

Cisco Securely Connects the Rio 2016 Olympics to the World



EXECUTIVE SUMMARY

Customer: Rio Summer Olympics 2016

Size: 1,000+ Employees

Industry: Sporting Event

Location: Rio de Janeiro, Brazil

“Cisco provided us with the connectivity and security that allowed Rio 2016 to connect with the world.”

Marcelo Souza

Technology Systems General Manager of the Rio 2016 Organizing Committee for the Olympic Games

All roads to the Olympics start with a dream. For the over 15,000 Olympic and Paralympic athletes from 205 countries who congregated in Rio de Janeiro in 2016, it's the dream of competing at the highest level possible. It's also about standing on the podium wearing a gold medal while their country's flag rises and the national anthem plays. For Cisco, as a proud supporter of the 2016 Olympic and Paralympic Games in Rio, it also starts with a dream: that when we securely connect everything, anything is possible.

Supporting a global event of this size is a monumental task that demands a network like no other. The Rio 2016 Games required connectivity, bandwidth, security, and support for:

- 37 competition venues
- More than 100 support venues
- 15,000 athletes
- 70,000 volunteers
- 9 million ticketholders
- 25,000 media personnel
- 123 network broadcasters from around the world

All this while delivering 170,000 hours of video content and providing infrastructure for 5 billion TV viewers – up from 4 billion viewers for the London Olympics in 2012. In short, if this network were competing in the Olympics, it would break world records.

At the Rio 2016 Olympic Games, Cisco:



Blocked an average of 23,000 suspicious sites daily using Cisco Umbrella



Delivered a secure network that handled over 2.144 PB of traffic



Provided secure access for attendees, staff, media, and athletes across 37 competition venues

However, simply providing the infrastructure wasn't enough. Cisco also had to provide effective security.

"The challenge we faced at Rio 2016 was making memorable Games, and one crucial aspect was to provide uninterrupted connectivity to our athletes, guests, media, and critical systems, all while keeping everything secure," said Marcelo Souza, Technology Systems General Manager of the Rio 2016 Organizing Committee for the Olympic Games. "We needed a vendor that could handle the traffic demands in a complex environment and deliver the security needed for such a monumental event."

Comparisons don't come easy when we talk about a world stage event such as the Olympic Games. Securely connecting the Games required 60 tons of equipment and more than 60,000 hours of work. As the official networking and enterprise server supporter and supplier, Cisco deployed over 5,000 access points (a 400 percent increase from the London 2012 Games) and over 113,000 local area network (LAN) ports. Cisco also supplied 440 Cisco Unified Computing System™ (Cisco UCS®) servers, 480 vehicle routers, and 177 security devices. In addition, the Cisco network protected core activities such as accreditation, volunteers, sports entries and qualifications, and workforce management.

The network connected 183,044 unique devices of which 168,158 were wireless (92 percent of all devices). Cisco Identity Services Engine (ISE) and Cisco TrustSec technology were used to identify devices and segment accordingly. Any unrecognized device would connect to the guest network. Network traffic was extremely heavy – 2.144 petabytes of traffic over the course of the Games. To put that into perspective, it's equivalent to 950,000 hours of HD video, which would take more than 110 years of nonstop streaming to watch.

As a highly visible target for sophisticated threats from around the world, the Rio 2016 Games demanded a security architecture that is fundamentally integrated into the network. Cisco Talos, an industry-leading threat intelligence organization, reviewed the sheer number of threats mitigated on the network. During the first two weeks of the Games, there were 674 times the number of Trojans detected on the network compared to a typical large retail corporate environment during the same time.

"The network had to handle a substantially larger number of BYOD (Bring Your Own Device) technology than you would commonly see in a corporate environment. A larger percentage of these devices were infected with Trojans and various other malware families. This goes to show how important it is to have proper checks in place for corporate devices from both an external and internal network perspective," said JJ Cummings of Cisco Talos.

As the first line of defense, Cisco Umbrella (formerly OpenDNS) was deployed to prevent access to malicious sites. Umbrella found and blocked hundreds of Olympic-related fake domains. Over the course of the Rio 2016 Games, it protected on average 22 million DNS requests and blocked 23,000 suspicious sites daily.

For More Information

cisco.com/go/security

At the network edge, Cisco Firepower Next- Generation Firewall and Next- Generation Intrusion Prevention System appliances prevented close to 7 million security events during the Games. On the network, millions of devices were monitored for anomalous activity through Cisco Stealthwatch, and potentially vulnerable endpoints were identified and automatically segmented away from the rest of the network using Cisco ISE and Cisco TrustSec technology.

“The result was an amazing experience for everyone in Rio. Cisco provided us with the connectivity and security that allowed Rio 2016 to connect with the world,” remarked Souza.

In a span of just 40 days, Cisco successfully secured and connected key networks that made the Olympic and Paralympic Games a resounding success. From London to Rio, to Tokyo and beyond, there has never been a better time to build an Olympic legacy.

Products and Services

Cisco ASA 5500-X with FirePOWER Services

Cisco FirePOWER Services in use:

- Cisco Advanced Malware Protection (AMP) for Networks
- URL filtering
- Application Visibility and Control (AVC)
- Next-Generation IPS

Cisco FirePOWER Next-Generation Intrusion Prevention System

Cisco Security Manager

Cisco Identity Services Engine

Cisco TrustSec Technology

Cisco Secure Access Control System

Cisco Stealthwatch

Cisco Umbrella

Cisco Prime Network Registrar



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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)