.

- **Privileged Remote Access & ServiceNow ITSM**
  Enable just-in-time privileged access for employees, vendors, and OT systems directly from ServiceNow Change Management, Incident Management, and CMDB records with no plain-text credentials exposed. Session recordings and audit logs are automatically written back to the ServiceNow record, helping satisfy even the most demanding compliance requirements.

- **Password Safe & ServiceNow ITSM**
  Secure credentials for both human users and ServiceNow AI agents. Check out any privileged credentials, including those for AI agents, dynamically at runtime. Credentials are never stored statically, and every checkout triggers automatic rotation with a complete audit trail. Access is requested and granted via ServiceNow ITSM approval flows, with break-glass and auto-approve options for time-sensitive scenarios.

CUSTOMER SUCCESS

Keller Group
"With BeyondTrust and ServiceNow, we now have a single, unified workflow for every access decision. Our service desk team no longer holds standing privileges — every elevation request is ticket-driven, approved, and auditable. It's transformed how we think about IT security."

–Senior Security Administrator, Keller Group

Rethinking Service Desk Security

For organizations navigating today's threat landscape, service desk security must be embedded in a broader identity security strategy. BeyondTrust and ServiceNow deliver this, with **least privilege access, just-in-time elevation, dynamic identity verification, and real-time monitoring** — natively integrated, automated, and audit-ready. All integrations are available on the ServiceNow Store.

Explore BeyondTrust + ServiceNow

LEARN MORE