illumio

PRODUCT BRIEF

ILLUMIO CLOUDSECURE

Cloud-Native Security Simplified

Reduce cloud risk, simplify security management, and accelerate Zero Trust segmentation in the cloud

Cloud Risk: The New Challenge for Modern Enterprises

Cloud transformation is accelerating, as are the security challenges of providing Zero Trust protection to increasingly diverse digital infrastructure.

Gaining unified visibility into application traffic that spans an organization's multi-cloud, hybrid cloud and data center environments has remained elusive.

As a result, businesses struggle to understand how to implement and monitor Zero Trust security policies for all their clouds and data centers. Compounding the issue: A hodgepodge of tools from multiple vendors has created a fragmented view of cloud security risk, making it difficult for diligent organizations to see and address vulnerabilities, malicious activities or security incidents across their entire IT infrastructure.

With no comprehensive map that delivers clarity and insights about application traffic activity, clouds are opaque security risks full of disastrous potential for cyberattacks.

Visibility: The Foundation for Zero Trust

Illumio CloudSecure provides unprecedented real-time visibility into cloud workloads without the need for software agents. With CloudSecure, you can easily see into the digital traffic across multi-cloud and hybrid cloud environments.

And when coupled with Illumio Core, CloudSecure delivers a consolidated view of traffic among all your clouds and data centers, with the ability to build and enforce comprehensive, unified security policies spanning diverse computing infrastructures.

With CloudSecure, traffic data is always up-to-date and real-time with key contextual insights, helping you know more, know sooner and respond faster to security risks from cloud platforms.

CloudSecure makes it far easier to protect against breaches so organizations can embrace the cloud with confidence.

Embrace the Cloud With Confidence

Gain unmatched visibility, prioritize efforts and enforce security policies across multi-cloud and hybrid infrastructures

See Everything
Eliminate blind spots with a holistic view into cloud traffic flows. Proactively discover vulnerabilities and suspicious activity across multi-cloud and on-premises environments.

Understand and Respond
Gain deep insight into application behavior based on what did and what can happen inside and across clouds. Respond faster to policy changes and emerging risks.

Protect Everywhere
Easily program and enforce security policies across cloud-native applications and resources. Maintain a consistent security posture regardless of the environment.

How CloudSecure Delivers Visibility Into Cloud Environments

Gathering Data

CloudSecure collects object metadata and flow telemetry logs from public cloud accounts. These logs include:

- Traffic flow
- Service access (AWS CloudTrail)

In addition, CloudSecure gathers information about cloud objects and IaaS and PaaS infrastructure such as:

- Cloud servers and virtual machines (AWS EC2, Azure virtual machines)
- Cloud containers (AWS EKS, AWS ECS, Azure AKS)
- Serverless (AWS Lambda, Azure Functions)
- Cloud managed services (AWS RDS, AWS S3, Azure SQL Database)

> "I'm excited about Illumio CloudSecure because it can help us visualize risk in such a clear and informative way across Azure and AWS that was not otherwise possible."
>
> **— Greg Leibel, Cloud and Security Architect, Ixom**

Map Workloads and Connected Objects

Based on collected flow data, CloudSecure builds an application dependency map that offers a view of cloud environments — what is happening as well as what has happened inside and across clouds.

The map also defines guardrails that describe what should not happen by:

- Continuously looking for excessive risk
- Identifying and reporting policy violations in real time
- Suggesting how to change configurations to mitigate violations
- Detecting overly permissive configurations

Protect Everywhere

Using native controls, CloudSecure then uses the mapping data to recommend rules for guiding policy creation.

With CloudSecure, Zero Trust security policies can be automatically programmed inside cloud-native security controls such as AWS Security Groups, ensuring the continuous protecting of cloud-native apps, virtual machines and containers, as well as serverless, PaaS and IaaS infrastructure.

Cloud-Native Security Made Easy

The cloud is here to stay — and so are its security risks. Learn how Illumio CloudSecure brings unprecedented visibility and control to cloud computing.

Visit: illumio.com/cloudsecure

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.