Cisco Firepower
Strengthens Organisational
Cybersecurity Defences

Data#3 | CISCO Partner

Data#3 | **CISCO Partner**

Objective

As a large organisation that places a high priority on IT security to protect its business, it was clear that a replacement of aging firewalls to a more modern Cisco solution was needed to ensure business continuity.

Benefits

- Increased security
- A staged transition to the new Cisco Firepower technology
- Skills transfer for the inhouse IT team to self-manage their IT security
- Reduced risk
- Ample capacity to support a highly flexible and remote workforce

Project Highlight

The most important outcome for the organisation was enabling a large component of the workforce to work remotely, something that the aging ASA firewalls could not have handled before the project.

Approach

To ensure a smooth transition, the organisation enlisted the help of an experienced IT partner. The organisation had prior experience using Data#3's Project Services team for other Cisco projects so the organisation turned to their trusted partner for guidance and assistance to deploy the new technology.

Solutions & Services

- ☑ Cisco Firepower
- ☑ Project Services
- ☑ Security

Testimonial

"It is important for any organisation, and its stakeholders to know what they need and what they are hoping to achieve. Do your research, and don't be afraid to seek guidance. An experienced partner will provide valuable insight to help you on your technology journey."

Nicole Grice, Account Executive, Data#3.

"Cisco provided guidance on the designs before we positioned them with the customer. This gave the customer the confidence that they needed to proceed."

Nicole Grice, Account Executive, Data#3.

The Background

The existing Cisco Adaptive Security Appliance ("ASA") firewalls had worked well, however as the workforce became more flexible and technologies evolved, it was time to replace them with the more modern Cisco Firepower solution. A complex change, the endeavour needed to be completed without disruption to the business. Additional, outsourced expertise was essential.

The Challenge

The quality and dependability of the existing Cisco ASA firewalls had played a core role in IT security for several years, but as needs changed and technology advanced, stakeholders within the organisation knew it was time for an upgrade.

The growing need for working flexibly meant there was a greater load on the ASAs. The organisation's previous experience with Cisco technology made it an obvious choice to move to Cisco Firepower.

"It is important for any organisation, and its stakeholders to know what they need and what they are hoping to achieve. Do your research, and don't be afraid to seek guidance. An experienced partner will provide valuable insight to help you on your technology journey," said Data#3 Account Executive, Nicole Grice.

The organisation acquired the new firewalls, which offered twice the traffic capacity than the existing technology, with the intention of performing the transition in-house, however during planning it became clear that this would be no simple matter. Although the in-house team had experience managing the existing ASA firewalls, the magnitude of technology developments in Cisco's new offering highlighted concerns around potential disruption to business operations, and external help was needed.

"The customer had experience from an administrative view, but not from a transition perspective. ASA and Firepower are two very different beasts in terms of architecture and configuration, so they needed to minimise the risk," stated Grice.

However, when the initial attempt fell short of expectations set by the previous IT partner when an unplanned outage that impacted users, the in-house team elected to source a better suited partner to address what had become a pressing issue. As availability limitations meant using Cisco's own engineers would cause delays, the organisation chose to source an accredited Cisco partner with the necessary capabilities. Their first experience had made them more cautious.

"When you have a bad experience that can make you tread extra carefully. To help restore their confidence, we worked very closely with Cisco. Cisco provided guidance on the designs before we positioned them with the customer. This gave the customer the confidence that they needed to proceed," explained Grice.

Data#3 Customer Story

Cisco Firepower

"We were able to minimise the impact to the organisation through our plan to stagger the implementation instead of taking a 'big bang' approach."

Nicole Grice, Account Executive, Data#3.

IT Outcome

After examining the environment and reviewing user needs, Data#3's Cisco specialists determined that it would make most sense to proceed in carefully managed stages. During the planning stage they identified that migrating the VPN service in advance of other traffic would reduce risk and ensure that the transition proceeded more smoothly.

"As with any changes to plan, we helped the customer adjust their strategy slightly. It increased complexity for the Data#3 team, however our position with Cisco as a partner made it easy to accommodate the changes," said Grice.

The initial VPN element was prioritised, with cutover and support made possible within standard working hours. The new Cisco Firepower firewalls were installed in separate data centres, connected by a L2 link. Undertaking the first phase in January 2020 proved to be a sound choice that addressed the increasingly urgent challenge of enabling a remote workforce.

"For the customer, timing was imperative. If they had not sought out a fresh perspective, it could have been another six months of not knowing what was around the corner, and the impact on business if it went awry could have been disastrous," commented Grice.

What lay around the corner was a year that nobody could have imagined. With reduced pressure on the overloaded ASA firewalls and increased capacity, it meant that when lockdowns occurred, it was possible for the business to quickly switch to a work from home model. The timing proved critical to maintaining business continuity.

"We were able to minimise the impact to the organisation through our plan to stagger the implementation instead of taking a 'big bang' approach. Although COVID-19 increased the number of remote workers, it would have caused more load on the ASAs to the point where the straw was going to break the camel's back if the customer hadn't sought help when they did."

Facing a changing situation as lockdowns and restrictions shifted, the in-house team adjusted the process to fit its needs, and Data#3 supported this approach. Data#3 is one of the largest and most experienced Australian partners for Cisco, who have a high availability of specialist resources. Data#3 was ideally positioned to allow flexibility to match their needs. This capability proved beneficial, and ensured the in-house team was able to transition additional workloads.

"To provide assurance to the organisation, we left both firewalls in place for four to six weeks before implementing the VPN piece. This gave the organisation the opportunity to experience and gain familiarity with the new firewalls. Once the organisation was comfortable, our Data#3 team mentored their techs, so they had a strong knowledge from a live operating point of view," said Grice.

"Not only did the organisation benefit from maintaining business continuity, they could also see the statistics and connections which allowed them to troubleshoot issues that could arise."

"We're proud of the impact the joint effort between Data#3 and Cisco was able to make for our customer."

Nicole Grice, Account Executive, Data#3.

Business Outcome

As cyberthreats proliferated amidst the backdrop of a global pandemic, bolstering security with Cisco cutting-edge technology meant the business could better protect its environment. In particular, the Cisco Firepower firewalls are designed for today's flexible, hybrid workforce. As it turned out, the firewalls acted as a vital enabler for the workforce as they dealt with the ongoing challenges of 2020.

While the choice of investing in modern Firepower firewalls was relatively straightforward, the right planning and implementation support is essential.

"Without direct experience, they are more complicated. Like a lot of organisations, they upgraded without fully recognising that they were dealing with a very different architecture and platform. They knew they couldn't just move their existing configuration on to the new firewalls and expect it to know what to do," explained Grice.

After the downtime caused by the initial attempt with the previous IT partner, it was important for the IT team to rebuild trust with the business. Knowing that Data#3's Cisco-certified engineers had a wealth of experience handling similar transitions, and access to a highly skilled professional services team, helped to build confidence that the firewall upgrades could happen without disruption.

"From the very beginning, Data#3 conducted workshops with the business. Our teams would collaborate with the customer before going to work on the plan and would then re-present it to the organisation. When COVID-19 hit, our teams were able to maintain this collaboration despite working remotely."

More than ever, the service that the organisation provides to its customers was vital in keeping businesses operational throughout unprecedented challenges. A benefit of the project was that staff within the organisation were dedicated to ensuring business continued, no matter what.

To ensure that the business, already impacted by COVID-19 restrictions, was able to continue uninterrupted, some key parts of the firewall upgrade process were conducted overnight.

Ultimately, the most important outcome for the organisation was enabling a large component of the workforce to work remotely, something that the aging ASA firewalls could not have handled before the project.

Conclusion

With the benefit of hindsight, the in-house team learned much from the experience of upgrading its firewalls to the superior Cisco Firepower technology. After a disappointing experience with an initial partner, utilising a qualified partner in the project was critical.

"There is a real difference between knowing the technology from an administrative sense and performing a complex upgrade process. It is vital that your business knows that they are working with technology partners who not only have the capabilities, but also understands your business and where it wants to be now and into the future," commented Grice.

For Doug Browne, Director of APJC Cybersecurity SecOps at Cisco, this project was a clear example of what can be achieved when you leverage a partnership like Data#3 and Cisco.

"Technology is only one piece of the equation - careful planning and a partner with the skills required to implement and architect the solution are key. The Data#3 and Cisco teams worked alongside one another during the implementation and design phases, and only highlights how important it is to find the right technology partner to address your key security challenges," said Browne.

"We're proud of the impact the joint effort between Data#3 and Cisco was able to make for our customer, and we are thrilled to not only be their partner, but also part of their technology journey," concluded Grice.