veza | Customer Journey Barracuda

Barracuda teams up with Veza for modern, automated data security

Global cybersecurity solutions provider leverages data authorization to protect sensitive customer data and meet its compliance requirements

Industry
Technology - Security

Organization Size
1,700 Employees

Headquarters
California, United States

Veza features
Authorization Graph
Open Authorization API
Access Workflows
Tags

Challenges
Manual process to pull permissions and entitlements of users out of all corporate systems and apps

Benefits
Certification interface that empowers system owners to responsibly manage data

Extensible platform that allows secure authorization for custom applications

Key Integrations

Custom support app
GitHub
Azure
AWS

Thousands of customers worldwide trust Barracuda's cloud-first security solutions to safeguard their data and applications from a wide range of threats. The California-based company specializes in cybersecurity and, in the course of protecting its customers, filters quite a bit of sensitive data through its systems.

> **Everything we do handles data — it's central to our business. Customers trust us to protect what they share with us, so we take data security very seriously.**
>
> Dave Farrow • Barracuda's VP of Information Security

At first, the 15-year-old company built security appliances, but has since moved to the cloud to provide cloud security to its many customers that have also migrated. The centrality of data security to its business and its embrace of the cloud prompted Barracuda to seek a modern, cloud-centric solution capable of bringing zero trust security controls to data, which ultimately led them to Veza.

Barracuda is committed to upholding the highest security standards for the data it manages and stores for its customers. Key to that mission is knowing exactly who is accessing what, and how. Initially, that meant protecting access to applications, resources, and data using multi-factor authentication (MFA) at the front door. However, they soon realized that MFA was not a magic bullet, as they still found it difficult to ensure that users had the correct access levels or permissions within all of their applications. That's when the need for authorization came into play.

Streamlining access and entitlement reviews to make an unmanageable process manageable

A big challenge in governance is knowing who has access to what. The stock answer is to grant access using Active Directory (AD), but the ramifications of AD group design are not always clear. "Automating the ability to know who has authorized access — in every group at any given time — is critical. When you look at the gamut of systems and applications, and there are lots of them, it gets quite complex.

That was the core issue we needed to address," says Barracuda's VP of Compliance, Risk & Security, Riaz Lakhani. Addressing that issue was the key to meeting Barracuda's contractual commitments for protecting customer data and for complying with its SOC 2 audit requirements.

SOC 2 (System and Organization Controls) defines the criteria for managing data along five trust principles: security, availability, processing integrity, confidentiality, and privacy. The mandate calls for regular access reviews of all entitlements and permissions — a burdensome task for a large organization like Barracuda. "Our security and compliance team kept asking if there was any way to pull the info out of AD and tie it together with the various permissions that unique user identities had for accessing our systems, apps, and data resources. It was unmanageable and took a lot of time, because it was a very centralized, laborious process and not at all scalable," says Lakhani.

The solution? Barracuda engaged Veza to help decentralize the process. Leveraging Veza's identity-to-data access controls, individual system owners and managers are now able to see on a single pane of glass the information they need to take action on entitlement anomalies and conduct due diligence for access reviews and audits in a timely fashion. They can now quickly produce evidence that they have complied with any needed adjustments to specific data access authorizations. The solution has enabled Barracuda to meet one of its key objectives — to implement the principle of least privilege, whereby they can now see on a granular basis who is explicitly authorized to interact with any given data source.

> Stitching together identities with data sources and showing the connections between them in a way that's easy to consume — it's a simple idea, but a complex problem to solve. Veza makes the process of understanding who has access to what really, really easy.

Dave Farrow • Vice President, Information Security, Barracuda

Support for popular systems, apps, tools, and databases, including homegrown applications

Barracuda wanted a comprehensive solution that extended beyond systems like AWS that most companies use — a solution capable of providing complete visibility of how each support engineer was accessing customer data. The company evaluated products and technologies that only provide visibility into resources, apps, and infrastructure, but not data, and decided that wasn't enough. They needed to see what was going on in every one of its applications. It was then that Dave Farrow reached out to Veza to see if it could POC a use case that would factor in visualization across all of Barracuda's products, all its internal tools and systems, even homegrown ones.

"Help me solve that problem and I'll evaluate your product and champion it," said Farrow. Soon enough, Veza returned with a prototype push API that enabled Barracuda to get unprecedented insight into their systems. "My focus was on integration, bringing in additional data sources. Nobody but Veza was doing that."

Integrating a broad range of data sources with Veza's Open Authorization API

Veza's Open Authorization API supports a growing number of data systems and applications right out of the box, but also allows Barracuda to introduce its own applications. Self-service for integrating its own data sets enables Barracuda to advance its agenda independently, on its own timeline. Farrow noted that the company has several homegrown applications, but was never exactly sure who was using them or accessing the data. By ingesting the authorization models of its homegrown systems into Veza, he now gets the same picture for them as he did for public cloud systems. "Being able to visualize our private customer support systems and rolling that out to our access review managers gives us a broader picture of risks to the enterprise."

In addition to its homegrown applications, Barracuda's key integrations include its identity provider (IdP) and other core systems that have critical data. Atlassian, Jira, and Bitbucket are currently being developed by Veza, while Barracuda anticipates further integrations, including its CRM, ERP, and HRIS applications, which Veza will soon be adding to its portfolio of supported systems and apps.

An automated, time-saving solution for responsible data management and protection

With Veza, Barracuda developed a modern, automated solution that sharply reduces the need for manual processes and delivers reliable information, visually, to expedite access reviews. It's a real time saver. System owners can evaluate in real time who has access, limit access only to those who truly need it when they need it, and decide whether authorized access should continue. The information gleaned is used to produce reports and can be handed off to auditors, right out of the gate.

Learn how to incorporate Veza into your data security initiatives at www.veza.com.

About Veza

Veza is the data security platform powered by authorization. Our platform is purpose-built for multi-cloud environments to help you use and share your data more safely. Veza makes it easy to dynamically visualize, understand and control who can and should take what action on what data. We organize authorization metadata across identity providers, data systems, cloud service providers, and applications — all to address the toughest data security challenges of the multi-cloud era. Founded in 2020, the company is remote-first and funded by top-tier venture capital firms including Accel Partners, Google Ventures, Norwest Venture Partners, and True Ventures. To learn more, please visit us at veza.com.