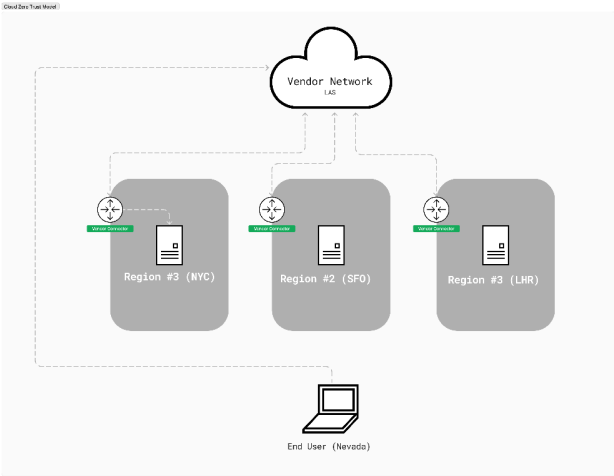
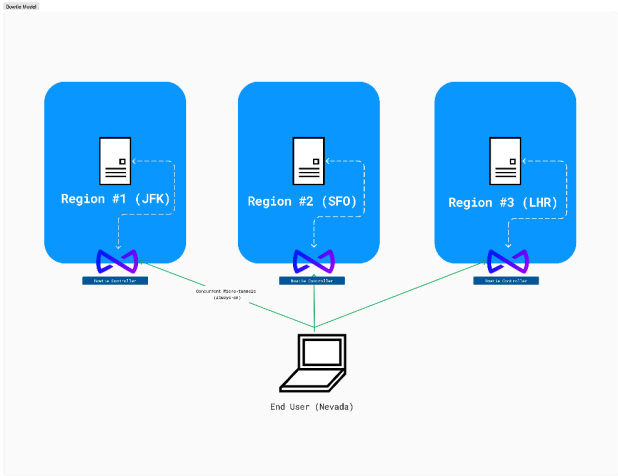
Product Overview

Bowtie is a next-generation distributed network security platform, engineered to offer seamless and secure access to private, public, and SaaS resources.

Unlike some systems, Bowtie does not centralize and backhaul customer traffic through a Bowtie network. Instead, Bowtie's architecture creates a cloud-like encrypted service mesh inside customers' existing networks, close to users, resulting in greater efficiency, speed, and security.

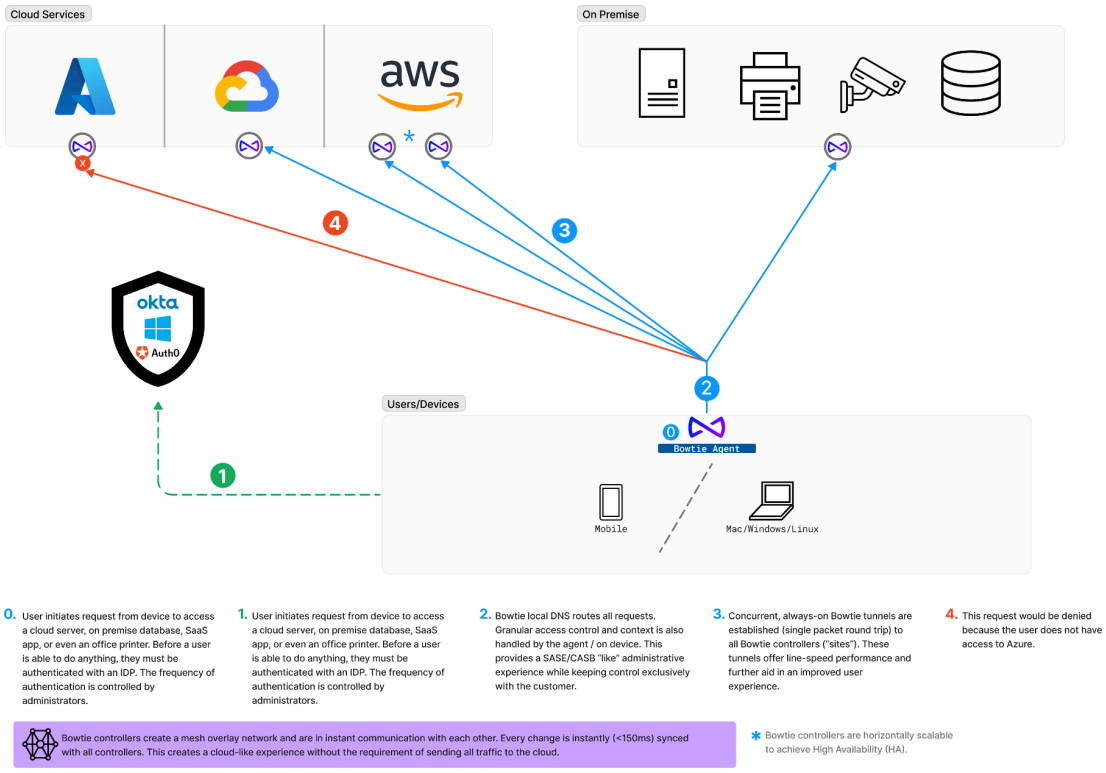




Conventional enterprise networks are a patchwork of site-centric security protocols. They lack context, stop working at perimeter boundaries, and necessitate unwieldy solutions like VPNs to let businesses function beyond network borders. Bowtie addresses these issues head-on by reimagining how enterprise networks are built as a user-centric, decentralized platform operating across user devices and enterprise resources.

Private Resource Access

Bowtie's first use case is to enable Zero Trust Network Access to private enterprise resources. With a user-invisible agent, Bowtie establishes parallel concurrent connectivity to Bowtie controllers at every enterprise network resource, such as a virtual private cloud, datacenter, factory, office, or anywhere the enterprise has resources deployed. The control plane uses a distributed, self-healing service mesh inside your network to build and manage configuration.



Private Access features include:

- Single packet round-trip connection establishment
- Multiple **concurrent connections** to each enterprise resource
- Near **line-speed** throughput
- Layer 3 connectivity, **all ports and protocols**, existing clients and software function without modification
- Conflict-free networking, **no risk of RFC1918 overlap**. Supports connectivity to networks with overlapping address space.
- Direct, **shortest path** through the Internet to private resources
- No **end-user** interaction required
- Rich context for **access control decisions**, including user and device attributes like full disk encryption status, endpoint protection software, patch level, time, and geography

Unlike many security platforms, Bowtie is intentionally not an operational member of the customer's mesh fabric. This design choice ensures that the entirety of the mesh network remains under the customer's control, allowing for a greater degree of customization and security. Moreover, policy decisions can be executed right on the device, further enhancing the speed and responsiveness of Bowtie's system.

Public Resource Access

Building on Bowtie's distributed mesh control plane, Bowtie is able to provide a highly available identity proxy for public SaaS products. In this model, access control decisions to SaaS products can be enriched with attributes such as device status, geography, time, patch status, and endpoint protection status. The identity proxy can also admit users without the Bowtie agent running, either temporarily or by exception, such as for contract employees or vendors. By joining advanced security protocols with an intuitive user interface, we ensure that access control is both versatile and robust, effortlessly adapting to your organization's unique security needs.

- Highly available identity proxy at the SAML2 layer allows **enriched access control decisions without IP address allowlisting**
- Allow temporary access **from non-Bowtie protected devices**
- **Mitigate the impact of cookie theft** by requiring access from Bowtie protected devices

SaaS / Web Filtering

Leveraging Bowtie's agent which utilizes both DNS and packet filtering, on-device enterprise traffic policy can be enforced for general web traffic. On-device logic enforcement accelerates traffic flows, providing near-transparent web access for users. In addition to significant performance acceleration, content enforcement scales horizontally without the cost of backhauling all user traffic to central content inspection sites.

- On-device traffic policy enforcement provides **native client performance**
- Distributed mesh control plane ensures **timely client policy updates** and exception reporting
- **Always-on visibility** into client traffic flows that can feed into existing SIEM tools for global visibility without brute-force traffic backhauling
- **Shadow IT discovery** utilizing correlated traffic inspection

Use Cases

Use Case	Bowtie Solution
ZTNA Initiative	Support for Zero Trust Network Access journey leveraging Bowtie's granular access control and seamless client experience, which ensures all employees, regardless of department, are able to use Bowtie.
Legacy VPN Replacement	Achieve the same outcome of securing access with a traditional VPN without the common pitfalls by deploying Bowtie's secure access solution.
Network Modernization	Networks are no strangers to technical debt, becoming unruly to manage with a variety of patchwork solutions. Bowtie creates a conflict-free overlay network that can help transition to a new enterprise fabric.
Multi-cloud access and uniform policy enforcement	Simple, environment-agnostic deployment means you can have Bowtie up and running quickly, without having to consider the security implications of leveraging a reverse proxy to access new cloud services. Unique networking techniques mean all you need to know is the names of your new services, even if networks overlap.