DDI UNCOVERED Solution Overview

efficient iP® *for* NIS 2 Compliance

The NIS 2 Directive enhances Europe's cybersecurity framework by expanding the scope of the original NIS Directive and enforcing stricter security measures. In order to avoid substantial fines for non-compliance, organizations must significantly increase cyber resilience.

DNS, DHCP, and IP Address Management (DDI), along with advanced DNS Security, are critical to provide comprehensive visibility and control across hybrid multicloud environments and protect users, data, and networks against cyber threats, ensuring service availability and data integrity. This aligns with key NIS 2 requirements for risk management, incident handling, business continuity, and transparent reporting, helping organizations achieve NIS 2 compliance.

Solution Benefits

ENHANCED NETWORK VISIBILITY	unified, up-to-date network asset inventory with IPAM as an extensive NSoT for improved risk management
FASTER THREAT DETECTION	key DNS analytics and insights into DNS traffic to identify malicious activity and support incident reporting
ELEVATED SECURITY POSTURE	proactive threat prevention, detection, and automated response for effective incident handling
ENSURED SERVICE AVAILABILITY	highly scalable, reliable DNS and DHCP services and robust DNS Security to sustain business continuity
IMPROVED OPERATIONAL EFFICIENCY	automate network and security workflows to reduce incident response time and gain agility

NIS 2 Context and Overview

In an ever-growing cybersecurity threat landscape, the rapid evolution of digitization has heightened the need for robust cybersecurity measures. According to the latest IDC DNS Threat Report, 90% of organizations have suffered DNS attacks in 2023, with the average cost of a DNS attack estimated at $1.1 million. In this threatening context, the NIS 2 Directive aims to enhance cybersecurity resilience across the European Union (EU) by broadening the scope of cybersecurity requirements, covering a wide range of entities and sectors, and enforcing top management accountability. Businesses must comply with the directive to avoid substantial fines, up to €10 million or 2% of global turnover for essential entities.

The NIS 2 Directive lists cybersecurity measures required, aiming to protect network and information systems and the physical environment of those systems from incidents, including:

- **Risk management and security requirements:** appropriate operational and organizational measures to identify, assess, and mitigate risks posed to the security of networks
- **Incident handling:** actions and procedures aiming to prevent, detect, analyze, and contain or to respond to and recover from an incident
- **Business continuity:** definition and implementation of business continuity plan, including backup management, disaster recovery, and crisis management
- **Reporting and disclosure:** notification within 24 hours of any incident significantly impacting service delivery, including cross-border effects.

How EfficientIP Solutions Help

EfficientIP SOLIDserver™ DDI provides IT teams with scalable, reliable, and high-performance DNS, DHCP, and IPAM (DDI) and DNS Security solutions. This all-in-one platform manages, automates, and secures diverse infrastructures anytime from a unified, consistent interface, enabling global visibility and control, and ensuring robust defense against cyber threats in order to meet compliance with stringent NIS 2 requirements.

At its core, IPAM features an extended Network Source of Truth (NSoT), a comprehensive, central, and unified repository of connected assets including IP-related data as well as VLANs/VxLANs, and metadata across networks for improved visibility. Leveraging IPAM, the SOLIDserver™ DDI platform automates the design, deployment, and management of critical DNS and DHCP services across distributed, multi-vendor, and hybrid multi-cloud environments, simplifying disaster recovery for enhanced service continuity.

EfficientIP's DNS Security, including DNS Guardian, a Protective DNS service, DNS Threat Pulse (DTP), and DNS Intelligence Center (DNS IC), enables security teams to leverage DNS as the first line of defense to effectively safeguard their networks. It helps proactively protect data, users, and applications from a wide range of cyber threats such as phishing, malware, data exfiltration, DDoS, and more. Thanks to AI-driven algorithms, the solution quickly detects malicious DNS activity and effectively responds to DNS-based attacks with adaptive countermeasures and automated remediation.

Key DDI Capabilities for NIS 2 Compliance

ENSURING RISK MANAGEMENT

EfficientIP's IPAM, along with NetChange IPLocator and Cloud Observer, automatically discovers, collects, and reports on network assets across on-premises, public, private, or hybrid multicloud infrastructures, creating a comprehensive inventory of connected assets including VLAN/VXLAN/VRF, applications, and devices that serves as a NSoT crucial for global network visibility, control, and anomaly detection. All changes are tracked and reconciled, ensuring an accurate and up-to-date repository essential for risk assessment.

Implementing EfficientIP's innovative and protective DNS Security provides a first layer of defense to secure DNS and significantly reduce the risk of cyber attacks. This risk is further mitigated when combined with DTP, a groundbreaking, accurate, and up-to-date DNS-centric AI-driven threat intelligence feed, or advanced application access control with Client Query Filtering (CQF), a fine-grained DNS filtering feature that enables micro-segmentation, and high-volume DDoS prevention in DNS Guardian. These capabilities enable organizations to monitor their DNS traffic, efficiently restrict access according to Zero Trust principles, and proactively prevent threats.

HANDLING INCIDENTS EFFECTIVELY

As part of the EfficientIP DNS Security solution, DNS Guardian facilitates real-time threat detection leveraging patented DNS Traffic Inspection (DTI) and behavioral threat analysis. It permits security teams to identify and counteract threats like cache poisoning, DNS tunneling, malware, zero-day DNS attacks, data exfiltration, and command and control.

DNS Guardian also provides patented adaptive countermeasures such as blocking IP addresses or quarantining suspicious devices to significantly mitigate impact. With actionable DNS insights and security event sharing, it seamlessly integrates with the security ecosystem and tools such as SIEM, SOAR, and NAC for automated remediation, helping reduce incident response time.

In addition, DNS IC delivers advanced domain name intelligence and key DNS analytics such as threat matches, available from a cloud-based portal for early threat detection and efficient investigation.

EfficientIP's end-to-end DNS Security solution helps organizations prevent, detect, and respond to incidents quickly and effectively.

MAINTAINING BUSINESS CONTINUITY

Thanks to adaptive countermeasures and recovery innovations such as Rescue Mode, EfficientIP's DNS Guardian ensures the reliability and availability of DNS services in the face of threats, even from unidentifiable attack sources.

Leveraging SmartArchitecture™, a library of state-of-the-art, policy-driven templates for DNS and DHCP architectures, SOLIDserver™ DDI helps quickly restore service operations in disaster cases across distributed multi-vendor DNS and DHCP environments. Edge DNS Global Server Load Balancing (GSLB), enhancing application traffic distribution by optimizing routing at the network edge, also ensures business continuity and disaster recovery through extensive failure detection capabilities and automatic failover across sites. This strengthens DNS resilience and supports business continuity.

ACHIEVING TRANSPARENT REPORTING & DISCLOSURE

DNS Intelligence Center and DDI Observability Center (DDI OC) provide vital DNS insights, key statistics, and analytics through interactive dashboards for efficient, real-time incident investigation and accurate reporting. Push and pull of security events and data with the broader security ecosystem ensures comprehensive threat visibility and contributes to detailed incident reporting.

Key Takeaways

The NIS 2 Directive aims to enhance cyber resilience across Europe by enforcing stringent security measures to safeguard digital infrastructure against increasingly sophisticated attacks.

By embracing EfficientIP's reliable, high-performance, and future-proof DDI and DNS Security solutions, organizations can better manage risk, improve incident handling, ensure business continuity, and achieve transparent reporting to meet key NIS 2 security requirements. They offer a robust framework for network and information system security to increase cyber resilience and protect digital infrastructure while achieving NIS 2 compliance.

efficient iP®

REV: C-240719

As one of the world's fastest growing DDI vendors, EfficientIP helps organizations drive business efficiency through agile, secure and reliable network infrastructures. Our unified management framework for DNS-DHCP-IPAM (DDI) and network configurations ensures end-to-end visibility, consistency control and advanced automation. Additionally, our unique 360° DNS security solution protects data confidentiality and application access from anywhere at any time. Companies rely on us to help control the risks and reduce the complexity of challenges they face with modern key IT initiatives such as cloud applications, virtualization, and mobility. Institutions across a variety of industries and government sectors worldwide rely on our offerings to assure business continuity, reduce operating costs and increase the management efficiency of their network and security teams.

Americas
EfficientIP Inc.
1 South Church Street
West Chester, PA 19382-USA
+1 888-228-4655

Europe
EfficientIP SAS
90 Boulevard National
92250 La Garenne Colombes-FRANCE
+33 1 75 84 88 98

Asia
EfficientIP PTE Ltd
60 Paya Lebar Road #11-47
Paya Lebar Square SINGAPORE 409051
+65 6678 7752