Revvity Signals: SaaS Products that Secure Your Research

We design, develop, and deliver our solutions using the security, confidentiality, and availability principles within the Trust Services Criteria (TSC). Protecting client data and ensuring uptime for our clients is paramount to Revvity Signals. Learn about the ways in which we work to keep your information secure and ensure business continuity.

Our Commitment to Service Quality

Revvity Signals follows an Agile Software Development Life Cycle, governed by Standard Operating Procedures under our ISO 9001 Certification. We follow the NIST 800-53 cybersecurity standard to deliver a secure, resilient solution to the market. This includes software design, development, verification, security, operations, and global support. Controls that conform to these highest standards are developed and deployed at all stages of our cloud services delivery. Our development practices are designed to adhere to OWASP and SANS 25 secure software development controls. We maintain a professionally developed platform and our service personnel operate this platform with the highest levels of training policies and operating procedures. All Revvity Signals staff undergo regular security awareness and confidentiality training as part of their employment obligations

Security

Cloud Security

Revvity's in-house developed SaaS solutions are TSC Type 2 tested for security, availability, and confidentiality requirements and ISO 27001 certified. These solutions, delivered using public cloud infrastructure from Amazon Web Services (AWS), address the needs of our customers in research and clinical review markets. We employ SSAE-18 SOC-2 (Systems and Organization Controls 2) attested services whenever we use third-party services as part of our offering. We assure industry-accepted security practices from our vendors either by reviewing their SIG Lite or CAIQ disclosures or their SOC-2 attestations.

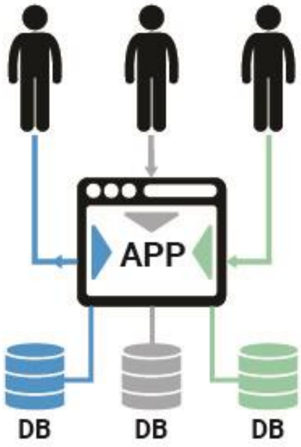
Security Assessments

Revvity conducts proactive security risk assessments at network, host, and application levels. All identified vulnerabilities are documented and remediated. Annual audits and penetration tests confirm the robustness of such strong practices. Revvity executes external penetration testing and vulnerability scans, static and dynamic code analysis. A multipronged vulnerability management strategy backs this risk and security assessment posture, along with our Security Incident and Event Management System (SIEM). We have a 24/7 operations center (SOC) with alerting and monitoring and on-call response teams.

Encryption Data is encrypted in transit and at rest using AES 256-bit encryption technology. Data transfer through the public network is encrypted in transit using HTTPS encryption. HTTPS encryption offers protection from “eavesdropping” and “man-in-the-middle” attacks. Communications between applications and database servers are encrypted.

Security Controls

In addition to the above, to address threats arising from the cyber risk world, we employ a robust set of access controls, privileged access management, SIEM, and web application firewalls (WAF), leading endpoint protection, log review, Intrusion protection system/ intrusion detection system (IPS/IDS), and threat and vulnerability management.



Confidentiality and Data Privacy

Revvity has multiple cloud environments in regions around the globe. Services are configured in the environment closest to the customer or in a specific region upon request. Our standard offering is multitenant infrastructure with complete data separation and isolation of customer environments with a separate schema and data storage bucket. Each customer is provisioned with their own end-point URL providing network data route isolation.

GDPR Compliance

We have controls and processes in place to comply with GDPR guidelines. This is enabled by isolated data storage within the multitenant environments. Figure 1.

Service Management

Incidence Response

Revvity Signals SaaS solutions are monitored for system security and application performance as well as availability. Security events and log data are aggregated for regular review. Exceptions are reported to support personnel and relevant actions are taken accordingly.

Service Availability

Revvity Signals SaaS solutions are designed to be resilient and can automatically survive many failures. Our SaaS solutions have physical redundancy using AWS availability zones, use load balancing throughout the applications, and multi-AZ RDS servers and services are deployed with auto-healing technology.

Business Continuity and Disaster Recovery

Revvity utilizes regional availability zones for service and access to all cloud applications. Our platform is resilient and designed to auto-recover from adverse events that may impact databases, application servers, or network services. Automatic database backups occur daily for disaster recovery and are geographically dispersed across multiple availability zones. Our services offer 24-hour Recovery Point Objective (RPO) and 48-hour Recovery Time Objective (RTO) Service Level Agreements (SLA).

Commitment to Delivering the Highest Level of Services

The efficacy of our controls is only valid when we can assess the effectiveness and demonstrate compliance. We perform annual third-party and internal audits of our services. Our multilevel risk management process reviews our entire business risk framework, then assesses risk and enforces remediation processes at a quarterly cadence. Individual products undergo risk assessment during product-release planning—occurring multiple times per quarter.

revvitysignals.com
77 4th Avenue
Waltham, MA 02451 USA
P: (800) 762-4000 (+1) 203-925-4602

Revvity Signals
RevvitySignalsSoftware
revvitysignals
Revvity_Signals
RevvitySignals