illumio

SOLUTION BRIEF

Illumio for Compliance With Gulf State Data Protection Laws

Illumio Zero Trust segmentation helps organizations safeguard sensitive data and comply with new data protection regulations in Gulf states

Gulf States Are Adopting GDPR-Like Requirements for Data Protection

Around the world, countries have noted the success of the European Union's General Data Protection Regulation (GDPR) as a standard governing the collection, management and protection of consumer data. Several Gulf states have recently passed their own data protection laws modeled on the GDPR. Organizations working in those countries or processing the data of their residents need to comply.

These new regulations, which vary in specifics, include:

- Bahrain's Personal Data Protection Law
- The Kingdom of Saudi Arabia's Personal Data Protection Law
- Qatar's Data Protection Law
- The United Arab Emirates' Personal Data Protection Law

Organizations need to monitor and protect personal data in the face of rising cyberattacks, including ransomware. At the same time, they need to ensure that security tools don't create new privacy vulnerabilities.

Illumio Zero Trust Segmentation Protects Private Data

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 converts into rules for the host-based firewalls built into the systems running the organization's IT services.

Using Illumio, organizations can implement Zero Trust segmentation rules to protect sensitive data from ransomware and data theft (exfiltration). At the same time, they can be confident that Illumio has no access to sensitive data. Illumio's product suite monitors and manages traffic without reading it, keeping your data secure and confidential.

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

Protecting Data From Ransomware and Other Cyber Threats

See Data Risks
Get both real-time and historical visibility into application traffic to detect unauthorized traffic to or from key data systems on-premises, in the cloud, and across hybrid environments.

Isolate Attacks
Assess and prioritize risks, automatically build and recommend rules, and apply Zero Trust policies quickly and efficiently, reducing pathways used for spreading ransomware or exfiltrating data.

Secure Data
Orchestrate and enforce security policies in data centers, cloud systems and remote endpoints to mitigate exposure, lower operational costs, and accelerate your path to Zero Trust — without sacrificing performance.

Illumio Makes Zero Trust Security Practical for Organizations of All Sizes

Illumio addresses critical risks to data privacy and security:

- **Discover unauthorized access into your data center and hybrid cloud network**

  Illumio reveals how applications with personal data are communicating with other systems, so that administrators can curtail unauthorized data access.

- **Block ransomware from stealing, destroying or encrypting your data**

  Illumio blocks pathways used by cybercriminals to collect, modify and exfiltrate personal, financial or organizational data. Even if criminals break into a network, Illumio stops them from moving through the network.

To deliver this protection, Illumio translates high-level data security and privacy policies into host-based firewall rules. You can enforce Zero Trust policies on every system in the enterprise.

> "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**

These rules block the unmonitored ports and protocols that attackers rely on for moving laterally through an organization's hybrid cloud network and accessing data.

The same visibility that helps IT teams identify pathways for lateral movement also helps identify any unexpected or unauthorized access to critical systems.

Gain Real-Time Visibility of Application Communications

Use Illumio application dependency maps to track and confirm communication pathways for an application or data repository without disclosing the sensitive information that those communications contain.

Working from these maps, IT teams can enforce policies to ensure that only authorized users and systems are accessing any applications or repositories storing personal data.

Illumio's product suite provides visibility into application communication flows and 24/7 control to stop lateral movement across IT environments — in the cloud, on-premises, in hybrid environments and at the network edge.

Protect Your Critical Data and Meet Regulatory Demands

Learn more about how Illumio keeps organizations of all sizes safe, operational and compliant.

Visit: www.illumio.com

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.