



# Brazil's Credit Union SICREDI Selects eEye's Retina Scanner to Tame its Network Security Issues

## The Challenge: Gaining Fine-Grained Security Analytics

While the financial sector in the U.S. is being swamped with regulations aimed at shoring up and standardizing Internet security, this is not the case in many other countries.

In Brazil no formal regulations exist to address Internet security, yet the financial sector is increasingly global, meaning Brazilian banks cannot ignore regulatory trends that are happening outside their country. Banks in Brazil keep an eye on U.S. regulations such as PCI and SOX and do their best to bridge regulations intended for other countries with their own unique needs.



### Customer:

Credit Union SICREDI  
of Brazil, South America

### Fast Facts:

Financial institution with  
locations across central  
and southern Brazil

13,000 workstations  
and 900 servers

Serves 1.5 million customers

### Key IT challenge:

Finding a comprehensive  
vulnerability scanning solution  
to help them regain control of  
their heterogeneous network

SICREDI, which has branches across central and southern Brazil, serves approximately 1.5 million customers. While SICREDI is considered as having a fairly mature security posture versus other banks in South America, the credit union knew that it could be at risk if it didn't continue to bolster its security profile.

Compared to other South American banks, SICREDI considers itself secure; compared to United States and European Union banks, however, they posed an enticing target for hackers.

SICREDI had robust perimeter security in place, but it lacked advanced security tools. The credit union needed to gain insight into specific security incidents, assess network and end point vulnerabilities, determine which incidents and vulnerabilities were the most risky and develop a deeper understanding of its changing network and the security needed to protect it.

### Selection Criteria: Automating Manual Tasks and Increasing Visibility into the Network

SICREDI's internal network began small, with only a few servers and a small number of workstations. However, as the credit union grew, as more and more branches moved onto the Internet and as more tech-savvy individuals configured devices to meet their own needs, IT quickly lost control over the environment's security.

Firewalls and antivirus tools may ward off threats – but only known threats. Moreover, with an out-of-control computing environment, it's difficult for IT to even know where vulnerabilities exist and what holes will entice hackers.



What happens if someone turns off their antivirus? What if a patch created a new security hole? How many patches and updates were needed that they didn't know existed?

SICREDI's IT team knew that it needed to get a better handle on its environment. They also knew that they were exposed to both internal and external threats.

Moreover, they hoped that next-generation security tools would help them automate some of the cumbersome IT tasks contributing to network sprawl, increasing vulnerabilities and security blind spots.

SICREDI began its quest to improve its security by investigating vulnerability scanners. They looked at tools from other vendors, but felt neither offered the features they sought.

## The Answer: eEye's Retina Network Security Scanner

SICREDI next tested the Retina Network Security Scanner from eEye Digital Security. "The first thing we noticed was that Retina's scan returned no false positives. Not a single one," said Tiago Wegner, IT Infrastructure Coordinator for SICREDI. "No other vulnerability scanner we tested performed so well."

The Retina Network Security Scanner provides multi-platform vulnerability management. Retina identifies known and zero-day vulnerabilities and provides security risk assessments that enable security best practices, policy enforcement, and compliance with regulatory audits.

Retina is able to scan an entire Class C network in less than 15 minutes, discovering all networked devices. Retina also discovers wireless devices and their configurations, ensuring these connections can be audited for the appropriate security settings. If it has an IP address, Retina will find and assess it.

SICREDI was impressed with the demonstration, but its research wasn't finished. The company wanted to learn whether or not eEye, a U.S. company, could address the needs of a Brazilian financial institution.

SICREDI did its research and soon discovered that eEye - unlike a number of security vendors - has several customers in Brazil, including TIM Brasil, a Telecom Italia Group subsidiary

"We talked with some IT people at TIM Brasil, who endorsed eEye, and we were pleased to learn that eEye has a number of customers in the financial sector," said Wegner. "It was clear that they would understand our needs."

A final deciding factor was that eEye offers a security management tool, Retina Enterprise which would not only simplify security management in the short term, but would also help automate various IT-security tasks and scale to meet future security needs as the SICREDI network expanded.

### Key Benefits:

Comprehensive vulnerability testing

Detection of all vulnerabilities, including unpatched systems and misconfigurations

Zero false positives

Discovery of all connected computers, routers, and other network devices, even those not officially deployed

Ability to prioritize risks and focus on the most pressing threats

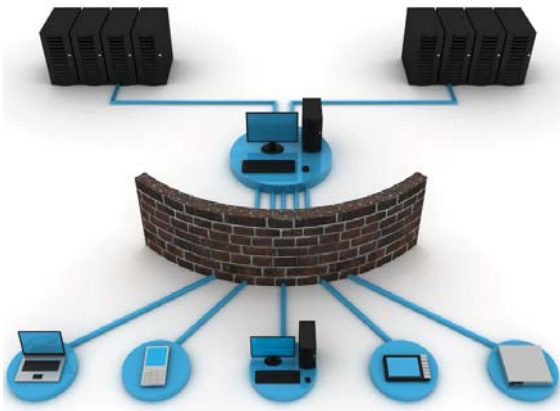
Centralized security management that provides a single point of visibility into and control over the network



eEye Digital Security®

To learn more, please visit [www.eeye.com](http://www.eeye.com)  
or call 866.282.8276





## Deploying Retina Enterprise to Control a Mixed-OS Environment

It took approximately 12 months for SICREDI to fully deploy Retina Enterprise. This may sound like a long time until you consider the particulars. The SICREDI IT staff must cope with a mixed computing environment that includes Linux, Microsoft and IBM AIX servers, as well as workstations running both Red Hat Linux and different versions of Windows. The network comprises 900 servers and 13,000 workstations spread across a number of different branches.

The Retina Enterprise rollout was partitioned, integrating certain types of servers, such as those powering ATMs versus those running e-commerce applications, one at a time.

“The Retina Enterprise roll out was very smooth,” said Rafael Dreher, IT Security Analyst for SICREDI. “We experienced no conflicts and everything went as planned.”

## Gaining Control over a Complicated Network

With Retina Enterprise in place, SICREDI’s IT staff began to tame the security of its network environment. “We knew that we had many flaws, but we didn’t know where they were or which ones were the most dangerous,” Dreher said.

Retina not only discovered flaws, vulnerabilities and patching gaps, but it also enabled SICREDI to prioritize and fix the most critical problems first.

In the past, SICREDI patched each program or applied each software update manually, machine by machine. If the team didn’t know about a machine or couldn’t apply a patch because of conflicts, SICREDI was at risk.

“There are special situations where we can’t follow a patching process right away,” said Wegner. “Retina Enterprise helps us protect ourselves in the meantime.”

Designed for enterprise scalability, Retina Enterprise provides SICREDI with a single point of visibility into and a centralized point of control over its entire network. Unpatched machines are protected from known and zero-day vulnerabilities and IT is immediately alerted to any security incident or potential threat.

***“The first thing we noticed was that Retina’s scan returned no false positives. Not a single one. No other vulnerability scanner we tested performed so well.”***

***– Tiago Wegner,  
IT Infrastructure Coordinator,  
SICREDI Credit Union***

## Other Key Benefits:

Executive-level reporting that provides a security overview

Ability to prioritize patches to meet project schedules and business objectives

Guidance on remediation

Ability to guarantee security of end devices

Automated notification when problems occur

Streamlined incident response



eEye Digital Security®

To learn more, please visit [www.eeye.com](http://www.eeye.com)  
or call 866.282.8276



## Adopting a Security Mindset

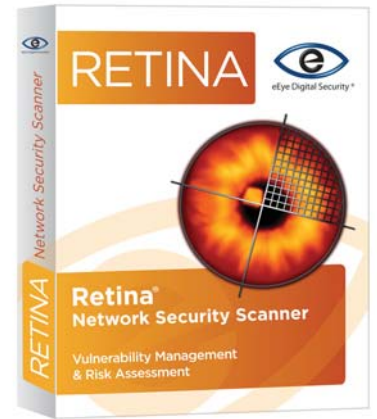
“Retina gave us the ‘big picture’ right from the start,” said Dreher.

What does the environment look like? Which devices have vulnerabilities? Which machines are out of date? Which risks will lead to immediate threats? Retina delivers all of that data. Now, with this information in hand, SICREDI is establishing security best practices.

For starters, Retina Enterprise delivers a report of the most serious risks twice a month. As part of their normal workflow, IT now regularly addresses those risks.

“Having these tools has helped us change how we think about security,” Dreher said. SICREDI is in the process of establishing specific security goals and milestones, and Retina Enterprise enables them to set time-sensitive, concrete ones.

“We’re adopting a security mindset in our IT team,” he continued. “With Retina Enterprise reports in hand, we can point to specific vulnerabilities and explain just how costly those vulnerabilities could be if exploited by hackers. We can say to our board, ‘we’ll face significant losses if we don’t act now,’ and we’re able to back up that assertion in detail.”



## eEye’s Integrated Threat Management Suite:

**Retina Network Security Scanner** provides multi-platform vulnerability management.

Retina identifies known and zero-day vulnerabilities and provides security risk assessment, enabling security best practices, policy enforcement, and compliance with regulatory audits.

**Retina Web Security Scanner** rapidly and accurately scans large, complex web sites and web applications to tackle web-based vulnerabilities, ensuring privacy, security integrity and compliance.

**Blink** delivers multi-layered endpoint protection in a single, lightweight client that replaces multiple security agents, protecting against known exploits, zero-day attacks, and all other attack vectors.

**Retina On Demand** simplifies the entire vulnerability management process by allowing an organization to rapidly deploy Retina Security Management Appliances within an environment and manage all of the job scheduling, reports, and results through a hosted version of Retina Enterprise. There is no need to setup servers, configure databases, or even install any software to benefit from Retina On Demand. eEye has created true black-box technology that can be plugged into any environment and managed via the Internet for a hands-free approach to vulnerability management and regulatory compliance.

To learn more, please visit [www.eeye.com](http://www.eeye.com)  
or call 866.282.8276

