# A Fortress for Cloud Security

## How Revvity Signals Software Protects Customer Data

Cyberattacks are becoming more frequent and more expensive. The global average cost of a data breach in 2023 was USD 4.45 million, a 15% increase over three years, according to IBM. Adaptation to the changing landscape of cyberthreats is paramount to the security of sensitive data and intellectual property. Especially for the life sciences industry, protecting data is paramount.

To this end, Revvity Signals Software employs a multilayered approach to protect customer data. This comprehensive strategy is called "Defense in Depth" in the cybersecurity field, as it treats security like a castle fortified with many layers of protection. If a hacker attempts unauthorized access, the first level of protection will most likely intercept. But in the unlikely event that a threat breaks through the initial layer of defense, they should be blocked at the next level. Multiple barriers are designed to keep customer data safe and untouched. This paper will explain why data is safer with Revvity Signals Software.

## Data Security: The Safe

Data security is like locking the crown jewels in a sophisticated safe. Revvity Signals Software uses a Zero Trust security model, which is an approach that requires authenticating all users on both sides of every data transaction. As a software provider that follows the Zero Trust model, Revvity Signals conducts weekly vulnerability scans to identify potential issues and subsequently patch vulnerabilities. Furthermore, patches are synchronized with monthly releases for operating system updates and third parties to minimize vulnerability windows. With this strategy, Revvity Signals Software has an outstanding 95+% patching ratio for vulnerability scanning.

AES256-bit encryption is universally employed across the product portfolio for data at rest and in motion. Each customer has their own data segment; virtual network barriers provide data segmentation.

Data is isolated and protected because external data access is not allowed. Furthermore, data classification categorizes data assets based on their information sensitivity. By classifying data, organizations can determine who should be authorized to access it, using the principal of least privilege, and what protection policies to apply when storing and transferring data.

Moreover, intermittent backups ensure business continuity and disaster recovery. Through an automated backup system, data is backed up every eight hours, contributing to comprehensive disaster recovery and data resilience.

## Platform Services: The Castle's Walls

On top of data security, the utilization of world-class industry-trusted solutions serves as another layer of protection.

Revvity Signals Software’s Saas Solutions includes numerous platform services:

- An AI-based endpoint protection platform
- SaaS security controls

- Cloud-based security services
- AWS security services
- Virus and malware protection
- CIS hardening standard

## Host security: The Castle Itself

The protection of virtual machines is rigorously enforced with patching, IP restriction, and whitelisting, which permits only approved users access while denying all others. Only the customer's platform administrator can create accounts and define role-based access.

## Network Security: The Moat (perimeter-level security)

An Intrusion Prevention Service (IPS) firewall continuously monitors network traffic for suspicious activity. If it detects a potential intrusion, it blocks and prevents it. A Web Application Firewall (WAF) helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. Revvity Signals Software's services include monitoring and alerting, such as Application Performance Monitoring (APM) and Service Level Availability Monitoring (SLA). The organization maintains a continuous watch for threats at every level. Vulnerability scans are performed weekly for host, web application, and network perimeter protection.

Comprehensive code and runtime security scans find vulnerabilities and coding errors that could cause security issues. Overarching Security Incident Event Management (SIEM), which is an event management system for threat detection, collects event log data from a range of sources (security tools, product logs, and infrastructure logs). The SIEM uses artificial intelligence real-time analysis to identify suspicious activity.

Hackers don't observe business hours, so perimeter-level security provides round-the-clock surveillance. The Security Operations Center (SecOps), staffed by cybersecurity engineers, is located in the United States and India for "follow the sun" coverage in all time zones. The team is on call 24/7 with analysts ever available to triage alerts and escalate security issues as needed.

## Policies and Procedures: The Kingdom's Forest

Despite numerous services and automated solutions, the human element remains essential to protecting digital assets. Revvity Signals Software follows the industry's gold standards for cybersecurity policies and procedures.

The threat management workflow helps identify, analyze, evaluate, and address threats based on each threat's potential impact. SecOps engineers do daily “follow the sun” triage and remediation of cybersecurity events identified by the 24/7 SecOps Center, the endpoint protection platform, and the SIEM.

The incident response plan is a documented plan or playbook for a course of action after a cyberattack is identified. Unauthorized access to the system triggers specialized SecOps personnel to intervene. Predefined incident response playbooks describe the plan of action for all potential cyberattack scenarios: limiting attack vulnerability; quarantining affected systems; and analyzing, identifying, and remediating the particular security breach. Collaboration with a third-party forensic company enhances the cybersecurity response with deep-dive cyber investigations to respond to attacks.

Predefined plans document how the Revvity Signals Software Incident Response team will continue operating in a “war room” scenario during a service disruption or security event. A business continuity plan minimizes downtime by temporarily addressing the incident to maintain critical business functions. On the other hand, disaster recovery focuses on restoring and recovering cloud infrastructure after a disruptive event, minimizing downtime and data loss.

Revvity Signals Software requires annual Security Awareness Training for every employee, plus role-based Security Awareness courses for employees whose jobs are specifically related to data security and production customer cloud environments.

Change management defines corporate strategies to prepare, support, and help Cloud Operations teams to securely make changes to customer production cloud environments or development build procedures to support customer production. We adhere to the principle of least privilege and require secure connectivity to customer cloud production systems.

Identity and Access Management policies are role-based and manage who can access cloud computing resources. They are based on predefined security roles to control the level of access permissions so that each person only accesses what they need based on their job, and nothing else.

Constant vigilance is maintained over risk management, a security and compliance process related to identifying, assessing, and minimizing the impact of production cloud risks that could cause loss, damage, or harm to a Revvity Signals Software internal process, environment, customer computational environment, or associated data.

The cloud governance program involves defining, implementing, and measuring continuous actions around security and standardization.

## Compliance and Third-Party Verification

Revvity Signals Software goes beyond the basic requirements for software providers by seeking third-party verification to ensure Revvity Signals software is as secure as possible. Revvity Signals ensures that the following regulatory and industry compliance standards are met:

- SOC 2 Type 2, a voluntary compliance standard that specifies how organizations should manage customer data. Developed by the American Institute of CPAs (AICPA), we adhere and attest to the following trust services principles: security, availability, and confidentiality.

- ISO27001, the leading international standard focused on information security. It was developed for companies to protect their information systematically and enterprise-wide by adopting an information security management system.

- CIS Hardening Standard, a third-party standard.

## Ongoing Efforts to Win the Cyberwar

In light of emerging cyberthreats, a consistent regimen to identify risks includes gap analyses and annual penetration testing. When threats emerge, SecOps experts intervene to handle the situation with the correct cybersecurity expertise. Security is regarded extremely seriously, and Revvity Signals Software experts continue to evaluate and implement the latest best practices

and industry standards. The security team regularly meets with customers to discuss any concerns and to share expertise. Knowing the cyber battle is never over, Revvity Signals Software protects its customers' data by constantly assessing risk, building the security posture, adopting new capabilities, filling emerging security gaps, and reacting to worldwide security vulnerabilities.

Still have questions about data protection, compliance, and Revvity Signals' security posture? Ask a security expert and contact us.

Visit our Security and Compliance Page

Legal Resources

---

*LePree Anderson, Joy. "Global cyberattacks increased 38% in 2022." Security. 20th January 2023, https://www.securitymagazine.com/articles/98810-global-cyberattacks-increased-38-in-2022#:~:text=New%20data%20on%20cyberattack%20trends,according%20to%20Check%20Point%20Research.

**Cost of a Data Breach Report 2023, IBM. https://www.ibm.com/reports/data-breach

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

Revvity Signals
RevvitySignalsSoftware
revvitysignals
Revvity_Signals
RevvitySignals