BERKSHIRE BANK

Implements SOC-based Security with RSA

AT-A-GLANCE

Challenges

– Berkshire Bank is obliged to ensure all customer and corporate data is kept safe from unauthorized access or sharing.
– As its employee base grew, its manual controls were becoming untenable. It wanted to create a Security Operations Center and centralize all security-related incidents.

Results

– RSA NetWitness® Logs and Packets pulls security data and insights across the business into one central tool, allowing greater visibility of threats and current security posture.
– With RSA Archer, the bank has centralized all risk and policy management into one tool, removing duplication and eliminating the risk of important tasks being missed.
– RSA Via Access enables application owners to monitor, review and provision application access quickly and centrally.

"The real-time dashboard is an extremely powerful tool to have at your fingertips. You can look at what's happening across the environment 'right now', and you can respond within minutes to ad hoc questions from stakeholders. We can also give auditors read-only access so they can go in and pull any information they need and see exactly what we've done."

RYAN MELLE, VICE PRESIDENT, INFORMATION SECURITY OFFICER, BERKSHIRE BANK

BERKSHIRE BANK
America's Most Exciting Bank

RSA

For over 165 years, Berkshire Bank has prided itself on delivering excellent service and performance for its customers. It operates a network of financial services, covering banking, insurance, and wealth management. Headquartered in Pittsfield, Massachusetts, the bank has 93 full-service branch offices throughout New England and New York.

What drove your security strategy?

Berkshire Bank has grown substantially in the last five to ten years. It was important to us to build out our infrastructure so our business can continue to grow. It's critical we get this done now, as trying to do a user access review with a larger number of employees manually is just not going to be feasible and it's definitely a security risk. The executive team and the board of directors understand that if you want to grow, you need the right foundations. Otherwise you can build great walls but they'll just crumble.

Building a Security Operations Center (SOC) and centralizing all our security-related incidents has been huge for us. Having the tools in place to see exactly what's happening and report on all activity in a timely manner is helping us shift the culture of the bank from being reactive about security, to being proactive.

Why and how are you working with RSA?

We've built a good partnership with RSA. We started off with VPN tokens many, many years ago just like many other companies. When we started looking at different tools for a vendor management program, we realized we needed to look at the bigger picture and not just keep building out silo tools. That's where RSA Archer came into play. We knew that we also needed a GRC solution and so we started talking to RSA about how we could address these needs in a cohesive way.

We're also using RSA Via Access, which enabled us to start monitoring and doing electronic provisioning, enabling our application owners to review applications electronically.

We've taken our time getting the implementation of RSA Archer, RSA Via Access and RSA NetWitness Logs and Packets right, but we're starting to see a lot of good information coming out of them now. We're building baselines of things we want to monitor, and this enables us to then look for deviations from that baseline. It's easier to do this now, with 1,200 employees than it'll be in two or three years' time when we have twice or three times that many.

What has it been like working with RSA?

It wasn't just a vendor relationship, it was a partnership. I think working with RSA was great – whether it was your account manager or the CEO it didn't matter. You were still treated as somebody that mattered.

What has the impact been on the way your team works?

Before we had our SOC in place, it would have been almost impossible to see if someone was trying to send out information they shouldn't be, and if it was it would have been many weeks or even months after the fact. Now, for example, we had an employee who had tried to send something out and we were able to detect it right away and respond in a matter of minutes. An analyst could contact the employee to check what they were doing and ensure they weren't creating a risk.

We're also taking proactive steps now like carrying out phishing tests. Someone clicking on something suspect will get a pop-up message warning them to be careful. So people are starting to get into that mindset of thinking about security and compliance as part of their daily work.

Our analysts can also look for abnormalities. For example, if you know Bob Smith logs in every day at 3 o'clock, then one day he logs in at 5 o'clock, you can check why. You can also reward people for good actions, like being proactive about keeping their data safe.

How important was company culture in driving the project's success?

Shifting that whole focus has been very important, and I think over the last two years our team has made great progress in changing people's mentality. It was very hard as there were some employees who'd maybe been with the company a long time and were being told they needed to change the way they did things – making their password more complex, not keeping it written down on their desk and so on.

How are you using the dashboard in RSA NetWitness Logs and Packets?

The real-time dashboard is an extremely powerful tool to have at your fingertips. You can look at what's happening across the environment 'right now', and you can respond within minutes to ad hoc questions from stakeholders. We can also give auditors read-only access so they can go in and pull any information they need and see exactly what we've done. They can see the incident journal, all the attachments, remediation records and anything else they need around a specific incident ticket.

As we start building SLAs around response times, and as we grow, we will be able to continue this close monitoring. We're planning to dive more into application details and behavioral analytics, building out from the baseline we've already established.