ALGOSYSTEMS
THE PATH FORWARD

Cisco and Algosystems

Security Case Studies

CISCO
Gold
Partner

INTRODUCTION

Disruptors now harness the power of digital to create new sources of value that reduce costs, improve the customer experience and scale their offerings. Digital disruptors also enjoy a decided innovation advantage over established companies: they are better able to identify new opportunities and move faster to take advantage of them.

In this intensely competitive environment, startups and agile firms are overturning incumbents with digital business models, products, and services. All companies are being pulled toward the center of a "Digital Vortex," which is characterized by exponential change and the blurring of industry lines. Companies must adapt, or their odds of being displaced - or even put out of business altogether - markedly increase.

Digital transformation requires a strong cybersecurity foundation. With this foundation, companies will have the confidence to implement digital processes and technologies that fuel innovation and growth. Without it, companies may hesitate to start digital projects-stifling their innovation potential and opening the door to digital disruptors.

Algosystems owns the expertise, experience and pre and after sales resources to fully support your secure journey to digital transformation. In the following pages, you may enjoy some of our latest Cisco security case studies, to find some inspiration for your next security project.

cisco

CISCO SECURITY SOLUTIONS

Own your security - don't let the hackers own you.

Cyber attacks are big business and only getting bigger.
Effective security helps protect you against a breach’s far-reaching effects.

Lost business

If customers lose trust and stop doing business, it can cost millions in revenue plus lost opportunities to gather market data.

Lost assets

Stolen intellectual property and confidential business information represent huge losses of investment and competitive advantage.

Lost productivity

On average, an attack takes 10 weeks to contain after it’s discovered - time lost for working on other business initiatives.

Fines, litigation and regulation

The money and time spent on settling sanctions and lawsuits damages shareholder value and discourages innovation.

Remediation costs

A single ransomware campaign cost consumers and companies $60 million.

Read what we've learned about the real threat landscape.

www.cisco.com/go/security

ELLAKTOR

CREATING A SECURITY MODEL

Ellaktor Group of Companies

ABOUT THE ORGANIZATION

Ellaktor Group of Companies is an international holding group based in Greece with long-term investments in key fields, including construction, environment and participation in concession projects, with more than 60 years of experience and expertise in complex and demanding projects.

With presence in 22 countries and 13.900 colleagues in Greece and abroad it is placed among the leading groups in construction and infrastructure management in South Eastern Europe and the Middle East.

ORIGINAL CHALLENGE

Ellaktor Group of Companies chose a Cisco Security Solution to complement its Cisco infrastructure. The original need was to control the internal network due to the nature of the employees' work, that force them to perform numerous and long term business travels.

Ellaktor's Group of Companies IT department was seeking for the transparency and control of its services and the internet access offered to the employees and guests. Its main target was to implement the above by permitting or prohibiting the access to precise services or applications.

THE DEPLOYMENT

The two existing ASA firewalls were upgraded to Firepower services. Intrusion Prevention System and Advance Malware Protection licenses were installed on the devices to maximize the user protection.

Cisco Security Architecture was combined with the superior transparency, contextual awareness and management control offered by the Cisco Identity Services Engine (ISE).

RESULTS

Persistent threat protection, fully integrated advanced malware protection, reduced complexity and centralized management improved availability and reliability, eased the daily routine of the IT staff, increased productivity - and resulted in an integrated scalable security infrastructure with minimum risks.

By implementing Cisco ISE, Ellaktor Group of Companies network visibility and control was further strengthened with the use of 802.1x port authentication capability for wired access and wireless access for mobile devices.

Access for Remote users is performed using Cisco's latest Anyconnect VPN Client Application for all operating systems.

WHY ALGOSYSTEMS

Algosystems has the expertise and the know-how to implement such demanding projects. Algosystems' personnel has participated in a variety of different deployments which helps better evaluate a situation, find the weak points in any infrastructure and secure them.

> The Cisco Security solution gives us visibility and control of the user that is trying to access our network, wired or wireless.

Fragiskos Morfonios
Head of IT Infrastructure & Operations
Ellaktor Group of Companies

MITIGATING SECURITY BREACHES WITH CISCO SECURITY ARCHITECTURE

Aegean Motorway

ABOUT THE ORGANIZATION

Aegean Motorway Concession Company for PATHE Motorway, Maliakos - Kleidi section was established in Larissa, Greece. The exclusive purpose of the Company is to carry out the design, construction, financing, operation, maintenance and exploitation of the Maliakos - Kleidi Motorway along with all supplementary works and relevant activities.

ORIGINAL CHALLENGE

Based in Larissa and with a large spread of users across its infrastructure, Aegean Motorway knew that it could not afford disruptions to its network. IT staff wanted to strengthen network security against increasing infections and attacks and at the same time, to simplify security management and monitoring for a limited number of staff.

"It is not sufficient to strengthen the external perimeter. You also need to strengthen the internal one, as a malicious action may originate from within', said Mr. Kiorpelidis, the S & IT Manager.

THE DEPLOYMENT

Two ASA5525 devices with Firepower Services were implemented to the customer's network, replacing the old ASA equipment and integrating the customer's security infrastructure.

Intrusion Prevention System, Advance Malware Protection and URL filtering licenses were installed on the devices, maximizing user protection. Access for Remote users is performed using Cisco's latest Anyconnect VPN Client Application for all operating systems.

Cisco ESA with Antispam, Antivirus and Outbreak filter was installed to keep critical business email safe from spam, malware, and other threat.

RESULTS

Consistent threat protection, fully integrated advanced malware protection, reduced complexity and centralized management improved availability and reliability, eased the daily routine of the IT staff, increased productivity and resulted in an integrated scalable security infrastructure with minimum risks.

With the E-mail Security Appliance, Aegean Motorway has control over its e-mail, encrypting sensitive outbound e-mail whilst at the same time blocking incoming attacks with its layered defense while the company has all these features built into a single appliance.

WHY ALGOSYSTEMS

Aegean Motorway IT staff credits Algosystems customer support as one of the main factors in implementing their Cisco security solution with us.

"The 30 years of experience and the multiple Cisco Security projects implemented and supported by Algosystems made us feel confident to rely on them for the success of our Security Architecture Project', said Mr. Kiorpelidis, the S & IT Manager.

> We have accomplished what we aimed to do. We have got a Cisco unified platform, great service and the security to deliver a higher level of service.

Charalampos Kiorpelidis
S & IT Manager, Aegean Motorway S.A.

SAIT COMMUNICATIONS
A SpeedCast Group Company

PROVIDING NEXT-GENERATION SECURITY

SAIT COMMUNICATIONS (A SpeedCast Group Company)

ABOUT THE ORGANIZATION

SAIT COMMUNICATIONS, a member of the Speedcast Group, is a well-established company in the maritime market for many years, offering full services concerning satellite telecommunications provisioning, ISP and support services as well as sales for a wide range of SatComs Solutions.

The company utilizes a proprietary developed solution combining embedded systems, cutting edge infrastructure, virtualization and a wide toolset of value added solutions, creating the unique Sigma Base Solution.

SAIT COMMUNICATIONS is located in Piraeus, Greece, and in Limassol, Cyprus, operating in the heart of the Mediterranean maritime activities offering its full portfolio of services and products in more than 60 countries.

ORIGINAL CHALLENGE

The aim was to create an Inmarsat enabled Data Center (DC) and Point of Presence (PoP) maintaining close to a hundred percent network availability in order to deliver Internet services and connectivity to maritime vessels. The solution had to be centrally managed and in the same time had to maintain state of the art security offerings to end customers. All the previous targets had to be achieved by utilizing a simplified and fully programmable approach into a single platform with limited ICT staff resources.

WHY CISCO

With Cisco, there's never a better time to know what's happening in our entire network. There's never a better time to be protected as the threats are stopped before, during and after the attacks. We can automate security, even after attacks, across physical, virtual and cloud to reduce complexity and quickly remediate attacks.

THE DEPLOYMENT

A cluster of ASA-X Next Generation Firewalls with Firepower Services in combination with quad ASR4K routers were deployed to the Data Center providing unparalleled resilience, availability and scalability to the DC itself and to the end customers' services.

At the same time, costs dropped drastically by simplification in operations, management and support services along with the streamlined integration with existing systems onto company's existing infrastructure. Intrusion Prevention, Advance Malware Protection and URL filtering licenses were installed on the devices in order to maximize the user protection while providing thorough complete reporting capabilities.

All the previous, led to a complete and rigid security infrastructure offering impressive security services while keeping CAPEX and most importantly OPEX low.

RESULTS

The solution provided a simplified and API-based, centralized management available to the involved staff while maintaining low headcount for operations. This results to state of the art services, availability and reliability of the networking services as well as robust scalability to meet future needs.

> “We have achieved all of our targets. With ASA-X Next Generation Firewalls we have a complete and rigid security infrastructure with unparallel resilience, availability and scalability.”

George Venianakis, CCIE™ #8418
Chief Technology Officer, SAIT COMMUNICATIONS

OLYMPIC
BREWERY S.A.

ONE SECURE NETWORK FOR ALL SITES

ABOUT THE ORGANIZATION

Olympic Brewery S.A. is a fast evolving Greek company that was set up in January 2010. At the same time, it is considered a healthy Greek business overseas too, since it exports its beer to several dynamic international markets. The company uses multiple sites for its operations. Two of those are production factories.

ORIGINAL CHALLENGE

The Olympic Brewery IT staff wanted to have an integrated, threat-centric next-generation firewall. One that not only delivers granular application control, but also provides effective security against the threats posed by sophisticated and evasive malware attacks.

WHY CISCO

Olympic Brewery, a longtime Cisco customer, is investing in a more end-to-end Cisco solution model. From the core to the access layer and from routing and switching to the internal and perimeter security of their network. "When we are looking to purchase new infrastructure, we are wondering whether it is Reliable, Scalable and Highly available. With Cisco, the answer has always been yes." says Mr. Levantis.

Cisco Firepower NGFW appliances combine network firewall with the industry's most effective next-gen IPS and Advanced Malware Protection. They provide multiple deployment options and integrate easily into the datacenter and the network. Actionable security events that will be identified as threats, are blocked before they can disrupt any datacenter services.

THE DEPLOYMENT

Properly sized ASA firewall devices with FirePOWER Services were deployed in the perimeter and in all the entry points of the company's network throughout its sites. These systems replaced the old ASA devices and others and provided a uniform security infrastructure.

Access for Remote users is performed using Cisco's latest Anyconnect VPN Client Application for all operating systems. Intrusion Protection, Advance Malware Protection and URL filtering services were activated on all devices to maximize the protection of the systems and the users of the company.

RESULTS

Datacenter footprint was reduced, security management and operations were simplified with room for future growth. We reduced Complexity and simplified our operations by consolidating all security functions into a single management interface.

WHY ALGOSYSTEMS

Algosystems is Olympic Brewery's trusted advisor for many years. Our longtime cooperation is based on Algosystems' experience in proposing the latest technological features that apply to our needs and implementing and supporting demanding projects.

> “With the Cisco Firepower NGFW appliances installed in all of our sites, we have reduced complexity of our security infrastructure and we are focused on the most critical events.”

Panos Levantis
IT Manager, Olympic Brewery

Algosystems S.A.
206 Syggrou Ave., Athens, Greece 176 72
Tel: +30 (210) 954 - 8000, Fax: +30 (210) 954 - 8099
www.algosystems.gr

FOLLOW US

f in You Tube