Infoblox

CASE STUDY

Top Middle Eastern Bank Implements Essentials of a Comprehensive Cybersecurity Strategy

The Customer

This fast-growing financial institution based in the Middle East takes a proactive and comprehensive approach to its cybersecurity strategy, which it takes very seriously. The bank also successfully aligns its network and cybersecurity operations team with its corporate values of doing business with absolute integrity and honesty and remaining on the cutting edge of innovation.

The Challenges

The bank encounters many challenges within the cybersecurity industry across the organization. The two primary challenges that the bank experiences regularly center on operations and budgeting. The bank's network and security operations team has developed a deep understanding of the threat landscape and what it takes to plan and execute a comprehensive cybersecurity strategy.

Organizational Challenges

Like many financial institutions, the first challenge that this bank had to overcome was the organizational one of ensuring that all employees follow essential cybersecurity best practices and use technologies effectively.

To minimize operational challenges, the bank trains all employees on best practices, such as how to identify and avoid clicking links within phishing emails. Common worldwide, phishing attacks are becoming increasingly sophisticated, stealthy and difficult to combat. "That is why it is so important to proactively train our employees to minimize accidental insider threats," says the senior manager of the bank's network and security operations team.

Facts & Figures

Industry: Financial Services

Location: Middle East

Outcomes: Data security, improved network availability and visibility

Budgeting Challenges

Securing budgets is the second key challenge that many enterprise network and security teams experience. While an effective cybersecurity solution can be expensive, for the customer a reliable solution was a nonnegotiable requirement. Budget challenges often arise when the entire staff is not aware of the importance of prioritizing a robust cybersecurity solution or lacks an understanding of the threat landscape. According to the customer, "A pervasive lack of awareness can become a significant obstacle in efforts to convince team managers and decision makers about the importance of proactively protecting users and data before an attack occurs—and just how much can go wrong in the event of a data breach."

> *"Your data are your crown jewels. Treat them as such. Work internally with your teams to prioritize your company's comprehensive cybersecurity strategy and implement it company-wide. Ensure that your data is protected everywhere. Do not wait!"*
>
> Senior Manager, Network and Security Operations,
> **Top Middle Eastern Bank**

Elements of a Comprehensive Cybersecurity Strategy

The bank's network and security teams understand the requirements of a comprehensive and future-proof cybersecurity strategy that will evolve with the company and new technologies. As the customer says, "The best cybersecurity strategy should include a triad of solutions that ensure three things: data availability, security and visibility."

Data Availability

First, a comprehensive cybersecurity strategy must address data availability. This means making data readily available from anywhere at a required level of performance in situations ranging from "normal" to "disastrous." From a cybersecurity perspective, data availability includes service data and process availability as well. Organizations must have appropriate and automatic data backup technologies in place.

Data availability is essential to ensure business continuity and reliable operations. If harnessed effectively, data availability can greatly enhance business performance over time. Today's networks have rapidly growing numbers of applications and devices on them, all of which can easily access the network from anywhere at any time. Thus, maintaining data availability is crucial in enabling operations teams to more effectively analyze, control and secure their networks.

Data Security

Second, a comprehensive cybersecurity solution must ensure that all data within any organization remains secure and protected at all times. While this may seem an obvious part of any security strategy, in practice, it entails a number of capabilities that many enterprises often overlook. These include, but are not limited to, proactively implementing solutions for data exfiltration prevention, DNS security and encryption.

To stop malware and data exfiltration, the bank's network and security operations team experts urge organizations to focus on DNS security. More than 90 percent of malware attacks use DNS at various stages of the cyber kill chain to penetrate networks and steal data. Accordingly, organizations must protect their DNS. According to the customer, "The best way to thwart data exfiltration is to prevent data from being exposed to DNS tunneling technologies. It's also important to use a combination of reputation, signatures and behavioral analytics to identify anomalies in the data."

The value of protecting data at the DNS level, both on-prem and in the cloud, is to allow organizations to prevent the spread of malware by automatically detecting the precise location of the malware, and to isolate and block it before it can spread. This strategy also protects devices on-prem, while roaming and in remote offices/branch locations.

Conclusion: Making a Comprehensive Cybersecurity Strategy a Priority

After years of experience in the trenches of cybersecurity, the bank's network and security operations team has advice for other enterprises: "Your data are your crown jewels. Treat them as such. Work internally with your teams to prioritize your company's comprehensive cybersecurity strategy and implement it company-wide. Ensure that your data is protected everywhere. Do not wait!"

To get started, organizations must look inside their networks, not just outside, and be sure that their cybersecurity strategies include these three essential elements: data availability, data security and data visibility. They must not overlook even minor details. It only takes one cyberattack to potentially compromise an organization's entire network.

For More Information

Learn more about how you can implement a comprehensive cybersecurity strategy to scale for future technologies and growth. Visit the Infoblox website to address your DNS security with a hybrid solution or start your free trial today.

Infoblox is the leader in modern, cloud-first networking and security services. Through extensive integrations, its solutions empower organizations to realize the full advantages of cloud networking today, while maximizing their existing infrastructure investments. Infoblox has over 12,000 customers, including 70 percent of the Fortune 500.

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054

+1.408.986.4000 | info@infoblox.com | www.infoblox.com