CASE STUDY

NORTHERN CALIFORNIA BANK TURNS TO WEBSENSE® FOR DATA LOSS PROTECTION

THE PROBLEM

This multi-billion dollar bank, with branches throughout northern and central California, needed a vendor that could help protect corporate assets and customer information against internal threats in a unique technology environment. At the recommendation of an external audit, the bank sought a unified solution with embedded data loss prevention (DLP) within the web and email gateways to protect against risky employee behavior.

LOCATION: Northern California, United States

INDUSTRY: Financial

PRODUCTS USED: Websense® TRITON® Enterprise

> **"I needed a vendor that was open to working with our current infrastructure, had credibility in the IT security space and exhibited ongoing innovation. Websense was the perfect match."**
>
> - Mark Jackson, Information Security Officer

THE SOLUTION

The bank selected Websense® TRITON™ Enterprise to provide comprehensive data loss prevention on both the network and the endpoint.

"During the evaluation process, I looked at three vendors," said Mark Jackson, Information Security Officer for the bank. "I needed a vendor that was open to working with our current infrastructure, had credibility in the IT security space and exhibited ongoing innovation. Websense was the perfect match. They were the only security company that surpassed our security requirements while also catering to our unique needs. Their team jumped through several hoops and delivered a solution that went far beyond our expectations."

THE RESULTS

TRITON Enterprise provides email security, web security and DLP within a unified architecture. It significantly helps the bank mitigate employee risk. On the production side of the banking infrastructure, which accesses customer information, Jackson uses DLP to control access and monitor the printing of sensitive documents to prevent confidential information from leaving the premises. Websense technology provides source and destination awareness, which enables Jackson to understand who is accessing what kind of data, how it is being used and where it is being transferred.

With Websense, Jackson can also make informed policy decisions in real time and create effective policies for the future. For example, he has set policies to prevent employees from leaving with company information on USB drives. Jackson can encrypt any data transferred and stored on USB drives and only allow access to the information from another Websense protected computer. He also uses

websense®

NORTHERN CALIFORNIA BANK TURNS TO WEBSENSE® FOR DATA LOSS PROTECTION

DLP to periodically check the network for client information and receive alerts based on the findings.

"I'm constantly learning new and effective ways to use Websense's TRITON Enterprise solution," said Jackson. "I would love to hire an additional employee just to explore the further capabilities of TRITON. There are just so many ways to use this technology to enhance the security of our company."

BRAVE THE NEW WORLD.

Learn more: **www.websense.com**