Caixa Seguradora protects critical data with web and email security

Reduces incident response time from days to hours, enhances cloud defenses

As the fifth largest insurance company in Brazil, Caixa Seguradora provides a wide variety of insurance solutions to individuals, companies, and the public sector. These offerings include life, auto, health, business, and home insurance, among others. Based in Brazil, Caixa Seguradora employs more than 1000 people in Brazil and Argentina, and serves over 12 million customers.

Operating in such a sensitive and highly regulated industry, Caixa Seguradora's IT team realizes the critical importance of filtering access to content to protect employee and customer data. However, the company must also provide employees with unhindered access to various applications for effective communication with external partners and clients. Achieving and maintaining this balance is the key focus of Caixa Seguradora's web and email security strategy.

Executive summary

Customer name:
Caixa Seguradora

Industry:
Insurance

Location:
Brazil

Employees:
1000+

Challenges

- Providing seamless Internet access to 1000+ employees while still safeguarding company data
- Protecting employees from spam and phishing emails
- Securing the use of cloud services

Solution

- Cisco Web Security Appliance (WSA)
- Cisco Email Security
- Cisco Advanced Malware Protection (AMP) for Email Security

Results

- 90 to 95 percent of emails blocked due to suspicious characteristics
- 25 to 30 percent of web transactions blocked
- Enhanced protection from cyberattacks and data theft

Web security to protect user and company information

Caixa Seguradora is using Cisco® Web Security to monitor and control employee and guest access to various web sites and cloud-based applications. For example, the company prohibits and blocks users from accessing public email services such as Hotmail, Yahoo, and Gmail to limit the risk of data loss. According to Caixa Seguradora Network Specialist Diogo Rodrigues de Sousa, the web blocking available via firewalls is not sophisticated enough for these needs, which is why the company turned to the Cisco Web Security Appliance (WSA) for more granular capabilities.

By automatically blocking risky web sites and testing unknown sites before allowing users to link to them, Cisco WSA improves security and compliance. Today, Caixa Seguradora is finding that 25 to 30 percent of its web transactions are suspicious and blocked by Cisco WSA. For example, in one month, approximately 80 million of the company's web transactions were allowed and 33 million were blocked. Cisco WSA also blocked 400,000 attempted uses of company-forbidden applications in one month, such as online content sharing platforms like Dropbox, Google Drive, and OneDrive.

"Cisco WSA is one of the most important pieces of security we have," said Rodrigues. "Access to the Internet is essential for many aspects of our business, yet this access needs to be very well protected to prevent the loss of user and company information."

According to Rodrigues, the web reputation capabilities of the WSA are especially beneficial since protection is achieved dynamically. "If one of my users tries to go to a site that is unfamiliar to our systems, WSA will automatically allow or block access based on the site's reputation without the need for me to create a static policy," he said.

Email security to prevent phishing and data loss

Another key piece of security for Caixa Seguradora is Cisco Email Security. "Email security is crucial for our company," said Rodrigues. "Email is our primary means of communication, but it is often used by attackers to phish and steal information."

Cisco Email Security protects companies against ransomware, business email compromise, spam, and phishing. Caixa Seguradora's employees exchange millions of emails per day. Cisco Email Security is blocking 90 to 95 percent of those emails due to suspicious or malicious qualities.

According to Rodrigues, Caixa Seguradora tested several email security products before selecting Cisco, and found that Cisco Email Security was the most accurate when it came to correctly classifying emails as valid or suspicious. He described an incident in which his employees' information was leaked to a marketing company by a third party. All of the employees began to receive spam from this organization, but Caixa Seguradora's IT team was able to easily stop it with rapid and simple configuration in Cisco Email Security.

“Cisco WSA is one of the most important pieces of security we have.”

“Cisco Email Security is blocking 90 to 95 percent of our emails due to suspicious or malicious qualities.”

Diogo Rodrigues de Sousa
Network Specialist,
Caixa Seguradora

For more information

Find out more at cisco.com/go/security.

Cisco Email Security also blocked a targeted cyberattack on Caixa Seguradora that was launched via email. “To our users, the emails would have appeared to be legitimate,” said Rodrigues. “But they were malicious, and Cisco Email Security recognized that and blocked thousands of them.”

Caixa Seguradora has also recently deployed Cisco Advanced Malware Protection (AMP) for Email Security. AMP analyzes emails for threats such as zero-day exploits hidden in attachments to protect against sophisticated attacks. “Although we have just started to use it, AMP seems to be a very effective solution for detecting and blocking damaging files within emails,” said Rodrigues.

Enhanced cloud security

Cisco is also helping Caixa Seguradora secure its transition from on-premises IT services to cloud-based services. This transition can often be challenging due to a loss of visibility into which services employees are using and how exactly they are being used. With Cisco WSA and Email Security, Caixa Seguradora can monitor usage of these cloud services and block suspicious transactions for better cloud security.

“At the end of the day, Cisco is reducing our incident response time from days to hours,” said Rodrigues.

C36-741443-00 10/18