ARGO EDGE CLOUD SECURITY PLATFORM

ARGO Edge

Secure Your Most Valuable Cloud Assets

Many organizations today contend with a patchwork of security solutions designed to protect traditional on-premises networks. With the rising popularity of remote workforce, BYOD, and cloud-first applications, organizations struggle to extend their security fabric to these emerging environments. As more business critical workloads migrate to the cloud, this mismatch of security solutions leaves critical gaps in security visibility that are often targeted by today's cyber criminals.

Argo Edge is a cloud-first security solution designed from the ground up to protect your users no matter where they are. As a **powerful cloud-based platform,** Argo Edge:

- Eliminates concerns from untrusted home or public network pathways
- Centralizes the security stack for policy enforcement, threat blocking, and monitoring regardless of user location
- Provides Cloud Access Security Broker (CASB) capabilities to identify and control "shadow SaaS" cloud usage
- Web browser isolation to thwart malicious websites from targeting your users

CISO GLOBAL

480-389-3444 | ciso.inc

ARGO EDGE CLOUD SECURITY PLATFORM

Advantages of Using Argo Edge

- Centralized security protection for your users at home, in the office, and on the move.
- Built-in threat-informed defenses powered by ML-enabled threat intelligence feeds, dark web monitoring, and CISO's team of expert threat hunters.
- Skip the pitfalls of managing multiple cloud security toolsets. Our experts will configure, manage, and monitor your cloud environment.
- Embrace the benefits of a secure cloud without the need for specialized expertise to deploy.
- Easy access to CISO's team of cybersecurity experts, compliance specialists, penetration testers, and threat hunters.
- Protect compliant cloud workloads with a solution that is secure by design from day one.

Capabilities

- **Secure Service Edge:** integrated security solution that connects users to cloud and web-based services and applications
- **Threat-informed Cloud Firewall as a Service (FaaS):** similar to traditional firewall that filters out potentially malicious or harmful traffic, but is hosted in the cloud
- **Zero Trust Network Access (ZTNA):** only allows users access to explicitly authorized applications and services
- **Remote Browser Isolation:** secures web access by hosting sessions on a cloud-based server, rather than on an endpoint device
- **Threat Intelligence Services:** data on cyber threat and context are gathered, analyzed, and used to help detect, respond, and prevent future attacks
- **Cloud Access Security Broker:** security checkpoint that is situated between cloud providers and cloud network users

CISO GLOBAL

480-389-3444 | ciso.inc