IDC Analyze the Future

IDC ExpertROI® SPOTLIGHT

# National Bank Minimizes Security Risk and Supports New Business with McAfee Security Solutions

Sponsored by: McAfee

Matthew Marden Robert Ayoub

February 2017

## Overview

As cyberattacks become more frequent and security threats become more evasive, pernicious, and costly, organizations must take ever more powerful countermeasures. A U.S. bank that serves a growing clientele of companies and other business customers recognized the threat posed to its competitive position by security-related incidents. To ensure business continuity and prevent financial and reputational loss that could result from a successful attack, the bank has deployed the McAfee suite of security products.

The bank, which ranks as one of the nation's top 100 FDIC banks by asset size, prides itself on helping its clients achieve their business-related objectives. As a leading financial services organization, the bank can ill afford to even have its name associated with security or data incidents that could cause substantial reputational or financial damage. As a result, the information security officer of the bank explained that it views maintaining a robust security environment that ensures business continuity as a top IT and business priority.

The bank first realized that it needed to take a more proactive stance toward network security after suffering an impactful security incident about seven years ago. At that time, it deployed McAfee Antivirus software as well as the McAfee Security Information and Event Management (SIEM) solution. Several years later, it added McAfee Threat Intelligence Exchange and McAfee Advanced Threat Defense, in addition to McAfee Endpoint Security and McAfee Data Loss Prevention.

According to the information security officer, these McAfee products have been instrumental in significantly improving the bank's network security. The information security officer indicated that the bank has largely avoided impactful network-related security events since deploying McAfee, in part because of how the various McAfee products

**Business Value Highlights**

**Organization:** National U.S. bank

**Challenge:** Ensure business continuity by minimizing the impact of network-related security incidents

**Solution:** McAfee Security solutions, including McAfee Antivirus software, McAfee Security Information and Event Management, McAfee Threat Intelligence Exchange, McAfee Endpoint Security, McAfee Data Loss Prevention, and McAfee Advanced Threat Defense

**Four-Year Cumulative Benefits:**

- Four-year benefits worth $8.68 million
- Return on investment (ROI) of 208%
- Payback in 20 months

**Other Benefits:**

- 90% faster resolution of security events
- 77% fewer impactful security events per year
- 98% less productive time lost because of impactful security events
- Support generation of $5–10 million in additional revenue per year

complement each other. In particular, the bank can now rapidly identify and contain any potential threats and take prompt remedial steps, thereby limiting the potential consequences of the threats. Endpoint security with McAfee is an important component of this for the bank by providing local malware protection and enabling communication between endpoints and the rest of the organization, allowing key threat information to be exchanged and minimizing the likelihood of unauthorized behavior. This capability has proven especially valuable as the bank has doubled the number of employees working on its network in recent years.

The bank's improved security posture with McAfee has meant significantly fewer user-impacting security events and faster resolution of such events when they do occur. As a result, these events exert a substantially lower toll in terms of lost employee productivity and potential revenue losses. In addition, the bank has been able to avoid larger-scale security events that can substantially affect users and cause reputational and financial harm. According to the information security officer, some of the client prospects of the bank proactively seek out information about the bank's security measures when making their banking decisions, and he believes that the bank's robust security environment with McAfee in place has contributed to winning a substantial amount of new business.

Based on several interviews with the information security officer of the bank, IDC found that the bank's use of the McAfee solutions has reduced infrastructure costs, improved both user and security staff productivity, and increased business revenue. IDC analysis shows that the bank will achieve benefits worth an average of $3.02 million per year over four years, resulting in a four-year return on investment (ROI) of 208% and a payback period of 20 months.

## Implementation

The bank first looked into deploying the McAfee SIEM solution in 2010 after suffering a cyberattack that required restricting internet service to its employees for a number of days. After evaluating products from four vendors, the bank chose the McAfee solution based on its performance and user-friendly interface. According to the information security officer, McAfee's approach also impressed the bank: "McAfee flew in six experts from all over the country to demonstrate its solution. They explained what the solution could do and why it was a good fit for us and never said a negative word about rival products. After the sale, McAfee brought a training person onsite, and within the first hour, we recognized some network problems and were able to fix them."

With McAfee SIEM in place, the bank significantly reduced its security exposure but still perceived a need to make its security position more pervasive and effective to support its business operations and meet evolving security challenges and expectations of its clientele. As a result, in 2013, when the bank decided to upgrade its security infrastructure, it again chose products — McAfee Threat Intelligence Exchange, McAfee Advanced Threat Defense, McAfee Endpoint Security, and McAfee Data Loss Prevention — from the McAfee suite, in large part because of the McAfee Global Threat Intelligence service. "We recognized that all of McAfee's tools were good, but we asked ourselves if there was extra value from having the tools work together with the threat intelligence service," said the information security officer. "We found there was."

This service unifies the McAfee security products and equips them to work in concert to thwart the most evasive security threats. The service draws on data collected from millions of McAfee products around the world, which act as sensors for the latest types of threats, including never-before-seen techniques and payloads. The McAfee suite of products can query this data via the cloud to obtain the intelligence needed to block threats, identify compromises, and expedite remediation.

The bank now uses the SIEM solution in concert with the McAfee Data Loss Prevention and Advanced Threat Defense products, using McAfee Threat Intelligence Exchange to communicate what new threats are emerging so that necessary action can be taken. According to the information security officer: "The McAfee tools have been working together for the past two years and have shown that the unified solution is greater than the sum of the individual parts."

## Benefits

With the deployment of the McAfee suite of security products and the Global Threat Intelligence service, the bank has considerably reduced its exposure to operational and reputational loss because of network-related security threats. It has achieved this benefit by substantially limiting the frequency of user-impacting security events and resolving them far faster, even as it has more than doubled the number of employees using applications on its network. As a result, it has minimized the impact of outages on its employees and business, which is especially beneficial given this growth. Further, it has avoided having its name tied to a major security-related event and positioned itself to compete more strongly for the business of security-conscious clients and businesses.

The information security officer explained that the McAfee suite of products his organization is using enables these benefits by integrating dynamic endpoint protection with intelligent analytics and a centralized management platform. This adaptive, open system reduces the number of threats that get through firewalls and helps the bank's incident response teams find incidents in much less time. Security and threat insights trigger automated action to expedite cleanup and quickly adapt current security policies, further reducing the likelihood of events becoming user impacting and meaning that less IT staff time is needed to take these actions. Further, by learning from security incidents never seen before, the system evolves continually, providing better protection going forward.

**"We can now do more valuable analyses and data correlations much faster. We can quickly identify events at different parts of the network, see if they're related, and track back to the first instance to determine when, where, and how the incident occurred."**

The net result is that the McAfee products have better secured the bank's employees, work devices, and servers. "We can now do more valuable analyses and data correlations much faster," said the bank's information security officer. "We can quickly identify events at different parts of the network, see if they're related, and track back to the first instance to determine when, where, and how the incident occurred. We can also monitor our environment through just one or two panes of glass, which makes it easier to figure out how to contain the problem and retain control of the environment."

He explained that before deploying McAfee, the bank experienced more frequent user-impacting security events that generally took substantially longer to resolve. Most importantly for the bank, it has now minimized the risk of infrequent but damaging security events that can affect its entire business operations for days at a time. Further, these events required the time of up to six to eight members of the bank's security and IT teams for up to a week to achieve full resolution.

More commonly, events impacting individual users can require confiscation of the infected workstations, which limits productivity for the several days it would take to provide replacements or fully resolve the problem. Events affecting remote users were particularly disruptive; they might be without their workstations for three or four days. Medium-impact attacks affecting groups of 30 or 40 users would limit user productivity even more because of the importance of the workstations in their work.

The information security officer reported that with McAfee in place, the frequency of user-impacting events has declined by almost 80% from about one per week to one per month, even as the bank's employee user base has more than doubled. Moreover, McAfee helps identify and resolve potential issues in far less time: "Now we can detect an attack within 60 seconds and complete the analysis to contain it within five minutes," said the information security officer. "Removing the virus and cleaning up afterward might take one or two minutes." He compared this with the hours or even days it took to identify and remove security-related issues before using McAfee (>99% faster). Once security-related issues are identified, McAfee also helps the bank move to full resolution in far less time; the information security officer said that it now takes about four hours in total per security event compared with a full workweek previously (90% faster).

For the bank, this means that McAfee has limited the disruption caused by network-related security events. Most importantly, the bank has confidence that it will not experience more significant security events that can affect its business. This has contributed to better positioning the bank to hold onto its clients and even win new business. Because of its track record of blocking attacks, the bank has avoided the unfavorable publicity suffered by other institutions. As the information security officer said, "McAfee has helped us stay out of the news, which is invaluable for us."

**"McAfee has allowed us to fundamentally tackle security, which has given us more comfort in handling customers and presenting our strong security posture in sales meetings."**

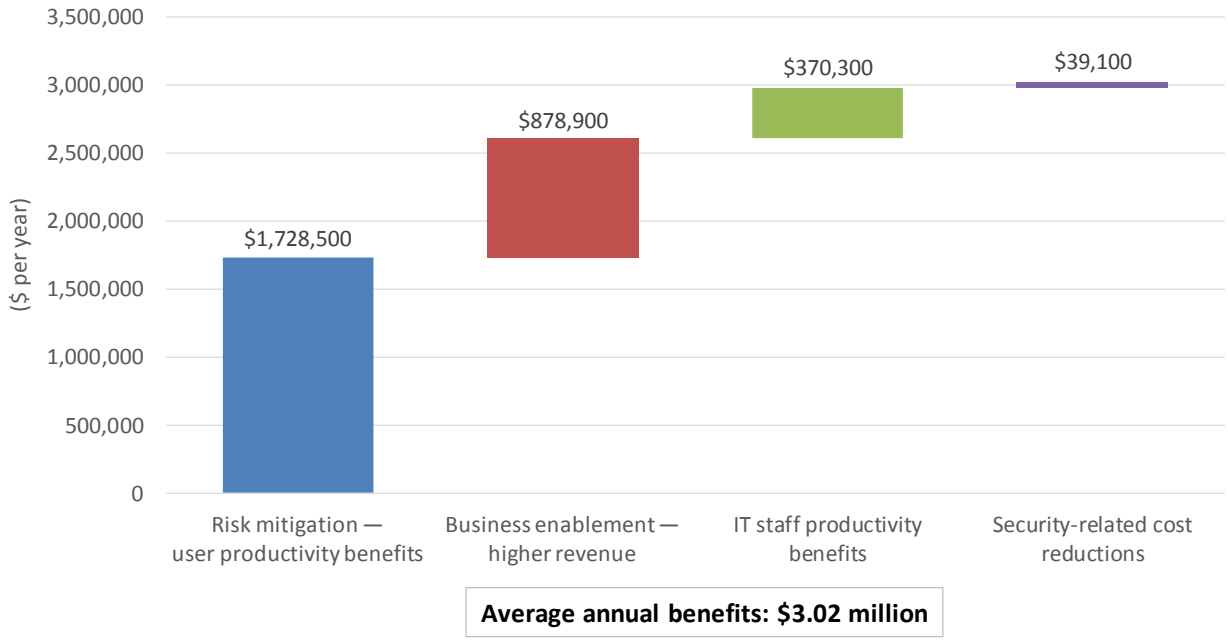
In addition, he noted that the prospective customers of the bank increasingly view its security capabilities as core to its value proposition. He said that he has been involved in many presentations with potential customers where security was a key topic, and he believes that improved security has contributed to winning a number of new clients worth millions of dollars of new revenue per year. He explained: "McAfee has allowed us to fundamentally tackle security, which has given us more comfort in handling customers and presenting our strong security posture in sales meetings."

## Quantifying the Benefits

By interviewing the bank's information security officer and asking questions about operations before and after deploying the McAfee suite of security products, IDC was able to quantify the benefits the bank is achieving. IDC calculates that when projected over four years, the benefits will average $3.02 million per year (see Figure 1). IDC used a four-year analysis because the bank required about one year to deploy the McAfee solutions and targets three-year refresh cycles.

## FIGURE 1

**Average Annual Benefits**




Source: IDC, 2017

### *Risk Mitigation — User Productivity Benefits*

Security events have the potential to exert a significant cost to the bank by limiting employee productivity and even causing lost revenue as these events are identified and resolved. With McAfee in place, the bank has significantly limited the frequency and duration of these types of events as well as their impact on its business operations. The value of this benefit is even more significant given growth to the bank's employee base accessing applications and services on the bank's network since deploying McAfee. IDC projects that in total, the bank will achieve benefits worth an annual average of $1.73 million in value by limiting the business and operational effect of security events over four years by:

- Experiencing fewer events that impact the broader organization, up to and including shutting down internet access, and enabling much faster resolution of larger-scale problems
- Limiting the frequency of more isolated security events that affect one or several employees and may require taking their workstations to be repaired
- Avoiding relatively minimal revenue losses associated with these events

### *Business Enablement — Higher Revenue*

The bank's record of avoiding major cyberattacks has positioned the bank to win new business. The bank's clients, which are aware of the criticality of network security, have increasingly focused on security as a driver of their choice of banking services. Since deploying the McAfee suite, the bank not only has avoided potentially reputation-tarnishing news reports of security events impacting its business but also is able to support its sales efforts with its track record. Assuming the security record was only one factor involved in winning additional business, IDC puts the value of increased revenue at an average of $878,900 annually over four years.

### *IT Staff Productivity Benefits*

Decreased frequency of user-impacting security events and the ability to resolve events much faster mean that the bank devotes less security team and IT staff time to identifying, containing, and resolving such events. In addition, automated monitoring with the McAfee security solutions means that these teams can handle such day-to-day activities more efficiently. IDC calculates that in total, the bank will save IT staff time worth an average of $370,300 per year over four years.

### *Security-Related Cost Reductions*

The bank has realized savings by discontinuing its use of other security products even as it has improved its security posture with McAfee. On average, the annual savings in licensing costs for the displaced software amounts to $39,100 when projected over four years.

## Return-on-Investment Analysis

IDC projects that the bank will realize a four-year ROI of 208% from its deployment of the McAfee solutions. Payback on the investment occurred within 20 months (see Table 1).

**TABLE 1**

**Four-Year ROI Analysis**

| | |
|---|---|
| Benefit (discounted) | $8.68 million |
| Investment (discounted) | $2.81 million |
| Net present value (NPV) | $5.87 million |
| Return on investment (ROI) | 208% |
| Payback period | 20 months |
| Discount rate | 12% |

Source: IDC, 2017

IDC conducted several interviews with the bank's information security officer to understand the impact of the investment in the McAfee suite of security products from McAfee on the bank's operations and business. IDC used these interviews to gather the information needed to quantify the benefits and investment associated with the bank's use of the products as outlined in this study and created an ROI analysis from the results.

IDC calculates the ROI and payback period in a three-step process:

1. Measure the financial benefits directly resulting from the solution, including higher user productivity, revenue gains, and reduced security-related costs since deployment.
2. Ascertain the total investment.
3. Project the investment and benefit over four years and calculate the ROI and payback period. The ROI is the four-year net present value (NPV) divided by the investment. Payback period (expressed in months) is the time required to pay back the initial investment and establish a positive cash flow. To account for the time value of money, IDC bases the ROI and payback period calculations on a 12% discounted cash flow.

## About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

## Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com

---