Customer Story

Unión de Créditos Inmobiliarios Strengthens NIS2 Compliance

Unión de Créditos Inmobiliarios (UCI), a leading mortgage lender in Spain, has trusted Forcepoint since 2016. After years of success with Forcepoint Next-Generation Firewall (NGFW), UCI is expanding its cybersecurity posture to achieve full compliance with the EU's NIS2 Directive. NGFW remains the cornerstone of this effort, delivering advanced protection, centralized control, and regulatory alignment across UCI's distributed environment.

Challenge

Centralize IT management and reduce cyber threats

UCI needed to consolidate security operations across a distributed environment to eliminate manual processes, reduce on-site maintenance, and gain real-time visibility into network health. This was critical for reducing exposure to advanced cyber threats and ensuring consistent policy enforcement across all locations.

Achieve and maintain full compliance with the NIS2 Directive

The NIS2 Directive introduced stricter requirements for risk management, incident detection and reporting, and operational resilience. UCI faced the challenge of aligning its security posture with these mandates, which includes implementing governance controls, ensuring high availability, and avoiding costly regulatory fines or failed audits without disrupting user productivity.

Customer Profile:

- Unión de Créditos Inmobiliarios is a leader in marketing mortgage loans through professionals in the property sector. UCI provides professionals with a unique financial offer, in accordance with market demand to create credit facilities at the right time, allowing customers to arrange the purchase of property and the financing means with the same provider.

Industry:

- Finance (non-banking)

HQ Country:

- Spain

Product(s):

- **Forcepoint NGFW**

Approach

Expanded deployment of Forcepoint Next-Generation Firewall (NGFW) to strengthen security controls across all sites

Unlocked advanced NGFW functionality to meet NIS2 requirements for risk management, detection, and resilience

Rolled out new security policies aligned with NIS2 mandates, including centralized governance and incident response readiness

Leveraged NGFW's compliance-focused capabilities such as intrusion prevention, deep packet inspection, and high availability to ensure uninterrupted operations and regulatory alignment

Results

Reduced travel and maintenance costs
By centralizing policy management through Forcepoint NGFW, UCI eliminated the need for on-site visits and manual updates. This not only cut operational expenses but also ensured **continuous policy enforcement without disrupting users**, a critical factor for maintaining NIS2 compliance across distributed environments.

Continuous policy enforcement without user disruption NGFW's centralized control and automated updates guarantee that security policies remain consistent and up to date, supporting NIS2's requirements for governance and resilience without impacting productivity.

Full NIS2 compliance and readiness for future regulatory changes

Finding a True Security Partner

Before partnering with Forcepoint, UCI faced significant exposure to cyber threats and found that previous vendors, including Microsoft, fell short in meeting their needs.

Forcepoint's reputation for protecting data and users made it the clear choice. NGFW became a foundational layer of UCI's security posture, helping reduce travel costs and maintenance hours while providing centralized policy management and real-time network health visibility.

> "Forcepoint Next-Generation Firewall is an excellent product, with continuous improvements, and it's easily applicable. It covers everything necessary for our company to be strongly secured from undesirable external agents."
>
> **JOSÉ ANTONIO BORREGUERO** DIRECTOR DE TECNOLOGÍA, INFRAESTRUCTURAS Y SERVICIOS

Securing NIS2 Compliance

The NIS2 Directive introduces stricter requirements for cybersecurity risk management, incident reporting, and operational resilience. For UCI, this meant ensuring:

- → **Robust risk management and threat prevention**
- → **Centralized visibility and control across distributed environments**
- → **High availability to maintain business continuity**
- → **Incident detection and response capabilities** to meet reporting obligations

To achieve these requirements and avoid penalties for non-compliance, UCI relies on Forcepoint Next-Generation Firewall (NGFW) as its primary defense. Forcepoint NGFW delivers features that directly align with NIS2 obligations:

- → **Advanced intrusion prevention and deep packet inspection** Helps UCI detect and block sophisticated attacks, supporting NIS2's mandate for proactive risk management and threat mitigation.
- → **Centralized policy management for distributed environments**
- → **High availability and reliability** Guarantees uninterrupted operations, reducing the risk of downtime that could lead to compliance breaches or fines.

(By partnering with Forcepoint, UCI avoids costly regulatory fines, reputational damage, and the operational burden of failed audits, while maintaining a strong security posture that meets evolving EU standards.)

> **"Given that NIS2 has a direct impact on the UCI Group and that the Directive enhances cybersecurity protection, detection, response, and resilience to cyberattacks, there is no doubt that having a market-leading solution will help UCI to minimize risks in a highly volatile environment."**
>
> **JOSÉ ANTONIO BORREGUERO** DIRECTOR DE TECNOLOGÍA, INFRAESTRUCTURAS Y SERVICIOS

Audit-ready Network Security

UCI plans to extend NGFW deployment across its infrastructure to protect 1,200+ users. With enhanced visibility and unified control, and proven compliance support, UCI is well-positioned to minimize risk, maintain resilience, and stay ahead of future regulatory requirements.