


Data#3 Customer Story

BTC Markets

BTC Markets Enables Growth and Boosts Security with Cisco Solution from Data#3

Data#3

 btc markets

Data#3



Objective

As BTC Markets grew, the business wanted a network solution that could scale to match, while addressing important security requirements.

Project Highlight

BTC Markets have the knowledge and reassurance that the implementation of the technology has enhanced the security, reliability and scalability of their network.

Benefits

- High-speed connectivity
- Rigorously enforced security applied to all users, wherever they may be
- Secure and reliable connectivity between office and Microsoft Azure
- Increased visibility of user traffic
- Internet access for guests via segregated Wi-Fi and approval workflow
- Users have a consistent experience across multiple devices
- Reduced risk of security incidents
- Users can work safely from home and on-campus
- The technology is ready to support continued business growth

Approach

BTC Markets had a trusted relationship with Data#3. When BTC Markets moved to larger premises, and their existing network technology no longer suited their needs, they engaged Data#3 to design an enterprise-level architecture that would accommodate future growth and secure network connectivity. It was then logical to use Data#3 to implement the solution.

Testimonial

“We are quite a flexible workplace in terms of the location of our people, so if people want to work from interstate, or from home, they need to connect to the network, and to have product suites like Microsoft 365 in the cloud. Wherever they work, we want to make sure they get the best experience.”

Andreas Kafka, Cybersecurity Expert,
BTC Markets.

Solutions & Services

- ✓ Cisco Umbrella
- ✓ Cisco Identity Services Engine
- ✓ Cisco AnyConnect
- ✓ Cisco Meraki MX84 Security Appliance
- ✓ Cisco Meraki vMX
- ✓ Cisco Meraki Advanced Switches

BTC Markets

“The new solution also included VPN access, and that has been rolled out, so now it is easily possible for remote workers to use their devices to access the resources they need via secure remote connections.”

**Andreas Kafka, Cybersecurity Expert,
BTC Markets.**

The Background

Founded in 2013, BTC Markets has grown to become Australia’s largest cryptocurrency exchange. More than 325,000 users have traded over \$20 billion on the BTC Markets platform.

After BTC Markets expanded into new premises, the skilled in-house IT team determined that the ageing network technology no longer met the organisation’s needs. A shift to remote working when the COVID-19 pandemic struck placed additional pressure on the environment, and meant it was necessary to adjust the business’s security stance.

The Challenge

After strong growth, BTC Markets moved into a larger premise, and the move prompted a fresh look at how well its enterprise technology environment could scale to serve an increasing number of users. At this point, BTC Markets Cybersecurity Expert, Andreas Kafka, identified issues that could affect user experience and hamper future growth.

“Last year, we decided to move into a new office location, based on the company’s growth, so that we would have more capacity for staff members. In our old office environment, we had identified a number of performance issues around the network. Also, the network equipment we had been using was not ready to scale with the business,” explained Kafka.

“We were operating with limited Wi-Fi coverage in the office, and there was no redundant internet connection. Being an internet-based company operating fully in the cloud, internet connectivity is business-critical.”

Security was among the issues that most concerned Kafka. The legacy system offered very limited visibility of the corporate environment and did not allow for insight into users, representing a missed opportunity to understand and improve user experience. For an internet-based company, user experience is a key component for attracting and retaining the very best staff.

“We had a number of security controls in place, which we wanted to improve. Therefore we knew we had to upgrade our network equipment,” said Kafka.

“We are under constant attack and need to protect our front-end, cloud native based AWS and Microsoft Azure, but also protect the back-end office operations, and that’s where Data#3 and our network project comes in.”

The challenges were heightened when the COVID-19 pandemic struck, and health restrictions caused the workforce to rapidly transition to a remote working environment. As a cloud-based business, remote working was less of a culture shock than for many organisations more reliant on on-premises infrastructure, but the change emphasised the importance of a strong, secure environment that supports flexible work options, while securing both network and users.

“We had a number of requirements, including remote access via VPN. We didn’t have a true enterprise solution, our content and web filtering were limited, we didn’t have network segmentation, reliability was shaky, and we couldn’t apply policies to network rules in the way we wanted,” outlined Kafka.

“We had to support a remote workforce, and COVID-19 restricted us from leveraging our office space. We still believe in face-to-face teamwork and teambuilding, though, and our preference is to have people in the office. We are quite a flexible workplace in terms of the location of our people, so if people want to work from interstate, or from home, they need to connect to the network, and to product suites like Microsoft 365 in the cloud. Wherever they work, we want to make sure they get the best experience.”

BTC Markets

“Wherever our staff work, we want to make sure they get the best experience.”

**Andreas Kafka, Cybersecurity Expert,
BTC Markets.**

IT Outcome

Initially, BTC Markets sought consulting help from Data#3 to design a network that would offer greater insights, stronger security, and improved management. A series of discovery workshops helped to identify the exact requirements and align technology options with business direction. This early phase began before Kafka joined the business, and he inherited an engagement already underway, but he was happy to continue the trusted relationship that had been built between BTC Markets and Data#3.

“There was an original initiative where we had a Data#3 engineer come in and define a logical and physical architecture for the new network. We were happy with the proposal, and it was the logical next step to engage Data#3 for the implementation phase.”

With the high-level design and bill of materials approved, a detailed design was created by the Data#3 engineer, supported by the relevant technology partners. This outlined the configuration that would be needed. Unsurprisingly for an internet-based business, cloud management platforms are at the heart of the solution, with Cisco Meraki dashboard for switches, wireless, firewalls, 4G internet backup, and software defined WAN (SD-WAN). Cisco Umbrella was chosen to provide a secure web gateway for both on-premises and remote users. Cisco Identity Services were included to deliver a dynamic and automated approach to policy enforcement, simplifying delivery of a highly secure network. AnyConnect client software was deployed to give clients always-on web security, so they could work securely from any device, in any location.

The outcome is a secure, policy-based network that is user and application defined. As one of only a handful of Cisco Gold Partners in Australia, Data#3 was recognised as a Leader in Customer Experience and Enterprise Networking in 2020, and this focus was evident in the consideration of the user's needs as they adapt to new working conditions.

“The majority of the implementation work was done by Data#3, including all configuration and set-up of equipment. We had myself and another person from BTC Markets to help with the physical installation of equipment, and configuration of a few things on our side, as well as some solution components. It was an 80-20 workload share,” recounted Kafka.

With COVID-19 restrictions still affecting users, and many embracing the flexibility of hybrid work, Kafka said that network traffic has not entirely returned to previous patterns. He anticipates that adjustments may be made as more workers return.

“Since we implemented the new network, we have had few people in the office, mostly tech support staff, so we haven't had a full load on the equipment yet. The solution also included VPN access, and that has been rolled out, so now it is easily possible for remote workers to use their devices to access the resources they need via secure remote connections.”

Kafka's team has adapted well to the new technology, with the support of Data#3. He described the introduction of enterprise-level networking technology as involving a “learning curve”, making it essential to work with a partner that is equipped to offer guidance through this vital phase. He cited one security feature that decrypts and inspects internet traffic for malicious events, impacting functionality on a small number of websites. This was overcome with custom configuration, making specific exceptions for the trusted sites involved.

“When it came to such hiccups, we were able to turn to the Data#3 engineer to help us resolve them,” commented Kafka.

BTC Markets

“Now, we can just log in to a dashboard, see what’s happening, who is connecting with what app, and network events are all visible to us.”

**Andreas Kafka, Cybersecurity Expert,
BTC Markets.**

Business Outcome

BTC Markets can now be assured that it has put enhanced, enterprise-level security in place to protect its people and assets. When a user logs on to a BTC Markets machine as an authorised user, the network adapts to the device, providing effective and secure policies that meet requirements set by the business. While industry standards are not onerous for Bitcoin trading businesses, BTC Markets opted to meet the ISO 27001 international standard, assuring staff, customers, and partners that, among other things, the business meets a higher standard of information security.

“The certification covers network security requirements, and the kit brought in definitely helped us to also comply with our own security controls and requirements. BTC Markets chose to comply with ISO certification, even though it is not mandated, to demonstrate to customers and technology partners that we are doing the right thing. It creates trust in the industry and clients that we have a highly trustworthy exchange of cryptocurrency in place, setting us aside from our competitors,” explained Kafka.

The new network offers higher reliability, and ensures business continuity while greatly reducing the risk of downtime. Importantly, Kafka said that clear documentation has been established, so that the IT team can make any changes needed with far less stress.

“Visibility is absolutely better. When we moved office last year, we didn’t know what had been done. The network equipment we had in the office was inaccessible, we couldn’t log into the console unless we plugged a laptop into the management port directly. Now, we can just log in to a dashboard, see what’s happening, who is connecting with what app, and network events are all visible to us.”

Kafka, though, was quick to point out that security is about more than just technology. He advocates communicating well about any changes, so that users understand and support the underlying aim to make the business and its customers secure.

“All our staff undertake cybersecurity training, so that they are all aware how important it is and what is at stake if we were hacked. If we are clear about what security controls we need to implement, it is easier to get buy-in when we need new network equipment.”

Conclusion

Rather than seeing the implementation of the new network as an end of the project, Kafka said it should be viewed as an ongoing process.

“When my predecessor planned the solution, it was said that this is a great solution that just runs in the background. While that is partly true, in that it does not require constant monitoring or maintenance, if we want full value we should not ‘set and forget’. We need to log in and respond to incidents, to look for recurring traffic patterns, and investigate them for signs of malicious activity,” described Kafka.

While this may have been initially *“underestimated,”* Kafka said it brought home the importance of working with a trusted, knowledgeable partner that doesn’t walk away at the end of implementation.

“Some of the learning is by doing, the engineer doesn’t just hand over on the last day and expects us to be experts. His expertise was excellent, and he was happy afterwards to answer all our questions and find the right support to help us out. We appreciate this aspect of our relationship with Data#3, we never feel like the door is closed. Data#3 is definitely on the priority list to do work for us in the future because we know we can rely on them, they have people with right skills and the right attitude.”

BTC Markets

Data#3 and Cisco

As a Cisco Gold and Master Specialised Partner, Data#3's relationship with Cisco has grown progressively over more than 20 years. During this time, Data#3 has become one of Cisco's largest partners in Asia Pacific with significant capacity throughout Australia and the capability to deliver business outcomes using Cisco's technology.

Through a committed partnership, our technical team has developed deep expertise across Cisco's portfolio, giving Data#3 an edge when it comes to navigating the complexity of the digital era and solving your business challenges with the best technology solutions.

Data#3

