Case Study

Budapest Bank

Replaces IT Security Infrastructure with Help from Symantec™

Challenge

Following its 2015 sale to the Hungarian national government, Budapest Bank needed to stand up a comprehensive, new IT security environment to protect its infrastructure, endpoints, and data.

Solution

- Symantec Endpoint Protection
- Symantec Data Loss Prevention Enforce Platform
- Symantec Endpoint Encryption
- Symantec Data Loss Prevention Cloud Service for Email with Cloud Console

Benefits

- Comprehensive endpoint protection that effectively stops advanced threats based on the world's largest civilian threat intelligence network
- Automated enforcement of data loss prevention policies with centralized device control, incident detection, remediation, reporting, and system management
- Strong laptop data security with full disk and removable media encryption, centralized management, and reporting
- Secure email in the cloud with PGP encryption technology

Symantec Strategic Partner

Quadron Cybersecurity Services

Client Profile

Organization: Budapest Bank
Site: budapestbank.hu
Industry: Financial services
Headquarters: Budapest, Hungary
Employees: 2,800

Budapest Bank, a full-service commercial bank based in Budapest, Hungary, was part of GE Capital until 2015, when it was sold to the Hungarian government, requiring a complete replacement of the bank's IT security infrastructure. By choosing Symantec™ solutions to replace former tools for endpoint and data security, Budapest Bank gained adaptive, in-depth protection for its servers, desktops, and laptops; centralized data-loss prevention with universal policy enforcement; and strong full-disk encryption for all laptops. With a better integrated security stack and local hands-on management, Budapest Bank has tightened its IT security and lowered costs and is now finalizing a project to secure and encrypt email.

Retooling IT Security

With 2016 assets of US$3.4 billion, annual revenue of US$230 million, and nearly 100 branch offices, Budapest Bank is one of Hungary's largest universal banks. Its IT environment includes more than 100 applications, two data centers, local and wide-area networks, and the usual range of client systems to support 2,800 employees.

After the sale to the Hungarian government, Aurél Huszthy-Torok, the bank's IT security, risk, and compliance leader, knew he could improve Budapest Bank's security and reduce costs by replacing the IT security environment with purpose-built infrastructure selected, scaled, and managed specifically to the bank's exact needs.

Drawing on the annual threat report issued by European Union Agency for Network and Information Security (ENISA), Huszthy-Torok and his team devised a requirements list for a new multilayered defense that would secure the bank's endpoints, applications, data, and networks against the evolving threat landscape. They issued requests for proposals and evaluated the results on functionality, cost, and local integration support.

Combining Endpoint and Data Security

Symantec and local partner Quadron Cybersecurity Services submitted the winning proposals for three key components—endpoint protection, data loss prevention (DLP), and endpoint encryption. "We really wanted a solution that combined DLP with classic endpoint protection tasks," Huszthy-Torok says. "Symantec gave us that functionality from a single vendor, and Quadron brought the local product expertise."

"When we heard about WannaCry, we immediately checked our reports from Symantec and other security tools to see if the vulnerability was known and the antivirus engines were up-to-date, which they were. Of course, we monitored our logs and reports a little more closely than usual, but we knew we were protected."

– Aurél Huszthy-Torok, IT Security, Risk, and Compliance Leader, Budapest Bank

For system security on all its endpoints—servers, desktops, and laptops—the bank chose Symantec Endpoint Protection. "In addition to the traditional antivirus function, we use nearly every feature this solution offers," Huszthy-Torok says. "We've created location-based policies for the firewall, and we rely on its intrusion prevention, reputation-checking, and traffic-blocking capabilities. We enforce our removable media policy with the device management function, and if any malware gets through, application control lets us find and terminate its activities. It's also made us more efficient. We can easily build multiple installation packages for different assets because a single template isn't always a good fit."

The bank chose Symantec Data Loss Prevention Enforce Platform for its combination of automated data policy enforcement, centralized detection, incident remediation, reporting, and system management. Now the security team can define data policies once and apply them across network storage and endpoints. The platform monitors outgoing email and will, for example, allow a customer to receive a bank statement if there is only one customer account number in the message. But if the message contains multiple files of protected data, it will flag the message and issue an alert.

Because the bank's network proxy provides Secure Sockets Layer (SSL) decryption, the DLP platform can also inspect internet data, even if it's encrypted. "Now we can block uploads to personal network shares and see what data is entered in online services like Google Translate," Huszthy-Torok says. "Of course, we block most such services except for employees with a legitimate need, and we block the use of peripheral storage devices."

To secure the data on its 1,100 laptops, the bank also deploys Symantec Endpoint Encryption, which combines strong full disk and removable media encryption with centralized management and reporting. "We encrypt all of our laptops," Huszthy-Torok says. "We can afford to replace a lost or stolen machine if we have to, but we can't afford to lose that data."

Surviving WannaCry

Budapest Bank's new IT security infrastructure is a multilayered, multivendor security environment that has already proven remarkably agile and robust. When the WannaCry ransomware outbreak struck suddenly in May 2017, encrypting hundreds of thousands of systems worldwide and holding them for ransom, the bank's systems were saved by Symantec Endpoint Protection, which draws upon the world's largest civilian threat intelligence network. "When we heard about WannaCry, we immediately checked our reports from Symantec and other security tools to see if the vulnerability was known and the antivirus engines were up-to-date, which they were," Huszthy-Torok says. "Of course, we monitored our logs and reports a little more closely than usual, but we knew we were protected." Not one of the bank's systems with Symantec Endpoint Protection was infected by the WannaCry virus.

Symantec endpoint security solutions also helped the bank manage a recent zero-day incident. "The attack vector was a phishing email, and it was an hour or two before we realized what had happened," Huszthy-Torok says. "We isolated the affected machines, deleted the suspect email, and uploaded the sample into the Symantec portal. In a half hour, all of our antivirus engines had been updated with the new signatures and all further infections were stopped."

"We now have the devices, the tools, and the processes we need to keep the bank safe. Most of the time I sleep soundly in my own bed, and Symantec is an important part of that."

– Aurél Huszthy-Torok, IT Security, Risk, and Compliance Leader, Budapest Bank

Securing Email in the Cloud

Huszthy-Torok and his team have almost completed the last part of their new security environment, a secure email system for both sensitive data exchange and threat protection that uses Symantec Data Loss Prevention Cloud Service for Email with Cloud Console. "We'll have a webmail inbox where internal users can send encrypted messages," he says. "External users will be able to register, receive messages, and open them in a secure environment. It uses public internet transport, but all the messages are encrypted using PGP technology. We'll use it as needed to supplement our existing Exchange service." When it comes to threats, the system delivers additional protection against spear phishing and ransomware attacks.

Ensuring the CISO has a Good Night's Sleep

Budapest Bank's new IT security infrastructure is a far better fit for the organization than its old environment. Every component was chosen for functional fit, cost-effectiveness, ease of integration, and local support. With its comprehensive endpoint and data security, the bank is also well-prepared for the European Union's General Data Protection Regulation (GDPR), which takes effect in May 2018.

But for Huszthy-Torok, the greatest benefit may be a good night's sleep. "Have you seen the cartoon about 'How do IT managers sleep?'" he asks. "The CIO is asleep in his bed; the infrastructure leaders are asleep in their beds; but the CISO's bed is empty because he can never sleep. My experience is not like that because we now have the devices, the tools, and the processes we need to keep the bank safe. Most of the time I sleep soundly in my own bed, and Symantec is an important part of that."

For Additional Information

Contact your local Symantec Sales Representative or Business Partner, or visit: broadcom.com

Symantec™
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com

SED-BUD-BANK-CS100 June 8, 2020