Forcepoint

Customer Story

National Bank of Fujairah Sets the Gold Standard for Data Protection

National Bank of Fujairah secured buy-in at all levels of the business to systematically mature its data security culture and successfully deploy data-level controls.

Implementing a comprehensive data protection framework enabled the National Bank of Fujairah to systematically acquire buy-in at every level of the organization, clearing the path for a successful Data Loss Prevention (DLP) deployment. The bank reviewed its data security strategy in order to prevent confidential data from leaving the firm and to comply with different regulations. Now, the bank is one of the select few in the region that leverages DLP blocking to its fullest extent, with sophisticated fingerprinting technology ensuring all sensitive data remains under protection.

CUSTOMER PROFILE:
Established in 1982, with headquarters based in both Dubai and Fujairah. The National Bank of Fujairah is a commercial institution offering corporate services, treasury, trade financing, and personal banking. With 16 locations of operation across its three subsidiaries.

INDUSTRY:
Banking

HQ COUNTRY:
United Arab Emirates

PRODUCTS:

› Data Loss Prevention (DLP)

Securing Digital Transformation

The National Bank of Fujairah's (NBF) clients and institutional customers have implicit confidence that they will receive the best service and funding available.

When it came to the sensitive data it collects from its users, NBF believed its data deserved just as much attention as the other areas of its operation. It's why in 2014, NBF started its journey as an early adopter of innovative data security controls.

"Our customers and leadership team were beginning to focus on confidential data and where it was going," Hariprasad Chede, Chief Information Security Officer at NBF, said. "With new channels for banking coming online at the time, like mobile, we knew we needed better security controls, or we wouldn't be able to move forward very far."

Chede understood that the bank needed a way for its workforce to handle data more securely without interfering with the daily routine. An initial conversation with its partner, Paramount, led NBF to explore Forcepoint's Data Loss Prevention (DLP) solution.

Follow the Data

When it comes to implementing new processes or platforms, Chede is a big proponent of the acronym T-A-R-T, which he learned from his CIO.

Tools and techniques

Authority

Relationships, both upward and downward within the organization

Training and culture

"If you want to implement data protection, then of course you need the right tool," Chede said. "But you also need the authority to make the decision, the relationships to get buy-in at all levels, and the consistent training to change the culture to ensure it all meshes together well enough."

True to his word, Chede first piloted the DLP with a six-month Proof of Concept. A longer PoC afforded the bank a larger data set that could help identify monthly and quarterly behavior changes. In turn, NBF gained valuable insight on how data regularly flowed throughout the organization.

"We found that we had fewer incidents than we initially thought we might," Chede said. "We also also realized peoples' general awareness of data security was low, but average considering it wasn't very popular at that time."

Chede was able to easily persuade upper management of the importance of a DLP due to the abundance of data at his disposal.

"I shifted the focus away from what I was trying to accomplish and toward the business – in other words, what would be the impact of critical data getting in the wrong hands?" Chede said.

With the executive team bought in to the value of DLP, NBF moved to implement it.

The extensive groundwork accomplished during the PoC made deployment simple. Initially starting with monitoring, NBF was able to quickly identify incidents and report them to the business. With each incident, DLP gained more momentum and trust from organizational leadership.

After the first five months of DLP running, Chede was able to convince the C-level and the various departments to switch on blocking mode. Though initially met with push back from department heads, the support from leadership and the roadmap set out for implementation convinced NBF to take the leap of faith.

Challenges

- Comply with the Central Bank of the United Arab Emirates and other data protection regulations.
- Detect and prevent the exfiltration of sensitive information from the organization.
- Win stakeholders buy-in at all levels of the organization.
- Change the workforce culture from an obstacle to an advantage when it comes to data security.

Approach

- Run an initial Proof of Concept for six months to determine whether, how, and when data security issues occurred in the firm.
- Activate monitoring mode after deploying DLP.
- Turn on DLP blocking and hold at least six training sessions each month for all impacted teams, including C-level.
- Implement fingerprinting to improve blocking quality.

Continuously Improving Data Security

Every security project is unique. In the case of NBF, its story of DLP adoption didn't end by activating DLP blocking – it was another beginning.

The bank struggled for almost a year with false-positive incidents, whether it was protecting the wrong data, using the wrong keywords for classification, or dealing with anomalies in user behavior.

By implementing fingerprinting, NBF was able to improve its blocking accuracy. Chede investigated critical data tables throughout the organization to determine which were too sensitive to leave the organization, and which were only creating noise and unnecessary investigation.

However, an effective data security strategy doesn't only focus on how successful it is at blocking information from leaving the organization. It also needs to account for how widely accepted it is, as it only takes one blocked email that disrupts business operations to potentially close the program.

"People were growing upset that we were stopping business as usual, even if we were stopping incidents from happening too," Chede said.

NBF conducted a minimum of six training sessions per month to help the workforce understand how to work in harmony with DLP and why it was important. The meetings were mandatory for anyone who had something blocked, including the CEO. Participation and general data security awareness improved drastically with senior leadership involved.

DLP blocking brought ancillary benefits too, including the automation and encryption of certain processes, to a reduction in printing in line with the bank's sustainability goals.

"The biggest benefit is the confidence I'm able to supply to our customers that their data is protected – they see with their own eyes that we can't share personal data via email," Chede said. "In turn, they become our biggest spokespeople for how secure our organization is."

Now, with blocking successfully integrated into the organizational culture and NBF firmly in compliance with all relevant regulations, the bank is looking toward improving data protection within the organization through a profound understanding of how user behavior drives risk.

Results

- Deploy and leverage the entire functionality of DLP - one of the only organizations in its region to do so.
- Complete top-down support for DLP blocking and its benefits.
- Reduction in false-positive incidents due to fingerprinting.
- Compliance with PCI-DSS, NESA, and UAE consumer protection regulations.
- Automated 70+ internal processes were automated, and unsafe routes of connection with consumers were eliminated.
- Reduced number of printed documents to meet the bank's sustainability goal.