illumio

SOLUTION BRIEF

Implementing NIS Directive with Illumio:

A guide for operators of essential services

Organisations providing essential public services such as electricity, water, healthcare, and transport are of critical importance to society. Due to their pivotal role, they can also be an attractive target for malicious actors. In the last decade we've seen countless cybersecurity incidents on core systems within different business sectors by attackers who are often well-funded or state sponsored.

Incidents affecting any of these systems not only can result in substantial financial losses, but also have the potential to cause huge damage to the economy, underlying infrastructure, and the safety of consumers. The 2016 attacks on U.S. water utilities and the 2015 attack on Ukraine's electricity network clearly highlight the impact that incidents of this nature can have on such sensitive networks.

Secure by Design

With this in mind, the Directive on Network and Information Systems, commonly referred to as the NIS Directive or NIS-D, was formed by European countries to raise the levels of security and resilience of relevant environments. This framework provides operators of essential services (OES) a guideline for securing their systems.

NIS-D specifically calls out that all OES maintain a "secure by design" approach that supports the delivery of essential services through breach preparedness. Attacks and breaches are inevitable, but the more important goal is to prevent further damage by restricting the lateral movement by adversaries.

Breach Preparedness Through Segmentation

Data centres are often designed as large, flat networks to facilitate easy connectivity between systems. Unfortunately, this easy connectivity provides a large attack surface for malicious actors once they compromise the perimeter. Malicious actors typically gain foothold inside data centres through a variety of means such as malware, stolen credentials, default passwords, configuration errors, etc. Once inside the network, they are free to move around and, in many cases, remain hidden for weeks or months as they start moving laterally towards highvalue assets. Segmentation prevents attackers from moving laterally, reducing the attack surface and overall risk by minimising the breach's impact.

In order to comply with the NIS Directive requirements and address this common breach scenario, each EU member state has created a national framework regulated by a local authority. Each framework includes strategy that stipulates certain requirements for areas of focus.

How Can Illumio Help?

Illumio Core™ uniquely protects critical information with real-time application dependency and vulnerability mapping coupled with micro-segmentation that works across any data center, public cloud, or hybrid cloud deployment on bare-metal, virtual machines, and containers. Illumio Core can help operators of essential services reduce cyber risk and achieve the outcomes specified by the principles outlined below.

illumio

Risk Management

Your organisation has effective internal processes for managing risks to the security of network and information systems related to the delivery of essential services and communicating associated activities.

Objective – achieved	How Illumio can help
Your organisational process ensures that security risks to networks and information systems relevant to essential services are identified, analysed, prioritised, and managed.	With real-time visibility into environments afforded by a combination of application inter-connectivity mapping and vulnerability mapping to and from workloads, risk to critical applications can be determined. Management of risk can then be prioritised and mitigated by enforcing segmentation policies at a granular level.
Your risk assessments are informed by an understanding of the vulnerabilities in the networks and information systems supporting your essential service.	Vulnerabilities that exist within workloads can be mapped to applications and environments—providing a view into the real risk posed to critical areas. Vulnerability data can be incorporated directly into Illumio Core, helping inform segmentation policy and security posture. Severity, exposure, and application criticality all feed into a "vulnerability exposure score" that's assigned to a workload, allowing teams to focus on the most critical systems at any given point, and change/apply segmentation policies as required to protect critical infrastructure.
Your risk assessments are dynamic and are updated in the light of relevant changes which may include technical changes to networks and information systems, change of use and new threat information.	Illumio's real-time application dependency map is dynamic, reflecting changes to the connectivity to and from applications as they occur. Combined with regularly synchronised vulnerability data, changes in risk are visible and can subsequently be mitigated.

Data Security

You have a good understanding of data important to the delivery of the essential service, where it is stored, where it travels and how unavailability or unauthorised access, modification or deletion would impact the service. This also applies to third parties storing or accessing data important to the delivery of essential services.

Objective – achieved	How Illumio can help
You maintain a current understanding of the data links used to transmit data that is important to your essential service.	Illumio's real-time application dependency map provides visibility into traffic flow summaries, allowing application owners to understand the data link status; policy is defined to govern them. With the application dependency map, organisations are able to: • Eliminate blind spots inside and across data centre and cloud environments with a comprehensive view of application traffic. • Gain granular visibility into workload relationships with details down to the flow and service level. • Understand application dependencies on common common services (e.g., Active Directory, Exchange, database platforms). • See the vulnerable paths that a bad actor can exploit across environments. • Create optimal segmentation policies in minutes with automated policy recommendations. • Model security policy and receive visual feedback in real time to eliminate risk of breaking applications with new policies. • Pinpoint unauthorised communications and stop them immediately with the ability to quickly quarantine workloads.

Data in Transit

You have protected the transit of data important to the delivery of the essential service. This includes the transfer of data to third parties.

Objective – achieved	How Illumio can help
You have identified and suitably protected all the data links that carry data important to the delivery of the essential service.	Initially using application dependency mapping to map the relevant data links, policy can easily be defined to protect the essential service. Additionally, any new, undefined, or malicious connection attempts are automatically blocked – and alerts can be sent to the SOC via SIEM or related technology.
You apply appropriate physical or technical means to protect data that travels over an untrusted carrier, with justified confidence in the robustness of the protection applied.	Using Illumio's SecureConnect feature, the incumbent host-based firewalls within the relevant workloads can be configured to set up IPsec in transport mode – encrypting all or selected data links as they traverse untrusted environments.

Secure by Design

You design security into the network and information systems that supports the delivery of essential services. You minimise their attack surface and ensure that the delivery of the essential service should not be impacted by the exploitation of any single vulnerability.

Objective – achieved	How Illumio can help
Your networks and information systems are segregated into appropriate security zones, e.g. operational systems for the essential service are segregated in a highly trusted, more secure zone.	Illumio Core makes it incredibly easy to create segmentation policies. From simple application or environment ringfencing to nano-segmentation, it enables only specific process and ports to communicate to allow the services to function.
The networks and information systems supporting your essential service are designed to have simple data flows between components to support effective security monitoring.	Illumio's real-time application dependency map shows all network flows to and from specific workloads, or to and from entire applications, allowing teams to combine documented behaviour with actual, dynamic connectivity as it happens. The application dependency map can be filtered to show only new connections or only those outside of policy, or to remove core data centre services, for example, to show only application traffic.

Secure Configuration

You securely configure the network and information systems that support the delivery of essential services.

Objective – achieved	How Illumio can help
You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented.	Illumio Core adapts to any changes to the environment, maintaining connectivity and protection, even in the event of a workload migrated between data centres or into the cloud. The application dependency map enables the environment to be easily documented.

Secure Management

You manage your organisation's network and information systems that support the delivery of essential services to enable and maintain security.

Objective – achieved	How Illumio can help
You regularly review and update technical knowledge about networks and information systems, such as documentation and network diagrams, and ensure they are securely stored.	Illumio's real-time application dependency map allows for detailed network diagrams and dependencies to be mapped and updated as changes occur—with potential alerts on changes to network traffic as they occur.

Vulnerability Management

You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service.

Objective – achieved	How Illumio can help
You maintain a current understanding of the exposure of your essential service to publicly-known vulnerabilities.	Illumio Core can take in vulnerability data and map it to network port exposure, defining segmentation policies in response to prevent exploitation of vulnerabilities before patches can be applied.

Design for Resilience

You design the network and information systems supporting your essential service to be resilient to cyber security incidents. Systems are appropriately segregated and resource limitations are mitigated.

Objective – achieved	How Illumio can help
Your essential service's operational systems are segregated from other business and external systems by appropriate technical and physical means, e.g. separate network and system infrastructure with independent user administration. Internet services are not accessible from operational systems.	Illumio Core is designed to apply the exact level of enforcement needed for any environment, application, and workload by providing a range of segmentation options enforced at each protected workload. With Illumio, you can separate large environments like production and development with a single rule, microsegment a specific high-value application, define granular policy for control down to the process level, and even encrypt traffic between workloads and environments with a single policy. User administration is full role-based access control (RBAC), allowing separation of duties around policy creation and sign-off, and view/control over only the relevant areas of the environment depending on jurisdiction.
You review and update dependencies, resource and geographical limitation assessments and update mitigations when required.	Illumio's real-time application dependency map provides live insights across environments to help you visualise application dependencies, view how exposed vulnerabilities can be exploited, and automatically recommend policies to reduce the exposure of those vulnerabilities. In addition to being an important cybersecurity tool, the application dependency map is a tightly integrated component of the Illumio Core workflow used to: • Discover how applications are connected and communicating. • View potentially vulnerable workloads and connections. • Build better, more efficient policies without breaking breaking applications. • Confirm enforcement of policy and pinpoint policy violations. • Save critical time, accelerate security workflows, and reduce the risk of errors.

Security Monitoring

The data sources that you include in your monitoring allow for timely identification of security events which might affect the delivery of your essential service.

Objective – achieved	How Illumio can help
You understand, based on your knowledge of your networks and common cyberattack methods, what you need to monitor in order to detect potential security incidents that could affect your essential service. For example, presence of malware, malicious emails, policy violation by a user.	Illumio customers typically use a source of truth to establish the key workloads, applications, and environments within their infrastructure, which can then be segmented in a granular fashion down to port/process/protocol if necessary. Vulnerability data can also be fed into the system to further augment the security posture and inform policy.
Your monitoring data provides sufficient detail to reliably detect security incidents that could affect your essential service.	New and/or malicious connections within the monitored environments are immediately viewable on Illumio's application dependency map. Output relating to these connections can be sent out to technologies such as a SIEM for further alerting and enrichment. Detail around the connection down to process level is available in this output.
As well as your network boundary, your monitoring coverage includes internal and host-based monitoring.	Illumio Core is specifically designed to monitor internal East-West traffic, which comprises around 80 percent of data centre traffic flow. As a host-based technology, granular information is available from monitored workloads, and segmentation strategies down to port/protocol/process can be applied dynamically.
Your process for bringing new systems on line includes considerations for access to monitoring data sources	Customers typically integrate Illumio software into golden images or deploy out using incumbent automation technologies such as Chef, Puppet, SCOM, Ansible, and others. Illumio pairing profiles included in these builds can contain connectivity and labelling information, meaning that new workloads are automatically included in the application dependency map as they spin up, and segmentation profiles can be applied on the fly.

Generating Alerts

Evidence of potential security incidents contained in your monitoring data is reliably identified and alerted upon.

Objective – achieved	How Illumio can help
You are able to resolve alerts to network assets, using knowledge of the network and systems.	With the ability to both feed into upstream components such as SIEM technologies, and a full documented API for Illumio Core, output on new or malicious connections can be correlated against; security posture and segmentation policies change dynamically based on attack information and vulnerability data.
You are able to flag alerts that relate to essential services and use this information to support your incident management capability.	Critical applications, environments, and workloads can be closely monitored for new, out-of-policy connectivity and output to other systems for analysis; or quarantined directly using Illumio's micro-segmentation functionality.

Proactive Security Event Discovery

You define examples of abnormalities in system behaviour that provide practical ways of detecting malicious activity that is otherwise hard to identify.

Objective – achieved	How Illumio can help
You have a sufficient understanding of normal system activity (e.g. which system components should and should not be communicating with each other) to ensure that searching for system abnormalities is a potentially effective way of detectingmalicious activity.	Illumio's real-time application dependency map allows a normal baseline of connectivity and network traffic to be established, both within applications and across environments. Simple green lines (allowed traffic) and red lines (disallowed traffic) indicate the network flows.
You maintain descriptions of some system abnormalities that might signify malicious activity, informed by past attacks (on yours and others' networks), threat intelligence and a general understanding of what an attack might look like.	Feeding new connection information from Illumio Core in correlation technologies such as a SIEM allows comparison to threat intelligence information, vulnerability data, and attack vector simulation. A compromised workload will appear immediately in Illumio's application dependency map view with new attempted network connections clearly highlighted. In addition, process information tied to these network connections is also fed back into the system and upstream components for further investigation.
Your choice of system abnormalities to search for takes into account the nature of attacks likely to impact on the networks and information systems supporting the delivery of essential services.	Vulnerability data can be incorporated directly into Illumio's realtime application dependency map, helping inform segmentation policy and security posture. Severity, exposure, and application criticality all feed into a "vulnerability exposure score" assigned to workloads, allowing teams to focus on the most critical systems at any given point, and change/apply segmentation policies as required to protect critical infrastructure.

As you can see, gaining visibility into and control of connections and flows inside of essential networks by means of a micro-segmentation solution is key to the guidance provided by the local controlling bodies.

Getting Started: Visibility is Key to Enforcement

How do you get started? Real-time visibility of traffic flows and potential compromises is an essential first step — after all, you can't protect what you can't see. Once a real-time application dependency map is established to view communication flows, it can then be used to derive granular policy and reporting. This exercise can also facilitate discovering and segmenting large areas of the sensitive network away from corporate IT as required. As the IT and OT (Operational Technology) worlds merge, tight control of the boundaries is needed.

Illumio Core provides the visibility and enforcement needed to adhere to the NCSC guidelines around the NIS Directive.

Key benefits include:

- See all your application dependencies and vulnerabilities through a real-time application dependency map.
- Take control of lateral (East-West) traffic within your data centre – ensuring that an attacker cannot move freely within your data centre or cloud.
- Stop breaches in their tracks by turning every host in your data centre and public cloud into a sensor that detects unauthorised traffic and an enforcement point for segmentation policy.
- Secure connectivity within and between clouds and private data centres with policy-based IPsec encryption.
- Eliminate service delivery delays and deploy applications with security that operates at the speed of DevOps.
- Write natural language policies that Illumio Core turns into IP-based enforcement rules.

Illumio enables organizations to realize a future without high-profile breaches by preventing the lateral movement of attackers across any organization. Founded on the principle of least privilege in 2013, Illumio provides visibility and segmentation for endpoints, data centers or clouds. The world's leading organizations, including Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite, trust Illumio to reduce cyber risk. For more information, visit www.illumio.com/what-we-do.

Gartner peerinsights™

See what customers have to say about Illumio.