CISCO STEALTHWATCH CASE STUDY

Orange PLC Utilizes Stealthwatch to Detect Threats in Encrypted Traffic.

Introduction

This case study of Orange PLC is based on an August 2019 survey of Cisco Stealthwatch customers by TechValidate, a 3rd-party research service.

> "Stealthwatch is a must-have component of our security posture."

Challenges

The business challenges that led Orange PLC to evaluate and ultimately select Cisco Stealthwatch:

- A lack of visibility into a complex network with branches, IoT devices, remote employees and guests, cloud infrastructure, etc.
- A lack of a threat investigation and forensic analysis tool
- Protecting sensitive data
- Detection of insider threats
- Analyzing encrypted traffic without decryption
- Real-time malware detection
- Compliance requirements
- Creating and enforcing segmentation policies

Major security concerns related to cloud infrastructure are:

- Unauthorized access
- Data loss

Use Case

Orange PLC chose Stealthwatch for its:

- Comprehensive visibility
- Advanced security analytics using machine learning and entity modeling
- Ability to analyze encrypted traffic without decryption
- WAN traffic visibility

Results

Utilizing Cisco Stealthwatch, Orange PLC was able to:

- Detect and prioritize advanced malicious attacks and insider threats in real-time
- Provide visibility into what devices, users and applications are using the network
- Detect malware in encrypted traffic without decryption

Company Profile

Company:
Orange PLC

Company Size:
Large Enterprise

Industry:
Telecommunications Services

About Cisco Secure Network Analytics

With Cisco Stealthwatch, organizations can improve both network security and performance, and avoid the high costs associated with downtime, security breaches and other issues.

Learn More:

Cisco

Cisco Secure Network Analytics

Source: Manish Sharma, Network Operations, Orange PLC

Validated Published: Sep. 20, 2019 TVID: 4C3-9A2-F02

Research by TechValidate by SurveyMonkey