SALT

Berkshire Bank

CASE STUDY

Berkshire Bank strives to be a socially responsible, community-dedicated bank. With more than 100 branch offices throughout New England and New York, the company provides business and consumer banking, mortgage, wealth management, and investment services.

As with so many financial services organizations, Berkshire Bank is using more application programming interfaces (APIs) than ever in order to share information online. APIs help the bank roll out new and differentiated services, including ones that make it easier to effortlessly on-board new customers. At the same time, however, the bank's security staff are mindful of the security vulnerabilities that are inherent in widespread API usage.

"We want to be a business enabler," says Ryan Melle, CISO and senior vice president at Berkshire Bank. "We want to enhance digital transformation for ourselves and our customers, and the best way for us to allow business to move forward quickly is to stay out of the way, but our top priority is keeping everything secure."

The company recently deployed MuleSoft for API integrations. The MuleSoft platform connects applications, data, and devices and automates business processes, facilitating the sharing of data between third parties.

Melle explains, "We're seeing an increase in the number of API transactions, but we're also seeing an increase in API attacks." To strengthen the company's security posture, Melle developed an aggressive zero-trust methodology and API security strategy within the company's IT roadmap.

Melle and his team defined the primary capabilities the bank sought as core to developing its API security strategy. The top needs included API inventory, API design security, and runtime protection. Given those requirements, Salt Security quickly rose to the top of the possible solutions for Berkshire. "We considered other solutions, but they didn't provide the range of capabilities we needed, and we found the Salt architecture unique. The Salt system got stood up in a day, so it's been simple operationally too," says Melle.

BerkshireBank

Berkshire Bank provides business and consumer banking, mortgage, wealth management and investment services. The bank has approximately $12.1 billion in assets and operates 105 branch offices in New England and New York.

Headquarters
Boston, MA

Founded 1846

www.berkshirebank.com

Top security use cases for Berkshire Bank:

- **API inventory:** Berkshire Bank leverages Salt to automatically and continuously discovers all APIs, including third-party APIs, capturing granular details about them to help eliminate blind spots, assess risk, and keep APIs protected – even as the bank's environment evolves and changes.
- **data protection:** Salt offers Berkshire a range of data protection functionality, including API and sensitive data discovery to uncover undocumented APIs and potential data exposures that impact employee and user privacy, API attack prevention and blocking to stop attackers early in their attack campaigns, and API-centric incident response to provide context for operations teams to respond quickly and effectively.
- **API design security:** With the Salt platform, Berkshire has an easy way to provide developers with insights they can use to strengthen the APIs as they're developing APIs. Salt provides an analysis of gaps against API security best practices in pre-production.
- **runtime protection:** Salt provides dynamic runtime protection that identifies behavior anomalies that indicate attacks including credential stuffing, brute forcing, or scraping attempts.

We considered other solutions, but they didn't provide the range of capabilities we needed, and we found the Salt architecture unique."

– Ryan Melle, CISO and SVP

SALT

Salt Security protects the APIs that form the core of every modern application. Its patented API Protection Platform is the only API security solution that combines the power of cloud-scale big data and time-tested ML/AI to detect and prevent API attacks. By correlating activities across millions of APIs and users over time, Salt delivers deep context with real-time analysis and continuous insights for API discovery, attack prevention, and shift-left practices. Deployed in minutes and seamlessly integrated within existing systems, the Salt platform gives customers immediate value and protection, so they can innovate with confidence and accelerate their digital transformation initiatives.

CS-BRKS-20220721

Request a demo today!

info@salt.security

www.salt.security