infoblox

CASE STUDY

Askari Bank modernizes and enhances cyber security posture with Infoblox Threat Defense Advanced

OVERVIEW

Askari Bank opened for business in April 1992 and has grown to become one of Pakistan's leading financial institutions.

Askari offers a full range of personal and business banking services, ATM and mobile banking and credit and debit cards, and it maintains 537 branches across Pakistan. Since its inception, the bank has concentrated on growth through improving service quality, investing in technology and people and using its extensive branch network, which includes Islamic and agricultural banking. Askari's vision is to passionately support its customers' success and delight them with the quality of its service. A key element of this dedication to service is to maintain the absolute highest levels of privacy and security for the bank's customers.

> *"As we ran the PoC through various scenarios, there was not a single instance of a successful data infiltration or exfiltration event. Seeing Infoblox Threat Defense™ in action blocking malicious activity in our own environment gave us a lot of confidence in the Infoblox solution."*

Jawad Khalid Mirza
CISO at Askari Bank

THE CHALLENGE

Strengthening security posture to counteract emerging threats

As with all financial institutions globally, Pakistan's Askari Bank is a popular target for malicious cyber attacks. Maintaining a strong security posture has long been a top priority of the Askari IT team, and the bank has deployed multiple cyber security solutions over the years, including a security orchestration, automation and response (SOAR) solution and a Cisco DNS security product it relied on for years. In working with the consultants at Secure Networks, the Askari team came to understand that DNS-layer threats had evolved over time and that exploring other options in DNS technology could help to strengthen the bank's overall security.

askaribank LIMITED

"As we know, DNS is not designed with respect to security perspective," explained Jawad Khalid Mirza, the chief information security officer at Askari Bank. "The open architecture of DNS has led to it becoming a prime target for adversaries. In the financial sector, these threats most often manifest in attempts to exfiltrate/infiltrate data from enterprise."

"Legacy security solutions are designed to counteract threats by blocking DNS queries," explained Asad Effendi - CEO, Secure Networks, who helped carry out the PoC. "But with the malware attack scenarios we're seeing today, simply blocking suspicious traffic isn't always the best approach."

THE SOLUTION

Advanced DNS security with Infoblox Threat Defense™

With a test version of Infoblox Threat Defense installed in the Askari Bank data center, the team ran a series of networking traffic scenarios using the most recent data infiltration and exfiltration techniques characteristic of DNS Messenger and fast-flux attacks. "As we ran the PoC through various scenarios, there was not a single instance of a successful data infiltration or exfiltration event," said Khalid Mirza. "Seeing Threat Defense in action blocking malicious activity in our own environment gave us a lot of confidence in the Infoblox solution."

Threat Defense operates at the DNS level to see and uncover threats that other solutions do not, and it stops attacks earlier in the threat lifecycle. Through pervasive automation and ecosystem integration, it also drives efficiencies in SecOps to uplift the effectiveness of the existing security stack. These capabilities constituted a strong secondary consideration for the Askari team, which relies on its SOAR solution to manage its overall security operations. With the full scope of capabilities and benefits of Threat Defense now clear to the Askari team, the decision was made to move forward with a full production deployment.

THE RESULTS

Faster threat detection, reduced incident response times

"Threat Defense makes our entire security stack more effective," explained Umair Shakil, the head of Askari Bank's Security Operations Center Unit. "With the Infoblox solution integrated with our existing SOAR platform, all of the tools in our security stack now have access to real-time network and threat intelligence. Everything now works in unison to better identify and remediate threats through extensive automation."

The unique hybrid security design of Threat Defense uses the power of the cloud to detect a broad range of threats while tightly integrating with the on-premises ecosystem. It also provides resiliency and redundancy not available in cloud-only solutions. Through a common console, the Askari team can now centrally and automatically secure IoT and other devices, apps, virtual machines and switch ports wherever they reside. Threat Defense has enabled the Askari team to decrease the burden on strained perimeter security devices, such as firewalls, IPS and web proxies, because it converts powerful and already available DNS servers into the first line of defense. The team expects to get more value out of its security stack through sharing of threat and attacker information, as well as boost the productivity of its threat analysts and security administrators.

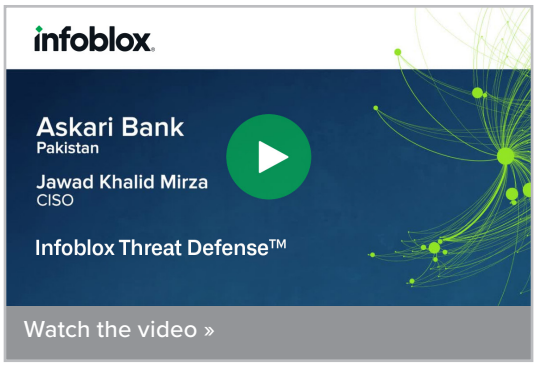
Customer: ***Askari Bank***
Industry: ***Financial Services***
Location: ***Pakistan***

INITIATIVES:

- Prevent data infiltration and exfiltration techniques with analytics and machine learning, including DNS-based data exfiltration, DGA, DNS Messenger and fast-flux attacks
- Detect and block exploits, phishing, ransomware and other modern malwares
- Identify malware propagation and lateral movement through east-west traffic monitoring
- Restrict user access to certain web content categories and track activity
- Protect brand with Lookalike Domain Monitoring for the most valuable Internet properties
- Control the risks of rising DoH use: block DoH (DNS over HTTPS) domain access and gracefully revert DoH requests to existing, trusted DNS

"Threat Defense enables our SOC analysts to take faster decisions based on highly accurate contextual information, which improves the overall time of analysis," said Hasan Imam, lead technical engineer at Secure Networks. "As DNS has become a more prominent attack vector these days, Askari Bank's proactive measures and professionalism towards securing this gap is highly admirable and sets a strong example within the industry of how to lead on security."

"To me, no other solution vendor is providing the level of DNS security that Infoblox is with Threat Defense," concluded Khalid Mirza. "By partnering with Infoblox, Askari Bank has the necessary protection for our DNS infrastructure that enables us to achieve our objectives on delivering secure services to our banking customers across Pakistan."



Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

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

+1.408.986.4000
www.infoblox.com

Version: 20250514v1