SOLUTION BRIEF

NIS2 Compliance

Transform Your Digital Resilience Journey with NIS2

Problem

Organizations across the European Union face an unprecedented challenge with the implementation of the NIS2 Directive. This enhanced cybersecurity framework significantly expands both the scope of affected entities and the depth of compliance requirements, creating urgent operational and strategic imperatives for businesses. The directive introduces stricter supervisory measures, enforcement requirements, and heavier sanctions.

Organizations must now navigate complex new obligations across risk management, incident reporting, supply chain security, governance, and information sharing. Many entities are struggling to understand their classification status, assess their current security posture against the new requirements, and determine what changes are needed to their existing cybersecurity programs. The expanded scope means thousands of additional companies must now comply, including many that have never been subject to such comprehensive cybersecurity regulations. The challenge is particularly acute given the need to coordinate across multiple internal stakeholders and external suppliers, and the significant operational and technical capabilities required. Without proper preparation and expert guidance, organizations risk substantial penalties, reputational damage, and business disruption.

2% fine of global turn over due to noncompliance[1]

67% personally liable if gross negligence is found[2]

Key Takeaways

- **Risk Visibility.** Get unprecedented visibility into human risk within your organization, compiled based on user behavior and real-world threats.
- **Adaptive actions.** Tackle unsafe behaviors with timely feedback and engaging training, delivered to those who need it, when they need it.
- **Proactive controls.** Mitigate human risk across your security landscape by proactively adjusting security controls to better protect users.

Solution

Today's organizations face increasing pressure to meet NIS2 Directive requirements while maintaining operational efficiency and strengthening their security posture. Mimecast delivers an integrated security platform that addresses all seven critical areas of NIS2 compliance through a unified, easy-to-manage approach. Our comprehensive solution combines robust policy controls and advanced incident management capabilities that enable rapid threat detection and response. We ensure business continuity through reliable email security solutions while providing the supply chain security controls needed to manage third-party risks effectively. Through engaging security awareness training, we transform employees from a potential vulnerability into a powerful line of defense. Our platform enables continuous security testing and auditing to validate control effectiveness, while enterprise-grade encryption protects sensitive data wherever it travels.

1 https://nis2directive.eu/nis2-fines/

2 https://www.dlapiper.com/en-us/insights/publications/derisk-newsletter/2024/nis2-directors-personal-liability-for-lack-of-compliance-is-a-warning-message

This integrated approach not only simplifies NIS2 compliance but delivers measurable value by reducing risk, strengthening security, and enabling secure, uninterrupted business operations. By partnering with Mimecast, organizations gain more than technology - they gain a trusted advisor committed to protecting their communications, data, and operations against evolving cyber threats while ensuring compliance with NIS2 requirements.

NIS2 Compliance Made Simple: The Mimecast Advantage

The NIS2 Directive strengthens the EU's cybersecurity landscape through seven essential pillars that work together to create a comprehensive defense against modern cyber threats. These interconnected pillars establish a robust security framework that encompasses risk analysis and system security policies, incident management protocols, business continuity measures, supply chain controls, comprehensive awareness training, regular security testing and audits, and strong cryptographic protections. By implementing these seven foundational elements, organizations can build lasting cyber resilience while meeting enhanced compliance requirements, ultimately protecting their critical assets and operations from evolving digital threats.

Through our integrated security platform, Mimecast delivers comprehensive protection across all seven NIS2 pillars, transforming regulatory requirements into practical security advantages that protect your organization's communications, strengthen compliance, and build lasting cyber resilience.

Policy

NIS2 mandates comprehensive security controls for email systems, requiring organizations to implement encryption, secure authentication mechanisms, and advanced threat protection. Especially in relation to protecting critical systems which may be infiltrated via an email attack. Organizations must deploy multi-layered email security measures which include continuous security assessment capabilities to protect against evolving email threats such as phishing and business email compromise attacks.

Incydr delivers comprehensive data protection and risk management capabilities that align with NIS2's requirements. Through real-time monitoring and advanced threat detection, Incydr provides continuous visibility into data movements across your digital environment, helping you identify and respond to potential risks before they escalate into serious incidents.

Incident Response

Mimecast's comprehensive incident response capabilities deliver robust security and compliance features your organization needs to meet NIS2 requirements. Our integrated solution suite includes Analysis and Response, Internal Email Protect, and Mimecast Email Incident Response (MEIR), providing continuous threat monitoring and rapid remediation across your email channels. MEIR streamlines your security operations by combining automated triaging with expert human validation, significantly reducing the workload on your security teams while maintaining accuracy. Through seamless integration with orchestration platforms, we automate response workflows for threat removal, policy updates, and documentation, ensuring consistent and efficient threat management.

By delivering comprehensive visibility into data movement and potential threats, Incydr helps you meet the directive's stringent incident reporting requirements. Our integrated case management system simplifies compliance by consolidating security functions that traditionally require multiple tools, allowing your security team to focus on strategic initiatives rather than managing complex reporting processes.

Business Continuity & Crisis Management

Continuity guarantees uninterrupted communication access during both planned and unplanned outages. Supported by geographically dispersed data centers and backed by a 100% service availability SLA. Sync and Recover enables swift operational restoration following accidental data loss or malicious actions. This specifically addresses email-based threats like ransomware, offering rapid, granular recovery of mailboxes, calendars, and tasks, with configurable retention policies.

Supply Chain

Advanced Business Email Compromise (BEC) protection serves as your critical defense against sophisticated supply chain attacks, leveraging machine learning and natural language processing to analyze communication patterns and block fraudulent activities before they impact your business operations. We strengthen this protection through Transport Layer Security (TLS) encryption and DNS-based Authentication of Named Entities (DANE), ensuring your email transmissions remain secure and authenticated throughout their journey.

Training

Mimecast Engage transforms potential security vulnerabilities into organizational strengths through targeted training and risk scoring. The Human Risk Management capabilities provide detailed insights into employee behaviors and risk profiles encompassing your security tools, delivering customized security awareness training that adapts to emerging threats.

Cryptography

Transport Layer Security (TLS 1.2 and 1.3) provides automatic encryption of your communications in transit. We enhance this protection through DNS-based Authentication of Named Entities (DANE), which leverages DNSSEC to verify email server authenticity and man-in-the-middle attacks. For organizations requiring maximum security, we support PGP and OpenPGP standards with intuitive key management, enabling true end-to-end encryption without burdening your IT team.

Additionally, our tools are designed to support your audit, integrated logging, and threat sharing requirements, enabling organizations to meet and maintain compliance. By partnering with Mimecast, organizations can confidently address NIS2 compliance while enhancing their overall digital operational resilience.

About Mimecast

Mimecast is a leading AI-powered, API-enabled connected Human Risk Management platform, purpose-built to protect organizations from the spectrum of cyber threats. Integrating cutting-edge technology with human-centric pathways, our platform enhances visibility and provides strategic insight that enables decisive action and empowers businesses to protect their collaborative environments, safeguard their critical data and actively engage employees in reducing risk and enhancing productivity. More than 42,000 businesses worldwide trust Mimecast to help them keep ahead of the ever-evolving threat landscape. From insider risk to external threats, with Mimecast customers get more. More visibility. More insight. More agility. More security.