Canterbury District Health Board
Te Poari Hauora ō Waitaha

gemalto
security to be free

CASE STUDY

Canterbury District Health

Gemalto Prescribes SafeNet Authentication Service to Secure Remote Access at Canterbury District Health Board

Physicians and other staff members at the Canterbury Health District Board wanted to access email and other services remotely. By leveraging SafeNet Authentication Service, the security team established strong defenses against phishing and other security threats, while improving end user convenience.

The Organization

The Canterbury District Health Board (CDHB) is the main planner and funder of health services in the Canterbury region of New Zealand. One of the country's largest health boards, the organization is responsible for serving more than 500,000 people, representing about 12 percent of the country's population. The CDHB is also the largest employer in the country's South Island.

"The reality is that without SafeNet Authentication Service, we would have had to shut off Outlook Web Access, which would have meant that users couldn't access email remotely. With the solution, we could address critical risks while enabling secure remote access. We now have more than 5,000 users enrolled in the solution, and people love it."

Mohammed Sayeed, Service Operations Manager at Canterbury District Health Board

Challenge

In the wake of damaging phishing attacks, the CDHB security team knew it needed to establish a broader framework for multi-factor authentication.

Solution

With SafeNet Authentication Service, the CDHB has been able to enforce two-factor authentication requirements for all remote users, including both administrative and medical staff.

Benefit

By leveraging SafeNet Authentication Service, the CDHB has established an efficient, cost-effective way to more consistently enforce access control policies and combat phishing attacks.

The Business Need

In the wake of devastating earthquakes that had hit the Canterbury region in 2011, the CDHB needed to quickly equip its employees with the ability to access email remotely so they could continue their vital work despite not being able get to their offices. In order to expedite delivering this access, the organization provided remote employees with direct access to their Citrix NetScaler platform, simply requiring users to submit their user names and passwords. While this was a necessary compromise to make during the aftermath of this natural disaster, it was not aligned with the security team's best practices.

Like many other healthcare organizations, CDHB's staff members were being targeted by phishing attacks. Unfortunately, some of these attacks were successful, and over the span of two years, the CDHB's email communications were blacklisted three times due to these breaches – severely impacting their staff's ability to communicate with anyone outside the organization, including patients, insurance and fellow healthcare providers. It also took a huge effort on the part of CDHB's IT staff to get the organization removed from security systems' blacklists. In the wake of these incidents, revisiting the security of their hastily-implemented Citrix environment became their number one priority.

The Solution

A longtime Gemalto customer, the security team at CDHB sought to upgrade and expand their use of two-factor authentication to include their Citrix applications. Local Gemalto distributor, MPA, recommended Gemalto SafeNet Authentication Service, which offered a variety of features that uniquely addressed CDHB's requirements.

"After MPA told us about the SafeNet Authentication Service solution, we found the value proposition was hard to refuse," said Mohammed Sayeed, Service Operations Manager at CDHB. "It seemed clear the solution would provide the security we needed, while minimizing our ongoing administration and costs."

As a pilot program, the CDHB deployed virtual desktop infrastructure (VDI) with VMware View. The organization initially implemented SafeNet Authentication Service for accessing their VDI environment, and this phase worked extremely well for users and administrators. They subsequently expanded the solution to enable users to connect to the organization's Outlook Web Access online email portal.

In time, the security team established a mandate for all users outside of the CDHB domain, requiring that they use two-factor authentication, either via a hard token or Gemalto's MobilePASS family of one-time password (OTP) software authentication solutions. MobilePASS combines the security of proven two-factor strong authentication with the convenience, simplicity, and ease of use of OTPs generated on personal mobile devices or PCs.

Given the success of the implementation, the boards of other regional health districts have started using the instance of SafeNet Authentication Service hosted at CDHB facilities. Through the solution's support for multi-tenant environments, SafeNet Authentication Service makes it efficient for these other healthcare boards to get set up and start using the solution. CDHB staff members simply need to provide other boards' administrators with access to the console and they can efficiently configure and implement the solution for their own organization.

"When we tell our colleagues around the country about SafeNet Authentication Service, they invariably want to buy it," said Sayeed. "Both within our organization and within our partner organizations, we expect the use of the solution will only grow."

The Benefits

By leveraging Gemalto solutions, CDHB has been able to capitalize on a number of significant advantages:

- **Enhanced security.** By more efficiently and consistently leveraging multi-factor authentication, the security team has been able to establish strong defenses against the phishing attacks that had been plaguing the organization.
- **Cost effectiveness.** SafeNet Authentication Service offered the competitive, cost-effective pricing model that helped CDHB realize maximum value from its authentication investments.
- **Streamlined administration.** SafeNet Authentication Service offers fully automated workflows that support the entire administrative lifecycle, including the provisioning and revocation of users and tokens. In addition, the solution offers automated red flag alerts that allow management by exception.
- **Convenience.** With Gemalto's solutions, CDHB can maximize security while also maximizing end-user convenience and flexibility. With MobilePASS, doctors and other staff members can use their existing devices—whether smartphones or tablets—for OTP authentication. Even when doctors are traveling overseas, they can use MobilePASS to gain access to corporate resources.
- **Flexibility to scale and evolve.** CDHB opted for the on-premises installation of SafeNet Authentication Service Private Cloud Edition, rather than cloud-based as-a-service delivery. Thanks to the solution's multi-tier, multi-tenant architecture, CDHB's platform can accommodate a virtually unlimited number of additional health boards, or tenants, while concurrently accommodating as many user groups and business units as required. With the solution's broad integration ecosystem, CDHB maintains the ability to grow and evolve its use of multi-factor authentication.

About MPA

MPA is a New Zealand-owned IT Security distribution specialist. For more than 25 years the company has delivered technology solutions via its channel partners to a wide range of New Zealand businesses, integrating world class solutions sourced from international vendor partners.MPA has been in partnership with Gemalto SafeNet for 10 years.

About Gemalto Enterprise Security

Gemalto offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of digital identities, transactions, payments, and data – from the edge to the core. Gemalto's portfolio of SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

Contact Us: For all office locations and contact information, please visit safenet.gemalto.com

Follow Us: blog.gemalto.com/security

GEMALTO.COM

gemalto
security to be free