



Workload Credentials

Authenticate with short-lived, auto-expiring credentials, reducing standing privilege, static secrets, and credential exposure.

Non-human identities (NHIs) outnumber human ones by 80:1.*

The access keys for NHIs sit in config files and repos for months, with teams stitching together native secrets managers that add complexity around ownership and auditing. While some providers issue ephemeral credentials natively, this configuration often stalls or breaks at enterprise scale, leading to errors, breaches, or failed audits.

BeyondTrust Workload Credentials solves these challenges with a streamlined approach to generate and auto-expire ephemeral credentials, reducing risk while accelerating audits. Short-lived credentials are generated on demand through OIDC Workload Identity Federation to authenticate CI/CD pipelines, Kubernetes services, and AI agents.

Workload Credentials then adds the crucial governance layer that native OIDC lacks, with centralized policy-as-code, deny-by-default enforcement, and a single audit trail.

*SASE/SSE Platforms Must Adapt to Secure the Rise of Agentic AI and (NHI) Non-Human Identity Access. Gartner. By Charanpal Bhogal, Charlie Winckless, Neil MacDonald, & John Watts. Dec 2025.

80% of initial access vectors used by access brokers are credential-based attacks.

Microsoft Digital Defense Report 2025. Microsoft. October 2025.

39% of breaches had credential abuse in the attack chain.

2026 Data Breach Investigations Report. Verizon. May 2026.

85% of organizations have plaintext secrets embedded in their source code repositories.

2025 State of Cloud Security Report. Orca. June 2025.

✓ **Eliminate Long-Lived Secrets**

Authenticate with OIDC Workload Identity Federation to obtain access on the fly, with workloads that prove their own identity.

✓ **Generate Dynamic Ephemeral Credentials on Demand**

Issue short-lived credentials that auto-expire.

✓ **Deliver Seamless Governance, Policy, and Auditing**

Track every credential issuance in a single, searchable record with a centralized control plane for defining, monitoring, and auditing workload access.

✓ **Rapidly Reduce Risk**

Minimize credential exposure and standing privilege by replacing static secrets with identity-based authentication in just a few simple steps.