CommSec

CUSTOMER SUCCESS STORY: **MANAGED SERVICE PROVIDER**

The Challenge

CommSec was founded in 2013 with a mission to bring enterprise-level security to all organizations, regardless of size. From day one,security has been the company's focus. While many managed service providers typically offer IT services, CommSec saw the need for a firm that concentrated solely on security.

Recently, CommSec experienced large growth (over 50% in 2021) as more customers seek out guidance on how to develop and implement a security strategy. With the rise in ransomware and high-profile cyberattacks, customers are in need of a trusted advisor. One cyber-attack that got international attention was at the Irish HSE, the country's public healthcare system. Darragh Reynolds, CommSec's marketing manager, explained the impact of this moment:"The HSE attack was an eye-opening experience for anyone who protects sensitive information or data. This led to a huge increase in business."

For customers working with CommSec, a key concern is knowing where to begin. CommSec offers a wide range of services including threat hunting, digital forensics, vulnerability management, anti-virus, endpoint protection, email protection, and more.

Typically, the customer journey begins with a security audit in order to find potential gaps or vulnerabilities. That's where Duo comes in. Ian O'Connell, who leads the security operations center at CommSec, emphasized the importance of a zero trust solution.

"Duo was the first vendor that put the zero trust model into practice with multi-factor authentication. It not only looks after MFA, it sees who the user is, what device they're using, whether it's a trusted device. Duo ties it all together in one product, especially for MSPs, and it makes it easy to manage customers of different sizes," O'Connell says.

"

The support given by Duo is above par. They're quick to get back, very helpful, and detail-oriented."

Ian O'Connell

Security Operations Center Team Lead, CommSec

The Solution

The Duo & MSP Partnership

CommSec began working with Duo in 2017. From an MSP perspective, the benefits range from ease of billing to quick setup time. According to O'Connell, it only took a few weeks to get Duo deployed and the staff trained. "Adoption is quick, it's pretty much plug-and-play. It provides flexibility for legacy systems that may not be easy to adapt. The API also allows for easy integration, it's fairly simple and intuitive, and Duo does a lot of the heavy lifting with the setup process," he says.

Additionally, CommSec has benefitted from the resources and guidance from partnering with Duo. "The support given by Duo is above par. They're quick to get back, very helpful and detail-oriented," O'Connell adds. CommSec has been able to use Duo's knowledge base to empower its customers to implement and take advantage of Duo. "From a support side, it's easier for a help desk or MSP to manage the queries that come in. You don't want to have to run around and look at a lot of different places, and with Duo you can find everything in one place," O'Connell says

Enable All Organizations on a Zero Trust Journey

After a client takes the security assessment, CommSec helps prioritize next steps based on the uncovered vulnerabilities. If a customer does not have multi-factor authentication in place, that's an important place to start. Next, CommSec demonstrates Duo's capabilities in order to show how it can integrate into the clients' system. "Duo is device agnostic and there are a lot of users with Macs now. It's good to have an MFA provider that aligns with everyone and integrates with everything. That's really important," Reynolds explains.

In addition to MFA, Duo's other features enable clients to begin their zero trust journey. "As we see migration to the cloud, it can be hectic for an organization to apply a holistic approach to zero trust. But with the Duo platform it helps them overcome that challenge," O'Connell says. "For example, bring your own device can make sure the endpoint is in line with the company policy. With Duo, you can check that the version of Android, iOS, or Windows is up to date, which is a great advantage of the platform."

Users Come First

Duo's usability is an important factor for both the security teams administering the product and the employees that use the product. O'Connell works closely with clients to deploy Duo. "With other authentication apps, there is a lot that needs to be configured," he says. "You need to set up identity, decide on different groups, but with Duo, the groups that you manage can be transferred into different systems. It can all be done from Duo."

Usability is also a significant driver when it comes to end users. Clients want a product that will improve their security position but will not take away from their workers' productivity or time. "Ease of use for the user is important. We use Duo ourselves and with token generators you can have two, three, or four of these on your device and it gets really confusing. With Duo, it's a big timesaver and if you add that up over a year, that's a lot of time saved," says Reynolds.

Business Results

Ultimately, Duo's success in 2022 is demonstrated by CommSec's client retention rate: 100%. While CommSec works with businesses of all types and sizes, Duo is able to adapt to that organization's needs and fit within diverse systems. While deployment can vary based on customer size and complexity, it typically takes a client a few hours to get the Duo portal up and running, with the majority of features and integrations working as well. Once Duo has been deployed, customers can feel at ease knowing their security posture has improved.

"If there has been a breach and passwords have been compromised, we recommend Duo," O'Connell says. "Security is like an onion, there needs to be an extra layer put in. That's where Duo comes in." While it is hard to quantify the number of attacks that do not happen because of strong security, it helps knowing that Duo is another line of defense keeping customers' systems and data safe. Reynolds said for most customers, "If they had Duo, they wouldn't have had the breach. Duo is the silent hero. It does its job and we don't hear about it."