COOP places Virtualisation in its Nationwide Network providing one common standard for Secure Operations

Cisco Self-Defending Network delivers powerful firewall, intrusion protection securing operations and customer data and providing real-time response capabilities

EXECUTIVE SUMMARY

Customer Name
COOP

Industry
Retail

Location
Italy

Number of network users
20,000

Challenge
- Combat emerging threats and provide a common standard for operations
- Satisfy new audit and data protection requirements
- Fortify security across all points within a highly distributed retail network

Network Solution
- Cisco Intelligent Retail Network
- Cisco Self-Defending Network design: total protection of VoIP and wireless communications, in-store partner solutions, supply chain data and building control systems

Results
- Greater protection of in-transit and stored data
- Lower cost of ownership and increased efficiency of security operations
- Growth can be accelerated without risk of creating network vulnerabilities
- Cooperatives better equipped to demonstrate compliance, without restricting their ability to implement local IT policy

Challenge

COOP is the largest supermarket and leading provider of food and grocery products in Italy with 56,000 employees spread across 1,394 outlets in 17 regions. The group is focused on improving the shopping experience for its customers and delivering growth. The retailer intends to optimise operational efficiency and store productivity, while also launching new in-store services designed to strengthen the customer relationship. COOP has set itself an ambitious target of opening 90 new stores and increasing revenue by around €2 billion.

COOP INRES plays a fundamental part in this strategic plan. The subsidiary company provides consulting services for co-operatives relating to the planning and design of supermarkets, shopping centres, and hypermarkets.

Gianluca Bigagli, IT and Telecommunications Manager for COOP INRES, describes this transformational role: "We act as a key enabler for the change process. Our role is to understand the requirements of the business and then, taking the best that technology has to offer, suggesting a shared and agile IT infrastructure to deliver those changes."

This new store model uses a Cisco network as a platform to support Cisco® Voice-over-IP and wireless communications, in-store partner solutions (including scales, self-scanning and point-of-sale applications), supply chain data and building control systems.

While this model had helped to accelerate growth, it also highlighted the need for a more coordinated approach to network security. With each co-operative retaining responsibility for its local infrastructure, security was being rolled out at a different pace and in different ways from store to store. For example, some co-operatives focused on securing the network at the edge (in the stores) while others had decided to begin from the core. Back office functions were more concerned with improving disaster recovery. And from a compliance perspective, auditors had even started to ask co-operatives for proof that a robust policy was in place before they would approve financial accounts.

COOP also recognised that the solution would make it easier to ensure compliance with Payment Card Industry Data Security Standards (PCI DSS) by providing end-to-end protection against security vulnerabilities and threats.

"Cisco understood this straight away. Drawing on validated network designs, proven products and built-in Self-Defending intelligence, they developed a solution that built on our existing technology investments."

–Gianluca Bigagli, IT and Telecommunications Manager, COOP INRES

Network Solution

With global threats and cybercrime on the rise and a tightening of data protection requirements, COOP needed to be able to demonstrate protection at all points across its retail network. Key requirements included ensuring that any wireless and cash register vulnerabilities were addressed. The decision to consult with Cisco early on made perfect sense.

Gianluca Bigagli explains: "We use Cisco architecture to run multiple services over the same network. Virtualisation is very important because it allows us to segregate and restrict access for different employees, co-operatives, suppliers and contractors. Cisco understood this straight away. Drawing on validated network designs, proven products and built-in Self-Defending intelligence, they developed a solution that built on our existing technology investments."

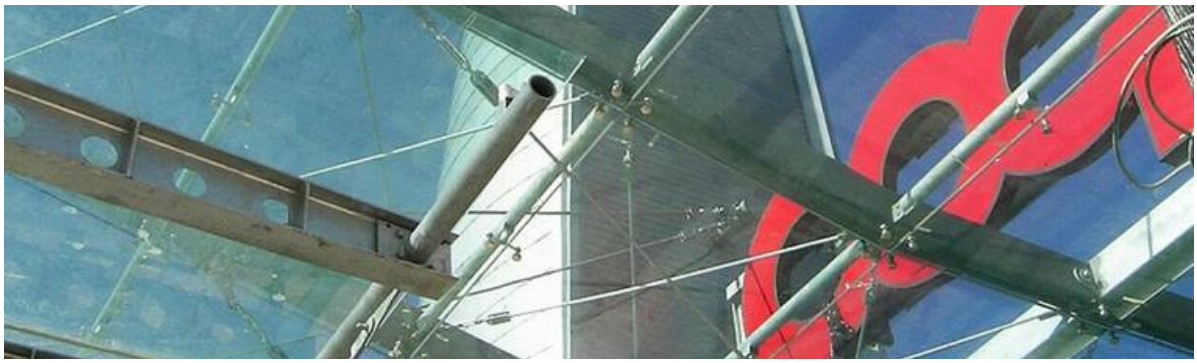
The architecture is based on Cisco's vision of the Intelligent Retail Network – a Self Defending Network approach that enables organisations to identify, prevent and adapt to threats as they occur. This is achieved by providing a common security architecture that is:

- Integrated collaborative: Various network and security components work together to provide new means of protection
- Adaptive: Innovative behavioural methods automatically recognise and adapt to new types of threats as they arise.

These architectural designs are proven and tested in Cisco labs, including a final evaluation from external PCI auditors. The resulting Intelligent Retail Network includes built-in security capabilities and specific intelligence needed to help ensure compliance with forthcoming PCI requirements.

Future plans include introducing the deep-packet inspection features and intelligence provided by Cisco IOS Intrusion Prevention System (IPS) to identify, classify and stop or block suspicious traffic. The solution combines Cisco ASA 5500 Series Adaptive Security Appliances with Cisco Security Monitoring, Analysis and Response System (Cisco Security MARS) for real-time monitor and control capabilities that identify, isolate and recommend precise removal of offending elements.

In order to validate its project investment, COOP undertook a Security Posture Assessment to ensure post-implementation assurance that any previous risks and points of exposure within network devices, servers, desktops, web applications and databases had been successfully strengthened.



> **"With such a federated network, any attempt to dictate security policy would have been totally unworkable. Cisco's flexible approach helped us to drive the project forward and develop a truly homogenous security solution. Realising this part of our strategy was absolutely crucial to success."**
>
> **–Gianluca Bigagli, IT and Telecommunications Manager, COOP INRES**

Business Results

The Cisco Intelligent Retail Network solution has enabled COOP to enforce security best practices, protect brand image and assets, and mitigate financial risk due to downtime or non-compliance fines and penalties. Security embedded in each component – rather than as a point solution or single device – has helped to significantly reduce these risks and the potential for data security breaches at nine of its largest co-operatives. The Cisco solution provides full availability for in-store services, including voice and checkout transaction, in a completely efficient and secure way.

The solution also allows co-operatives to tap into shared security resources without restricting their ability to implement local IT policy. Gianluca Bigagli says: "With such a federated network, any attempt to dictate security policy would have been totally unworkable. Cisco's flexible approach helped us to drive the project forward and develop a truly homogenous security solution. Realising this part of our strategy was absolutely crucial to success."

Consolidation and centralisation of day-to-day security operations are now more efficient. Also, the ability to run multiple services over a single converged IP network has increased overall business agility. It means that COOP can accelerate growth without worrying about increasing network vulnerability. For example, the Cisco solution would make it easier in the future to integrate video surveillance (CCTV is currently being run via proprietary protocols and separate networks). End-to-end security also opens up new opportunities to centralise control of common applications that are shared between multiple co-operatives.

Technical Blueprint

The Cisco Self-Defending Network combines best product in its category technologies to address emerging and pervasive threats. This comprehensive systems approach to information security encompasses:

- **Network and endpoint security**: integrating firewall, VPN, IPS and other security services into network devices and endpoints to create an integrated, adaptive and collaborative defence system.
- **Content security**: extending network defences beyond the traditional network perimeter to protect data in motion, incorporating e-mail, Web interactions, instant messaging systems and other applications.
- **Application security**: protects applications and data, providing XML and HTML inspection capabilities and fine-grained application control.
- **System management and control**: using sophisticated policy, identity and reputation services with powerful enforcement capabilities to unify disparate network, endpoint, content and application security services.

Product List

Security and VPN

- Cisco IOS Intrusion Prevention System
- Cisco Security Monitoring, Analysis and Response System
- Cisco ASA 5500 Series Adaptive Security Appliances

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in the UK ES/11088/0409