Case Study

Finastra

Adopts Integrated Cyber Defense Approach

Challenges

- No coherent security strategy across the newly formed organization
- Endpoints lack robust security control and protection
- Company culture does not prioritize information security

Solution

- Symantec Endpoint Protection
- Symantec Endpoint Encryption
- Symantec Advanced Threat Protection
- Symantec Email Security.cloud
- Symantec Data Loss Prevention
- Symantec Web Security Service
- Symantec Email Threat Isolation
- Symantec CloudSOC

Benefits

- Improved security visibility provides CISO team greater control
- More robust compliance with regulatory demands increases competitiveness
- ISO team gets more done with same personnel; force multiplier
- Security vendor consolidation significantly cut costs
- Integrated Cyber Defense Platform reduces complexity and risk
- Cloud-first strategy reduces data center requirements
- Better management of 12,000 endpoints for a geographically distributed workforce

Client Profile

Organization: Finastra
Site: finastra.com
Industry: Financial Services Software
Headquarters: London, United Kingdom
Employees: 10,000+

FinTech giant Finastra chooses Symantec™ as its cyber security partner and consolidates its security stack on Symantec integrated platform

Finastra is the third-largest financial technology business in the world. It's a new brand, formed in 2017 by the merger of Misys and D+H. A $1.9 billion business, it builds and implements innovative cloud-based technology for the world's financial services sector. Finastra's scale and geographical reach mean it has financial customers across the globe ranging from community banks and credit unions, to retail banking and lending institutions, to treasury and capital markets. Given the recent launch of its cloud-based platform FusionFabric.cloud—a platform service that champions innovation and collaboration—moving cyber security to the cloud was a matter of 'when' not 'if.'

Symantec Integrated Cyber Defense to the Rescue

Scott Barronton, Finastra's chief information security officer (CISO), has 20+ years information security experience across a wide range of Fortune 500 organizations, including senior roles at NYSE-listed retail and data information organizations. Reforming cyber security at Finastra was a must.

Even before the merger, D+H was a highly acquisitive organization. The task of integrating many separate companies and legacy technologies into one coherent security posture was a top priority. "Over time, point solutions were implemented across the organization," says Barronton. "With each new industry event, there's a new solution born. We had a great many security vendors in place. I don't have an extremely large security team so we couldn't scale to manage multiple solutions and legacy technologies." Barronton knew his team needed "tools do the work, to integrate, to talk to one another, and to be the multiplier for my team."

In the context of a sustained period of acquisitions and mergers, a focus on the basics also makes total sense. "The usual cause of security issues is not evil hackers," says Barronton. "It's far less glamorous. In our case, because we had no coherent vendor strategy, we had no reference point for security standards, no consistency to ensure there were no gaps, and no visibility into the organization's security posture. We had many tools—we had everything—but not enough understanding. I couldn't see what was happening, let alone deal with it."

"Symantec's Integrated Cyber Defense Platform is a great choice. Moving to an integrated platform takes the long view. Getting the foundations right, across such a vast organization, is obviously the first priority."

– Scott Barronton,
Chief information security officer (CISO), Finastra

"Symantec's Integrated Cyber Defense Platform is a great choice," says Barronton. "Moving to an integrated platform takes the long view. Getting the foundations right, across such a vast organization, is obviously the first priority. And it helps that by adopting a full suite of integrated products, we don't pay full retail price for individual solutions that have to be cobbled together. "

The list of challenges—network security, endpoint security, email security, cloud access infrastructure and applications— was long. Which should get the most attention? "They're all important, yet sometimes we found ourselves playing whack-a-mole," says Barronton. "We would knock something down on one end, but it would pop up somewhere else." The Symantec solution enabled Finastra to become better aligned with its own standards. "The more that we put the correct Symantec technologies and controls in place, the easier the mole becomes to hit," says Barronton.

The first task was to remove existing encryption and endpoint solutions. "For each bit of the business, as they came up for renewal, we moved to Symantec," says Barronton. "Multiple products, multiple contracts, multiple renewal timelines, but we got there. The context here was a tangled web of systems, so the prior situation was very complex with multiple single-point solutions that didn't talk to each other. There was lots of unpacking to do so we started with the basics and then built upon the foundation."

Journey to the cloud

The Cloud Generation wants information now, whether they are on premises or remote and, as Barronton explains, Finastra's security posture has to cover that data wherever it goes. "The Cloud Generation has really changed the way we look at information security," says Barronton. "At one time we would put controls in our data centers and that would protect all our employees; very little was exposed to the internet and it was much easier to define an organization's perimeter. If you don't have a cloud-based solution you're not in the running. Now there is no perimeter and the Symantec Integrated Cyber Defense Platform brings integration, visibility, endpoint automation, and the reassurance of the leading market option to the cloud."

"Symantec is currently helping us create our Data Loss Prevention business rules and policies, which is also helping us with our CloudSoc Cloud Security Access Broker deployment," says Barronton. "Upon initial rollout we gained visibility into how cloud-based workloads were being utilized. As an evolving technology it will continue to grow and provide further benefits."

Sector-Specific Challenge: Finance is a Highly Regulated Industry

The finance sector is a sea of regulations. Customers need significant assurance that the software they implement adheres to each and every standard. "We have a very demanding customer base in terms of adhering to regulations, and quite rightly," says Barronton. "Certainly, to stay competitive and help us win business we need the very best in cyber security. Being able to state we have Symantec is a terrific selling point that builds trust and reassurance."

“We don’t have to be the ones to experience it in order to stop it. Symantec is already seeing it and pushing that information into the products so we’re protected. That’s a great benefit to us.”

– Scott Barronton,
Chief information security officer (CISO), Finastra

Championing a Cyber Security Culture

Alongside the technology, Barronton champions a new approach to security within the company culture. “I would argue that all organizations need to create a culture where everybody feels as passionate about information security as we do in my department,” says Barronton. “Everyone has to participate, take responsibility and make it a priority.” Barronton’s group champions showing how security adds value to the businesses. “Rather than being the office of ‘No,’ I’m keen to take a balanced view between business needs and security standards.”

Symantec as the Force Multiplier

“Knowing that Symantec sees attacks all over the world, I know we don’t have to be the ones to experience it in order to stop it,” says Barronton. “Symantec is already seeing it and pushing that information into the products so we’re protected. That’s a great benefit to us.”

The Finastra security team is constantly trying to improve its controls, making sure that monitoring covers all the activities. “It’s the things that I don’t know that keep me up at night,” says Barronton. “Now, I know so much more because of the visibility I’m gaining through Symantec’s integrated approach in our environment. Our partnership with Symantec brings capabilities we didn’t have, protections we didn’t have. Symantec has truly been a force multiplier for us.”

For Additional Information

Contact your local Symantec Sales Representative or Business Partner, or visit: broadcom.com

Symantec™
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com

SED-FinTech-CS100 June 8, 2020