tenable™
network security

Broadridge Financial Solutions

Overview

Broadridge Financial Solutions was founded in 2007, as a spin-off of ADP, and has rapidly grown to become a $2.1 billion leader in securities processing, clearing and outsourcing and investor communication products. Its 6,000 employees serve a global customer base, with offices throughout Europe and Asia, and also in Australia and South Africa.

The company had the unusual opportunity to create security systems and policies from scratch; it also needed to establish processes that could keep up with extremely rapid growth.

Business Needs

Two intersecting needs defined the challenges of a rapidly changing market that is shifting the burden of security to its key vendors:

- Broadridge's security systems and processes needed to drive best-in-class compliance behavior across the enterprise – integrating business units that had previously operated with a great deal of autonomy
- It needed to competitively demonstrate this company-wide commitment and capability to customers – to showcase how Broadridge meets evolving industry standards, and uses its security processes as a key competitive differentiator

Customer Demands

In the financial services industry, the ability to protect customers' data is non-negotiable. It's also becoming a critical success factor in competing for new business.

When Jonathan Klein joined Broadridge in 2008, he saw an immediate need to address this growing market pressure. He also had a vision: For consistent, complete systems that would be used across the organization, creating a proactive compliance-driven culture. This new twist on operational excellence could be turned into a compelling sales advantage with customers who are increasingly concerned about the economic and social implications of a data breach.

Klein knew that first-rate security starts with communication, and then education. But Broadridge's network security team faced some specific challenges; the vulnerability and compliance reports it relied on were too raw and contained too much undifferentiated data to be useful. As a result, the IT group didn't bother to read them.

"The reports were overwhelming and simply indecipherable," Klein said. "It's impossible to educate employees on security procedures when you can't effectively communicate with them."

It became clear that its patch management process needed better tools. The team wanted a streamlined, effective process for scanning for vulnerabilities, and identifying, applying, and testing patches.

> "In the finance industry, IT security is more than reducing the risk to your company. If you don't have the right tools, people, and process in place, you will run afoul of your customers. Since overhauling our process, not only have we been able to make our networks more secure – we can now point to our security standards as a key benefit our products deliver."
>
> ***Jonathan Klein***
>
> CISO, Broadridge Financial Solutions

Hearts and Minds, Through Better Data

To get employee buy-in and turn its security process around, Broadridge planned to introduce several new security strategies and tools:

- A completely in-house system. Broadridge wanted to liberate itself from its subscription-based tools, which was too costly and presented potential security risks.
- "If our vulnerability data had leaked, it could have exposed potential weaknesses in our network," Klein said. "We needed better data, housed internally, and readily available for analysis whenever needed it."
- Simpler, easy-to-use solutions, which would provide key insights on the most compelling data and security trends needing attention. The goal was to engage line-of-business managers, as well as security and IT specialists.
- A much more connected relationship between the security and network teams. Broadridge suffered from the common tensions that can divide security and network teams; Klein knew that creating a unified approach would be critical to success – which could be as simple as getting patches and other corrections rolled out quickly and consistently.

People, Not Products

After evaluating multiple security products on their scalability, ease-of-use, customizability, size of the vulnerability database, and other criteria, Broadridge selected several new solutions, including Tenable SecurityCenter, Nessus Scanner, and Passive Vulnerability Scanner.

Equipped with these new tools and armed with better data, Klein had what he needed to effectively communicate the security risks the company was facing, establish employee guidelines, and instill firm security policies company-wide. Business unit owners now have much more knowledge about how their own group is faring, and potential vulnerabilities, which also drives compliance.

One measure of success: Not long ago, business unit leads often neglected to set time for necessary patch deployments, saying their operations needed to run 24/7. Now everyone is scheduled, and it has become a natural part of business operations.

"Products are a means to an end – my goal was to educate our employees," Klein said. "The tools gave me the ability to present the right data to people, and drive change."

With a new security-driven perspective, Broadridge's gains include:

- Establishing security as a part of the sales chain. The team comfortably manages the growing intensity of inbound queries, and displaces competition with its new proactive approach.

"Our sales team highlights our security standards, and it adds value to our products," Klein said. "We've turned security from a cost into a revenue generator."

- Reducing the number of unpatched and incorrectly patched systems by 90% or more. The new repeatable process monitors events and scans for vulnerabilities, reducing the company's own risk profile.
- Creating its first enterprise risk management committee. This group brings network and security management leaders to one table, building a framework for conversation that helps tackle challenging issues.

Selling Security

Since overhauling its security process, Broadridge has uncovered an unexpected capability in its suite of security solutions: It now can leverage audit files for configuration management, which it will roll out this year.

Broadridge also plans to showcase its best-in-class security standards, making security a core part of its sales activity, and educating customers with clear ROI metrics.

"It's tricky to define the ROI of security products – because at one level, it's as simple as how widely and consistently the products are used," said Klein. "Strategically, it's about reducing overall corporate risk. The more I can institute security policies that are actively applied, the more I reduce our total risk exposure – and that's how I deliver quantitative business value to my company."

For More Information

Questions, purchasing, or evaluation:
subscriptions@tenable.com or 410.872.0555, x506
Twitter: @TenableSecurity
YouTube: youtube.com/tenablesecurity
Tenable Blog: blog.tenable.com
Tenable Discussions: discussions.nessus.org
www.tenable.com

tenable™
network security

For More Information

Questions, purchasing, or evaluation:

subscriptions@tenable.com or 410.872.0555, x506

Twitter: @TenableSecurity

YouTube: youtube.com/tenablesecurity

Tenable Blog: blog.tenable.com

Tenable Discussions: discussions.nessus.org

www.tenable.com