illumio

SOLUTION BRIEF

Illumio for KSA Essential Cybersecurity Controls Compliance

Illumio Zero Trust segmentation isolates ransomware attacks and helps organizations comply with the Kingdom of Saudi Arabia's Essential Cybersecurity Controls (ECC-1: 2018)

Meeting the KSA's Requirements for Essential Cybersecurity

In 2018, the Kingdom of Saudi Arabia (KSA) enacted a sweeping regulation for cybersecurity: Essential Cybersecurity Controls (ECC-1: 2018). This is part of a global trend by governments to enforce more resilient cybersecurity protection within their countries.

The objective of ECC guidance is "to ensure the protection of [the] organization's network from cyber risks." Those risks include ransomware attacks that traverse networks through open ports, supported protocols and IP addresses to reach key data stores and application servers.

Detecting and stopping lateral movement is difficult. Attackers are stealthy, and network firewall configurations can be complex and challenging to maintain.

To comply with the ECC, organizations need to implement both network security management and vulnerability management so they can stop lateral movement and contain any breaches or malware, whether on-premises or in the cloud.

Zero Trust Segmentation for KSA ECC Compliance

By providing Zero Trust segmentation, Illumio helps organizations protect their networks and comply with ECC cybersecurity regulations, supporting the objective of ensuring "the protection of [the] organization's network from cyber risks."

Specifically, Illumio meets the standards set forth in the ECC for segmentation using "firewalls and defense-in-depth principles."

Illumio gives organizations visibility into their network traffic in data centers, cloud services and at the network edge. Using that visibility, IT teams can quickly define security policies, which Illumio automatically converts into rules for the host-based firewalls built into the systems running the organization's IT services.

By managing and restricting network services without requiring any replacement of network devices or software, Illumio makes network security management practical, efficient and affordable for organizations of all sizes.

With Illumio, organizations can implement ECC-compliant network segmentation in just days.

Practical and Precise Zero Trust Segmentation

Zero Trust Segmentation Made Easy
Traditional network segmentation solutions are complex, requiring IT teams to master a complex set of firewall rules. Illumio makes Zero Trust segmentation easy by automatically calculating and enforcing firewall rules.

Detailed Segmentation in a Snap
ECC regulations require organizations to segment development, test and production environments. With Illumio, organizations can easily segment networks by role, applications, environment, workload or location.

Confidence From Testing Before Deployment
Illumio allows organizations to run segmentation policies in test mode before enforcing them. This measure ensures that policies support authorized business traffic while blocking all other types of traffic without causing any network failures.

Illumio Makes Zero Trust Security Practical for Organizations of All Sizes

The Illumio product suite provides a detailed view of application communication flows so you know exactly what is talking to what on your network.

From that visibility, Illumio provides instant control to stop lateral movement — preventing the spread of cyberattacks across data centers, clouds and endpoint devices.

Illumio Zero Trust segmentation is purpose-built to support key tenets of the ECC, including Section 2-5 for Network Security Management and Section 2-10 for Vulnerabilities Management.

Network Security Management

By providing host-based micro-segmentation, Illumio Core (Illumio's flagship product) helps organizations stop lateral movement by isolating attackers and malware to keep them from spreading through your network.

Section 2-5-3 of the ECC requires this type of segmentation. Specifically, it calls for:

> "Illumio Core solved our challenges of managing fine-grained segmentation policies at scale. We now have the proper protections in place to stop lateral movement and keep hackers from accessing our critical applications and data."
>
> **— Edwin Leong**
> **Data Security Architect**
> **MGM China**

- **2-5-3-1: Logical or physical segregation and segmentation of network segments using firewalls and defense-in-depth principles.**

  Illumio enforces segmentation policies through existing host-based firewalls.

- **2-5-3-2: Network segregation between production, test and development environments.**

  Segregating environments is easy with Illumio, as well as segregating based on roles, applications, locations and workloads.

- **2-5-3-5: Management and restrictions on network services, protocols and ports.**

  Illumio restricts network traffic to just those services, protocols and ports explicitly allowed through Zero Trust policies.

Vulnerability Management

Section 2-10 of the ECC addresses the requirements for vulnerability management, including "the timely detection and effective remediation of technical vulnerabilities."

Subsection 2-10-3 calls for:

- **2-10-3-1: Periodic vulnerabilities assessments.**

  By monitoring endpoints and servers for suspicious activity, Illumio helps identify vulnerabilities that could compromise cybersecurity.

- **2-10-3-3: Vulnerabilities remediation based on classification and associated risk levels.**

  Once Illumio provides visibility into application flows and vulnerabilities, organizations can respond by containing any servers or endpoint devices that become compromised. They can also quickly refine security policies to eliminate specific vulnerabilities.

About Illumio

Illumio, the pioneer and market leader of Zero Trust segmentation, prevents breaches from becoming cyber disasters. Illumio protects critical applications and valuable digital assets with proven segmentation technology purpose-built for the Zero Trust security model. Illumio ransomware mitigation and segmentation solutions see risk, isolate attacks, and secure data across cloud-native apps, hybrid and multi-clouds, data centers, and endpoints, enabling the world's leading organizations to strengthen their cyber resiliency and reduce risk.