

BERKSHIRE BANK

Consolidates Security Operations with RSA NetWitness® Logs and Packets

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 needed a centralized, automated system to support secure business growth.

Results

- RSA NetWitness Logs and Packets pulls security data and insights from across the business into one central tool, allowing greater visibility of threats and current security posture.
- Analysts can take a more proactive approach to protecting customer data, tackling possible risks before they become threats.
- Employees are now more security-conscious and executive management has recognized the new system's value to the business.

“RSA NetWitness Logs and Packets is now our centralized security system. If somebody had tried to send a file out before, nothing would happen. If you try to send a file out right now, one of my team members is going to be calling you right away and saying ‘hey what are you trying to do?’.”

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

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.

Why is security important to you?

Being in the banking industry we're heavily regulated, so it's important that we are complying with our regulations. We also have a huge responsibility to protect our customer information.

What drove your decision to implement RSA Archer?

Three or five years ago, when we had only about 500 employees, we handled most of our security manually. We'd look at user access reviews or virus activity, or people sending files in and out of the organization. However, as the bank expands to say 1,500 employees, it gets harder to manually track everything. We needed to centralize everything as opposed to having everything in different places.

When we were building out NetWitness Logs and Packets we had an idea of the key things that we wanted to start looking at. For example, data loss prevention was important, because as a financial institution one of our top goals is to make sure that customer information is safe.

How are you using RSA NetWitness Logs and Packets?

RSA NetWitness Logs and Packets is now our centralized security system. 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.

NetWitness Logs and Packets for us is still relatively new. When we first put it in, it was the middle man. We have multiple other tools that send information to NetWitness Logs and Packets, we've built rules and alerts, and that goes into security operations. In the last few months we have started to switch from that, focusing on what more NetWitness Logs and Packets can enable us to do. For example, we're now much better placed to hunt for abnormalities. We identified one recently, and were able to dig into it and identify that we had a server with some issues. It was

nothing that posed a risk to the bank but it was impacting efficiency and we were able to respond to it.

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.

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.

What results have you seen so far?

We've had a lot of small wins. For example, if an employee keeps getting locked out of an account, now we can go in and find out why very quickly. I think the impact is going to grow as we get more used to the tool and take advanced training. We're looking to do a lot more with some of the versions that are coming up, so I think down the road it's definitely going to help us.

Already we're showing the value of being proactive, which has secured buy-in from executives.

What advice do you have for others?

I always tell people to keep it small, get your road map, understand what your resources are, what your executive buy-in is, what your budget is, and what your biggest risks are. If you try to cram in too many objectives up front, it's not going to be successful. You really want to start with one initiative that you feel will give you the best results and the most visibility, then you can build on that success. In our case, we started building all our controls in Archer, then looked at what the security operations team most needed from it - information – and provided them with that using NetWitness Logs and Packets. Now we have NetWitness Logs and Packets, we can feed in more pieces to give us greater visibility.

CONTACT US

To learn more about how RSA products, services, and solutions help solve your business and IT challenges contact your local representative or authorized reseller – or visit us at www.rsa.com

©2016 EMC Corporation. All rights reserved. EMC, RSA, the RSA logo and RSA NetWitness Logs and Packets are the property of EMC Corporation in the United States and/or other countries. All other trademarks referenced are the property of their respective owners. Berkshire Bank