Rescale Zero Trust Security

Using the NIST Cybersecurity Framework, Rescale enforces the principle of least-privilege security across people, devices, networks, and workloads.

BRIEF

Zero Trust is not a single product or tool. At Rescale, Zero trust is a comprehensive methodology that encompasses security architecture, security policies, and security procedures. Collectively this approach delivers best-in-class security protection that our customers can rely on.

Zero Trust security is an essential part of Rescale's defense-in-depth strategy to ensure the Rescale platform, its data, and its customers are protected with the most comprehensive cybersecurity defenses in the industry.

ZERO TRUST DEFENSE-IN-DEPTH

Our defense-in-depth security strategy focuses on four key security facets: people, devices, networks, and workloads.

Zero Trust means that trust in any one of the four key areas does not implicitly mean trust in another. At Rescale, we live by the mantra: "Trust no one and verify everything."

With our security approach, any entity (people and devices) requires authenticated trust at every level. We constantly monitor all four areas to ensure that entities are operating securely within our trust model. Any attempt to subvert our security model alerts our Rescale Security Incident Response Team, which responds immediately based on established protocols and proceedures.

ZERO TRUST SECURITY AT RESCALE

Our security stack includes a powerful combination of AI/ML-integrated cybersecurity products and platforms, combined with comprehensive security policies.

With our cybersecurity infrastructure, we are constantly monitoring the four key security elements and how they interact with data.

This allows us to ensure that:

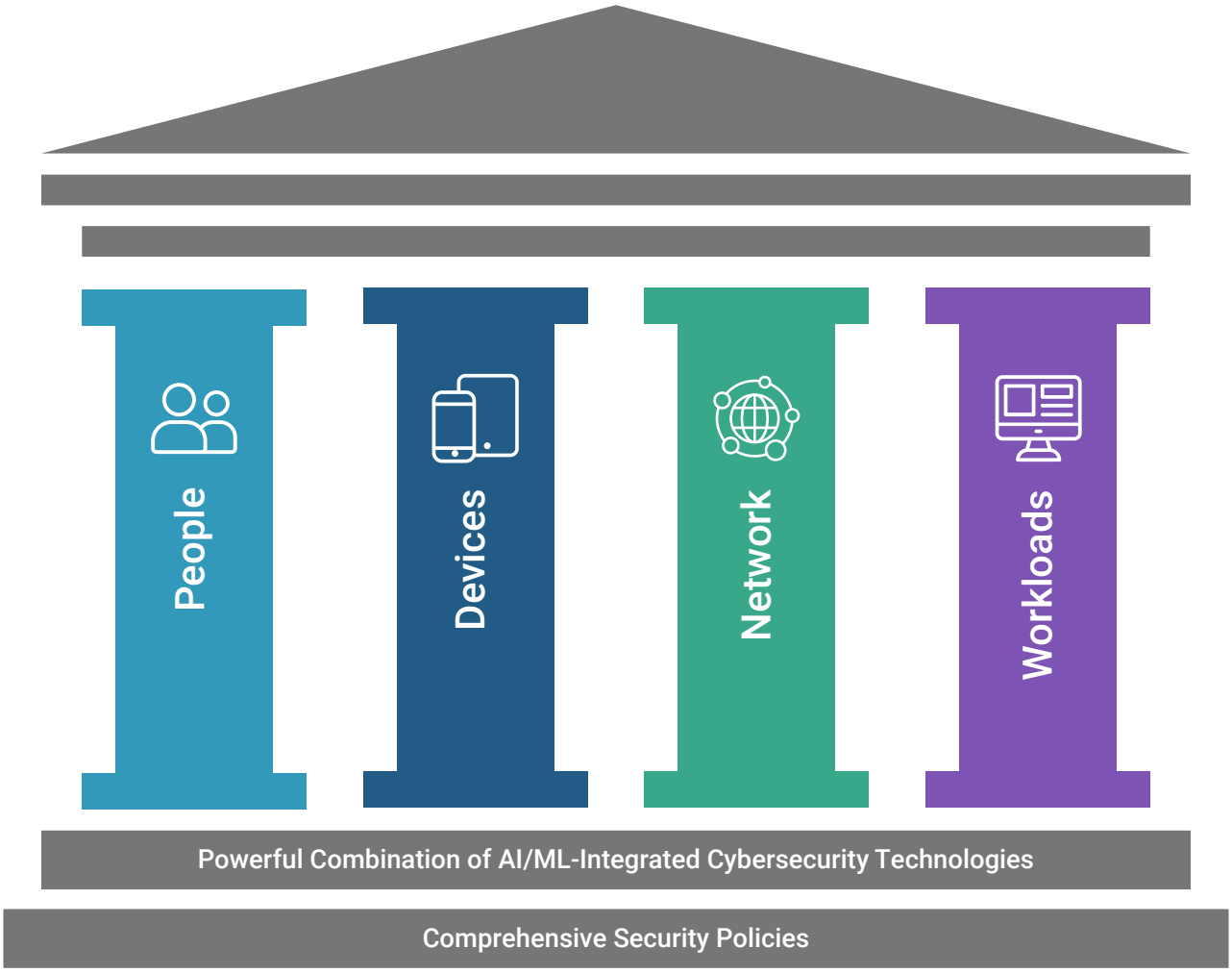
- Only authorized individuals (people) have access to data
- Authorized users are accessing company and platform data from secure endpoints (devices).
- All network access must be authenticated at all times, and we limit the flow of data to specific ports and protocols as defined by our principle of least privilege.
- Workloads are isolated from each other, are only allowed to move data within specified ports and protocols as defined by least privilege, and require authentication to access at all times.

Rescale adheres to the cybersecurity framework established by the National Institute of Standards and Technology in the U.S. Department of Commerce. The NIST cybersecurity framework guides Rescale in following all modern security best practices to mitigate risk and secure data and systems.

Rescale also uses independent third-party (external) auditors to validate and verify our security posture and maintain the current trifecta of cybersecurity certifications.

Rescale is your trusted partner for secure high performance computing built for the cloud.

Rescale's Zero Trust Framework



OUR SECURITY CERTIFICATIONS

Rescale currently has FedRAMP Moderate Authority to Operate (ATO), SOC 2 Type 2 certification, and ISO 27001 certification. Each of these requires third-party independent auditors to verify our level of cybersecurity and secure systems management, including comprehensive penetration testing and validation of our systems.

AICPA SOC · DFARS Compliant · CSA cloud security alliance · ITAR · FedRAMP · HIPAA

rescale

Headquarters
33 New Montgomery St., Suite 950
San Francisco, CA 94105
1-855-737-2253

About Rescale

Rescale is high performance computing built for the cloud to empower engineers while giving IT security and control. From supersonic jets to personalized medicine, industry leaders are bringing new product innovations to market with unprecedented speed and efficiency with Rescale, a cloud platform delivering intelligent full-stack automation and performance optimization. IT leaders use Rescale to deliver HPC-as-a-Service with a secure control plane to deliver any application, on any architecture, at any scale on their cloud of choice.