



## Arab National Bank

### Customer profile

One of the largest banks in the Middle East

### Industry

Banking

### IT environment

Approximately 5,500 endpoints, not including 720 servers—600 Microsoft Windows, 120 UNIX

### Challenge

Efficiently and effectively protect sensitive data across multiple locations, as well as comply with PCI and other financial regulations

### McAfee solution

- McAfee ePolicy Orchestrator software
- McAfee Endpoint Protection Suite Advanced
- McAfee Total Protection™ for Data
- McAfee Network DLP Prevention
- McAfee Network DLP Monitor
- McAfee Network DLP Discover
- McAfee Vulnerability Manager
- McAfee Email Gateway
- McAfee Change Control

### Results

- Reduces manpower required to manage endpoint security from six people to two
- Accelerates deployment of data loss protection—70 percent faster than competitive solutions
- Cuts administrative reporting from several days to minutes
- Saves \$152,000 in reduced manual intervention, thanks to integration with third-party security solutions

## McAfee Helps ANB Secure Customer Data, Stay Compliant, and Reduce TCO

Established in 1979, the Arab National Bank (ANB) is the third largest bank in the Kingdom of Saudi Arabia and one of the 10 largest banks in the Middle East. Headquartered in Riyadh, the bank provides services to retail and corporate customers through its 167 branches, which span the Kingdom of Saudi Arabia and its London branch, as well as via its 85 TeleMoney remittance service centers and 800 ATMs. The bank employs approximately 3,500 people and had a net income of USD\$579 million in 2011.

ANB prides itself on its technology leadership and is often the first in the region to adopt new technology to better serve its customers and meet business objectives. For instance, ANB was the first in Saudi Arabia to introduce Internet banking and SMS-based communications, and the first to be PCI certified.

### Top Bank Priority: Protect Customer Data

“We are constantly searching for ways to expand the bank’s reach and accessibility,” says Abdullah Al-Howish, head of the IT governance and compliance division at ANB. “However, no matter what new services or technology we introduce, the safety of our customer and bank data remains our top priority. Data protection is and always will be an inherent part of our core business strategy.” Compliance with Saudi Arabian Monetary Agency, PCI DSS, and international financial regulations; ANB customer confidence; and the bank’s reputation would all be at risk without adequate data protection.

### Choosing the Right Tools for the Security Operations Center

To improve data protection and compliance and to provide more effective, streamlined security management, ANB decided to build a security operations center (SOC). As part of that process, ANB IT assembled a team of experts to determine which security solutions should be implemented in the SOC. “We conducted a stringent due diligence process that included looking closely at our existing partners as well as other vendors,” states Al-Howish. “That’s when McAfee came into the picture in a major way.”

Prior to the SOC, ANB had used McAfee® Endpoint Protection for five years, gradually upgrading to McAfee Endpoint Protection Suite Advanced across its 5,500 PCs and laptops and 120 servers. ANB was extremely pleased with the solution and its central management console, McAfee® ePolicy Orchestrator® (McAfee ePO™) software. With the SOC initiative, ANB began to explore McAfee Data Loss Prevention (DLP) solutions as well.

“We looked at other data protection solutions, but McAfee was the only vendor that could meet all of our requirements for data loss protection,” declares Al-Howish. “In addition, McAfee data protection solutions were by far the easiest to deploy and manage, thanks to [McAfee] ePO [software]. We already knew how incredibly valuable [McAfee] ePO is, so it was an easy decision to stick with McAfee for this next security need—and the ones that followed.”

---

*“With McAfee ePO [software] and the unified McAfee platform, our team can much more seamlessly control security across our extended network, and with much lower TCO—both in terms of capital expenditure and operating expense—compared to other solutions in the market today.”*

—Abdullah Al-Howish  
Head of IT Governance  
and Compliance  
Arab National Bank

---

### Lower TCO and Easier Administration

Initially, ANB used McAfee ePO software to manage functionality within the McAfee Endpoint Protection Suite Advanced, including anti-malware, antispam, host intrusion prevention, desktop firewall, and host web filtering. ANB plans to add the solution's network access control and policy auditing functionality in the near future. With the introduction of the SOC, ANB next rolled out McAfee Total Protection for Data, which includes host data loss prevention, endpoint encryption, and device control. Concurrently, ANB deployed two McAfee Email Gateway appliances and McAfee Vulnerability Manager. A year later, the bank added McAfee Network Data Loss Prevention, McAfee Data Loss Prevention Monitor, and McAfee Data Loss Prevention Discover appliances to its network defense, and McAfee Change Control and McAfee Application Control to lock down its ATMs. Today, all of these security solutions—across endpoint, data, and network—are managed and monitored from a single console: McAfee ePO software.

“Security information from all these solutions feed into [McAfee] ePO [software] to give us up-to-date, comprehensive visibility, which enables faster decision making and faster response to threats or vulnerabilities,” notes Al-Howish. “With McAfee ePO [software] and the Security Connected platform, our team can much more seamlessly control security across our extended network, and with much lower TCO—both in terms of capital expenditure and operating expense—compared to other solutions in the market today.”

### Accelerated Deployment and Dramatic Time and Cost Savings

McAfee ePO software significantly accelerated the deployment of each of the McAfee security solutions. “When we deployed the McAfee data protection solutions, we met all of our 18 objectives within three months, whereas it would have taken over 10 months—more than three times as long—with competitive data protection solutions,” adds Al-Howish. “Having an easy-to-use central console that can automatically push out software agents and updates makes a huge difference.”

Using McAfee ePO software to manage endpoint protection across all 5,500 endpoints saved ANB security administration so much time that four people were freed up to focus on strategic objectives rather than troubleshooting and other reactive tasks. Security status reports, such as systems lacking up-to-date protection or locations of current vulnerabilities that used to take days or even weeks to prepare now take seconds or minutes with McAfee ePO software. Updating and patching software agents across thousands of endpoints can now be completed within 15 to 20 minutes.

Furthermore, ANB reaps additional time savings from its integration of McAfee ePO software with third-party solutions from McAfee Security Innovation Alliance partners ArcSight and HP. Security events captured by McAfee ePO software are automatically picked up by ArcSight security information and event management (SIEM) agents and fed into ANB's SOC for enhanced, more accurate analysis and reporting of security events. ANB estimates savings of 1,900 man-hours, or roughly \$152,000, due simply to reduced manual intervention enabled by McAfee ePO software integration with these two solutions.

### Monitoring and Discovering Sensitive Data Proves Compliance

ANB uses McAfee Network Data Loss Prevention appliances to determine what sensitive data to protect, monitor all sensitive data at rest and in motion, and enforce policies to prevent sensitive data from leaving the enterprise. Implementing McAfee Network DLP helped the bank gain a much deeper understanding of how bank and customer sensitive data moves within and how and when that data is at risk of exposure or loss.

“In addition to enabling us to run inventory assets across our extended enterprise, McAfee Network DLP immediately uncovered corporate policy violations and potential data loss risks that we didn't know about before,” remarks Al-Howish. For instance, ANB discovered sensitive information embedded in managers' reports and employee bios, and misuses of WAN connections. “Once we knew about these inadvertently risky practices, we then took measures to prevent them, including educating employees.”

Such comprehensive visibility into where sensitive data is and how and when it moves provides the proof of compliance required by ANB's internal and external auditors, senior management, and other stakeholders. "McAfee Network DLP makes compliance many times easier," notes Al-Howish. "We can tell immediately the who, what, where, and when of any data movement that needs investigation. We can also perform analytics on metadata much faster and more efficiently. Overall, we can now detect and remediate policy violations much more reliably."

---

*"McAfee Network DLP makes compliance many times easier. We can tell right away the who, what, where, and when of any data movement that needs investigation. We can also perform analytics on metadata much faster and more efficiently, and detect and remediate policy violations much more reliably."*

—Abdullah Al-Howish  
Head of IT Governance  
and Compliance  
Arab National Bank

---

### Preventing Data Loss Across All Devices

"Approximately 80 percent of our data loss prevention requirements are met by the host DLP protection in McAfee Total Protection for Data, but the other 20 percent—which is increasing as more mobile devices connect to our network—are covered by McAfee Network Data Loss Prevention," explains Al-Howish. Since both forms of DLP are integrated in McAfee ePO software, they can share tags and "learn" from each other. "By using both forms of data loss prevention, we have a multilayered defense that protects data across all our endpoints, regardless of operating system or type of device."

Furthermore, with McAfee Total Protection for Data, integrated with Microsoft Active Directory, ANB security administrators can control data-related policies at a highly granular level. Now, bank administrators can specify detailed content-based filtering, monitoring, and blocking of confidential data on any removable storage device. They also have the flexibility to make exceptions, so that specific actions don't trigger false positives. As a result, ANB has implemented a wide range of sophisticated data access policies based on each user's role and organizational unit. Only bank management executives have the ability to copy data to and from USB encrypted flash drives. Other groups within ANB have read-only access to such drives, while secondary groups, such as bank tellers, are unable to utilize removable storage media to completely eliminate the risk of data loss.

### McAfee—More Just a Technology Provider

"No single security solution is ever enough to keep an enterprise safe," declares Al-Howish. "This is why we have a multilayered security strategy. We have integrated security solutions and policies, and central management—all of which add up to a more proactive security posture. I can sleep much better knowing McAfee is protecting our data."

Al-Howish has been extremely pleased with McAfee because he sees the value the solutions bring to the business. "Anyone in a position similar to mine knows what a difference it makes to have a vendor that works closely with you both before and after the sale," he affirms. "McAfee has consistently delivered excellent advice and support and is so much more than just a technology solution provider. We consider McAfee to be one of our key partners."

