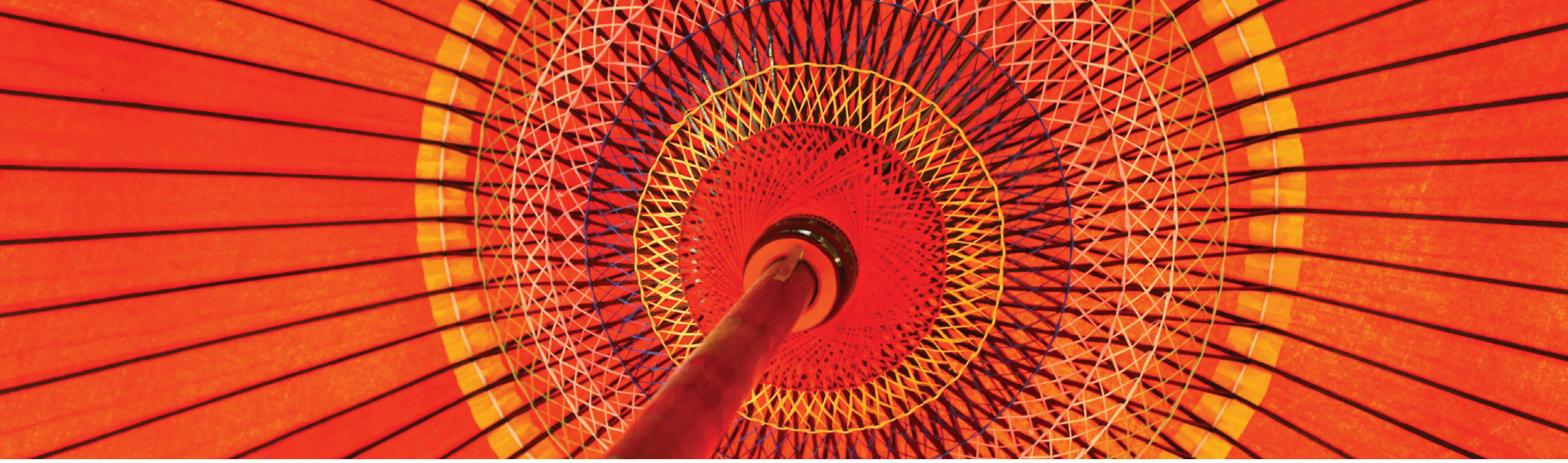


ARMOR AUTOMATED SECURITY AND COMPLIANCE—PRISMA™ PUBLIC CLOUD

MINIMIZE 'ACCIDENTAL' CYBER RISK ASSOCIATED WITH MISCONFIGURATIONS, IMPROPER SETTINGS, AND HONEST MISTAKES THAT CAN EXPOSE APPS AND DATA IN THE CLOUD

As organizations increasingly embrace the cloud, they must address both "accidental" and "intentional" cyber risk as part of their shared responsibility for security in Amazon Web Services (AWS). Cyber risk can be narrowed down to something as simple as the accidental risk introduced through cloud misconfigurations and open settings, or what IT or developers might do. But risk can just as easily come from the intentional risk caused by bad actors targeting your company or ransomware encrypting your data. And anything that gets in the way of delivering more code in support of business objectives typically means serious tradeoffs.

INTRODUCING ARMOR AUTOMATED SECURITY AND COMPLIANCE—PRISMA™ PUBLIC CLOUD

Armor Automated Security and Compliance—Prisma™ Public Cloud minimizes "accidental" cyber risk. Prisma™ Public Cloud provides industry-leading Cloud Security Posture Management (CSPM) capabilities to help you continuously discover, assess, and remediate security and compliance controls across your environment in the cloud. This includes identification of cloud misconfigurations and improper settings as a result of honest (and not so honest) mistakes and negligence that could put your applications and data at risk of exposure. In addition, the service provides an opportunity for organizations to establish a global security policy for assessing and managing risk across their cloud environments.

Get a Free Compliance and Security Assessment for:

- CIS v1.2.0 (AWS)
- GDPR
- HIPAA
- ISO 27001:2013
- NIST 800-53 Rev4
- NIST CSF
- PCI DSS v3.2
- SOC 2

ARMOR

Armor Automated Security and Compliance—Prisma™ Public Cloud

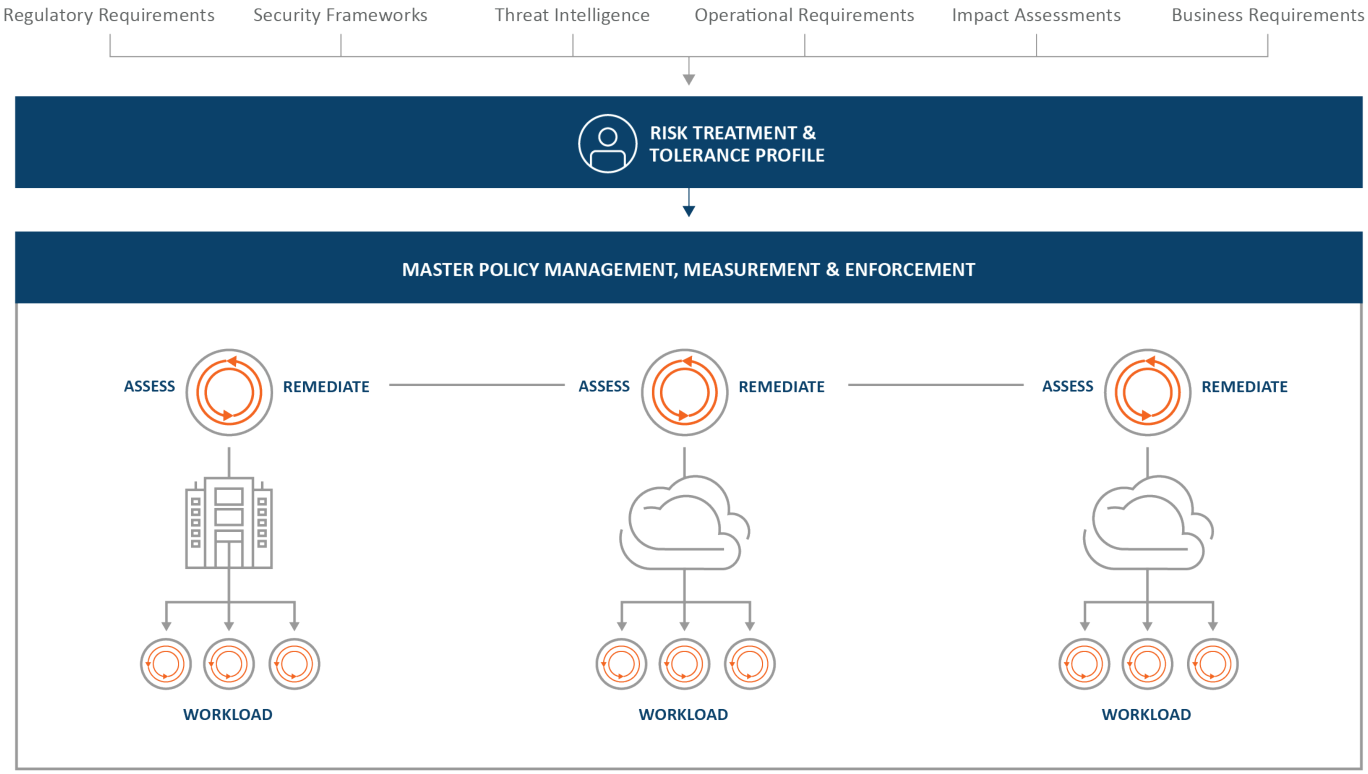
- Performs discovery of all instances and storage buckets (known and unknown) in the cloud
- Continuously scans your environment for misconfigurations, improper settings, and overall adherence to security policy
- Continuously scans your environment in AWS for adherence to compliance frameworks, such as PCI DSS, HIPAA/HITRUST and GDPR
- Applies automated security and compliance guiderails, starting early in the DevOps cycle, for accelerated application development
- Scans your storage buckets for misconfigurations that could expose data to the public

CLOUD SECURITY POSTURE MANAGEMENT (CSPM)

- Discovery
- Policy Visibility
- Policy Enforcement
- Continuous Scanning
- Controls Auditing
- Identification of Misconfigurations
- Risk Assessment
- Automated Remediation

ENVISION SECURITY AND COMPLIANCE TRANSFORMATION WITH THE CLOUD

Imagine a world where one global security policy is applied continuously across all of your workloads and across all your environments. Armor Automated Security and Compliance—Prisma™ Public Cloud provides organizations with the opportunity to fundamentally transform and simplify how you secure applications and data in the cloud, as well as comply with regulatory and other frameworks.



ARMOR.COM | 19010426