Redjack

Retail Firm Improves Business Continuity and Disaster Recovery Planning

Creates and Tests Plans to Recover From Outages in 15 Minutes

INDUSTRY	MANAGED ASSETS	CUSTOMER SINCE
Retail	**> 3 million**	**2017**

CUSTOMER CHALLENGE

Business Continuity and Disaster Recovery

The company — an American multinational retail corporation that operates chains of retail warehouses, hypermarkets, discount department stores, and grocery stores — was aware of cyberattacks on other companies that had disrupted critical business functions and was determined not to have it happen to them. Their goal was to be able to stand a critical business function back up in 15 minutes or less after it went down so that the company could restore its ability to do business. They had already identified their critical business functions (such as payroll, supply chain management, and communications) and were working on a plan to reduce their risk of failure. To do this, however, the company needed an accurate asset inventory that could be mapped to their critical business functions.

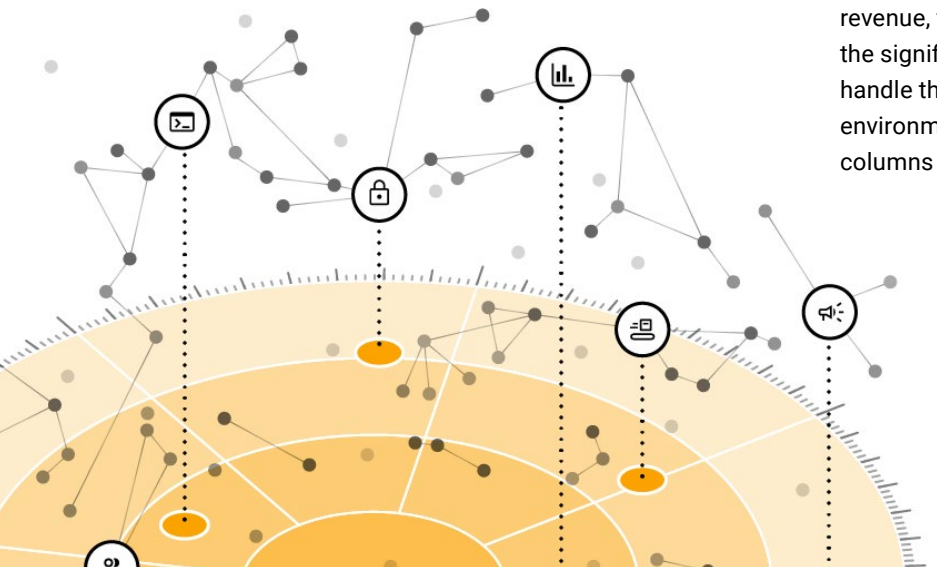
In the past, the company had worked with consultants to compile an inventory but felt that surveying the IT staff wasn't getting the job done.

Why Redjack

Redjack was chosen not just because the Redjack platform was able to give the company a complete asset inventory quicker than its existing solution, but because Redjack was able to connect assets to business functions. Redjack was able to do this because of its ability to ascertain relationships and map interdependencies between assets. This provided an additional layer of visibility and data that the company could use while creating a business continuity plan.

There are many techniques that can be used to create an asset inventory, however, most of these techniques are also excessively manual, tedious, and time-consuming. Many ignore large categories of assets, such as how cloud-based asset management services can't give you a view of your non-cloud assets or how physical asset tags can't keep track of software-based assets and neither solution has much visibility into containers. The industry-leading practice is to compile anything that has asset intelligence into a single asset inventory, but this lacks evidence and can't be proven to be correct or reliable. It's simply a bit better than the status quo and easy to achieve.

Redjack uses a communications-based technique to compile a complete, accurate, and dynamic asset inventory. By placing software sensors in the company's network, the Redjack platform captured communications data and used AI-driven analysis to create a map of the company's corporate infrastructure. This gave the company complete visibility into the true extent of its connected IT asset infrastructure, including which assets are interrelated or interdependent. This technique ensured that the company could connect assets to the critical business functions that they supported. This comprehensive and up-to-date IT asset inventory would be able to facilitate the organization's business continuity and disaster recovery (BCDR) planning. Redjack is also able to enhance the inventory with data from third-party partners, such as Tanium, to deepen the amount of information provided.



Business Results

Business Continuity and Disaster Recovery

One of the company's top priorities was the resiliency of its payroll system. They had evaluated the cost and, considering the size of the company, the total potential fines, penalties, and fees that the company would have to pay would be in the range of millions of dollars a day for every day the payroll system was down. Every hour the network wasn't working had a material impact on the business.

As a first step to building resiliency, the company wanted to verify the asset inventory information that it already had. The existing information had been manually compiled using questionnaires and looking at systems administrator's shared drives and it sized the payroll system as comprising 24 systems. Redjack deployed its sensors into the environment, focusing on known payroll system assets. The Redjack sensors collected communications metadata flowing between those assets and the wider environment. The Redjack platform was quickly able to determine that the payroll function was actually comprised of around 400 systems, with another 2,500 systems that communicated with payroll systems but were not considered a part of the core business function.

In order for a business function to operate and survive a failure, the organization had to understand what was going on around it. Redjack could demonstrate how these assets were connected, illustrating how the failure of one could have a ripple effect on connected assets. Redjack ended up pointing out large gaps in the company's understanding of its environment.

In the end, using Redjack the customer was able to not only build a comprehensive BCDR plan but to run simulations to verify that the plan could be carried out. Critical functions could be brought back online in 15 minutes or less, saving the company from potentially millions of dollars of lost revenue, fines, and other monetary damages, not to mention the significant non-monetary impact. Redjack was able to handle the massive scale of data generated by the customer's environment and provide actionable insights instead of just columns of numbers.

Identify Forgotten Legacy Network Elements

Enterprise networks evolve over time. As companies expand and add new infrastructure and systems, some assets and tools will be standardized and brought in line with the new infrastructure, while other parts are left in place to quietly keep doing their job until they drift into obscurity and obsolescence. This can cause problems later down the road.

As an example, the company decided that, as part of their planning they wanted to make sure that their communications infrastructure would still work during a disaster. In order to coordinate a response, they needed to be able to use email. The company had well over a million email addresses with a correspondingly huge volume of email flowing through the system at any given time, which made everything more complicated. It was assumed that everything would be fine, however, because they were using Microsoft Office 365. It was assumed that Microsoft's systems would still be running even if the company's systems went down. However, Redjack sensors found nearly 50 email servers and relays within their infrastructure. It turned out that these servers either routed email independently of Microsoft Office 365 or existed as a legacy bridge or gateway.

After working through the process with Redjack data, the company was able to test bringing all of their communications back up from total failure in less than 15 minutes. There was no way the company could have done that without knowing how it all worked, and what order to bring assets online.

Conclusion

Redjack was able to provide this customer with not only a complete and accurate asset inventory but also a comprehensive map of how their assets supported their critical business functions. Using that information, the customer was able to create comprehensive BCDR plans that allowed them to restore critical business functions in 15 minutes or less. Beyond planning, the customer was able to run simulations proving the effectiveness of those plans while using Redjack to troubleshoot and fine-tune their process. Overall, the customer was able to gain increased visibility into their environment and improve their ability to prepare for, respond to, and recover from cyberattacks and outages.

About Redjack

Redjack delivers total asset visibility and AI-powered business insights for cyber resilience. Our platform empowers enterprises to safeguard vital business functions, meet cyber regulatory standards, and digitally transform to align with business objectives.

Visit redjack.com

Redjack