Relativity® Trust

elevate

one | RELATIVITYONE SILVER PARTNER

Understanding Security in RelativityOne

Calder7, Relativity's In-House Security Team

Contents

Introduction

For any organization considering a software solution, no topic is more important than security. So much of a company's value and reputation is tied to the ability to protect their data and the data of their clients. Lasting reputational damage is just one of the impacts of a cyberattack. Effects of a breach can be widespread and unpredictable, including regulatory fines, litigation and investigation expenses, additional labor, lost productivity, and lost business, to name a few. In 2017, cyberattacks cost US enterprises $1.3 million on average.

Navigating the minefield of threats, risks, and vulnerabilities that make up today's ever-expanding threat landscape can be a daunting challenge. Simply deploying software and reacting to problems when they occur won't work. The most trusted organizations have a comprehensive security program—a holistic approach that weaves security into every aspect of the organization. It's the best and only defense for providing a secure and trusted experience for clients

When it comes to housing an organization's most sensitive data, there are no shortcuts— only a fully integrated security program will do. That's what we've built with RelativityOne. Customers can centralize their data and reduce risk with one secure SaaS solution backed by Relativity Trust, a security program that goes far beyond standard data security and privacy certifications. With preventative defense, automated processes, and transparent operations, we keep our customers' most sensitive data protected.

Preventative Defense

Relativity's goal is to anticipate threats and attacks before they happen to stay ahead of adversaries. Our security team, Calder7, leads the charge with a highly skilled crew of engineers, analysts, and subject matter experts tasked with protecting our customer's data.

Threat Intelligence

We've implemented a proactive approach to understanding the global threat landscape. We use advanced technology to rapidly contextualize billions of internal and external data points, gain insight into cyberattack trends, then detect, investigate, and analyze attacks. We also closely follow malware campaigns to ensure the malicious code cannot exploit vulnerabilities in our system.

From this intelligence, our security team curates a list of alerts that are triggered by suspicious events in our environment.

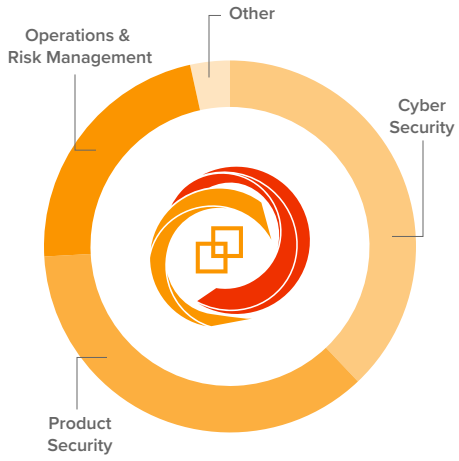
Using a combination of proprietary security controls and threat intelligence providers, such as Recorded Future, we gather, sort, and categorize threat intelligence activities by relevance. We use Anomali ThreatStream to store and distribute all intelligence, swiftly put protective and preventative controls in place, and create a central repository of insights for controlled sharing with the security community. This intelligence strengthens our defense against intrusion, proactively protects against potential incidents, and helps us rapidly respond to impending threats.

When it comes to housing an organization's most sensitive data, there are no shortcuts— only a fully integrated security program will do. That's what we've built with RelativityOne.

Dark Web Analysis

To gather intelligence from the dark web, we use a combination of advanced machine learning, text analytics, sentiment analysis, and string-matching algorithms that are employed across multiple languages to contextualize the data and find threats. We examine Tor sites, hacker forums, paste sites, and other open source sites not indexed by internet search engines. We look for indicators of suspicious behavior, such as malicious code, content targeted at our industry, relevant stolen documents, and user credentials. We work with technology platforms, including Azure Security Center, Redlock, Anomali ThreatStream, and Recorded Future, to provide us with insight into spaces where threat actors communicate, plan, and execute cyber activities. This enables us to implement strong defensive strategies before an attack.

Calder7 is made up of 58 security experts



Calder7 Quick Facts

- Formed in January 2018
- Nearly **tripled in size** in the first 12 months
- Name was inspired by Alexander Calder's Flamingo sculpture that resides outside of Relativity's Chicago office
- Last year, the team culled through over 130 billion events in RelativityOne
- We've had **zero severe incidents**

Threat Hunting

We have specialized analysts that focus on threat hunting to find, analyze, and mitigate suspicious activity that doesn't currently trigger alerts in our system. Every day, our threat hunters dig through terabytes of data to identify trends and spot unusual user behavior, traffic flows, or configuration changes that could indicate a new or emerging threat. We use and train machine learning technology to search for and identify new indicators of suspicious and anomalous activity and get to the root of the problem faster. This threat-hunting approach ensures we are examining data in multiple ways to continually learn and improve our threat-detection abilities.

Threat Investigations

Our digital forensics investigators reverse engineer malware and other malicious code to better understand the threats posed to the system and reduce the possible attack surface. We use a variety of system and network monitoring utilities, disassemblers, and debugger tools to examine the innerworkings of malicious software.

Malware can be investigated in several ways to better understand its behavior. Our investigators use a combination of sandbox technologies to provide a safe environment to triage the malicious code. This helps us better understand how the malware affects the computer, attempts to communicate, and spreads. Additionally, investigators may perform a dynamic examination of the malware by activating it in an isolated environment. Finally, we can perform a static analysis of the malicious code to fully understand how the malware functions, what capabilities is has, and to gain an understanding of its authors—ultimately allowing us to obtain a thorough understanding of the risks, as well as the means to defend against it.

Network Defense

We use a combination of monitoring techniques to protect our network in real time from cyberthreats and have safeguards in place to ensure data is encrypted while at rest and while it's moving around the network. Our security analysts use Palo Alto

Networks to keep a pulse on network traffic and interactions by monitoring customer access points and partner systems that can provide openings for cyberattacks. We search for unusual data traffic from users and applications on our network, such as large or unexpected data movement within the network and data downloads that are outside of normal parameters. We monitor our cloud assets for misconfigurations in cloud deployments, anomalous user behavior, and suspicious usage of IaaS and PaaS resources, helping us maintain a 360-degree view into vulnerabilities and remediate quickly before they are exploited.

Internal Threats

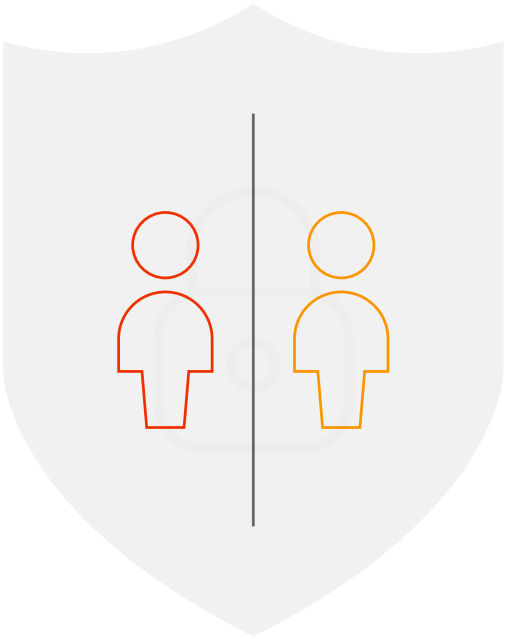
We protect against insider threats and ensure our intellectual property is secure by profiling the behaviors and activities of our employees, contractors, and customers. Based on profiles of what is considered normal behavior, we seek anomalies that could be indicative of an approaching internal threat. Our security analysts investigate these behaviors to determine the severity of the threat or whether it is purely accidental. We use this data to continually improve our understanding of customers, employees, and contractors, and to better protect our intellectual property and the intellectual property of our customers.

> Every day, our threat hunters dig through terabytes of data to identify trends and spot unusual user behavior, traffic flows, or configuration changes that could indicate a new or emerging threat.

Security Awareness

Relativity promotes an atmosphere of security awareness with our employees. From our hiring process to our continual training, employees are accountable for information security responsibilities and ensuring that security policies are upheld—even after their departure. Ad hoc campaigns are designed to spread security awareness, including individual responsibility to report suspicious events, potential phishing emails, and potential unauthorized access. Our gathered intelligence from our internal awareness campaigns also provides us with a source of knowledge that we share within the organization to keep awareness high at all times.

We provide employees with an understanding of the types of attacks we need to prepare for and defend against, regardless of whether they work in internal operations, support customers, or develop code for our product. We give employees techniques to spot attacks and defend against social engineering, and we regularly test their ability to correctly respond to and prevent attackers from gaining access to our system.



58 Calder7 | **78 Security Guardians**

Vulnerability Assessments

We conduct internal and third-party vulnerability assessments for identifying, classifying, and remediating potential weaknesses, increasing the difficulty and cost for attackers trying to take advantage of our systems.

At least once a year, a third-party firm is hired to purposely attempt to break into Relativity. Not only do they try to physically make their way into our secured offices, but they also attempt to gain unauthorized access to our network, machines, and applications. These engagements are designed to mimic the tactics of a real-world attacker, and the findings help us continually improve our security posture.

Along with hiring a third party, Relativity also conducts internal penetration testing engagements. We focus on risk reduction and perform penetration tests ranging from social engineering exercises, such as sending phishing emails or plugging in malicious USB drives, to attempting to exploit business-critical systems. Similar to the third-party engagements, the results of these tests help us continually improve our policies, procedures, controls, and detection and lower our overall risks.

Relativity promotes an atmosphere of security awareness with our employees. From our hiring process to our continual training, employees are accountable for information security responsibilities and ensuring that security policies are upheld—even after their departure.

Automated Security Processes

To achieve the ideal balance between accuracy and speed, we've implemented automated security procedures that maximize the effectiveness of our technology, processes, and people.

Log Automation

We leverage automation capabilities in tools like Splunk to eliminate much of the manual processes behind collecting, contextualizing, and making data readily ingestible to monitoring systems—historically a long, laborious, and error-prone process. Our log automation also improves the speed and quality of the data ingested into Relativity monitoring systems.

Additionally, we continuously monitor each RelativityOne instance for security-related events. A wide variety of indicators feed Relativity's alerting system, such as logon events, creation of new users, and alerts from Azure anti-malware. An aggregator ingests logs from the RelativityOne production environment, support infrastructure, and access logs, and an integrated rule-based tool provides automated alerts. Our security team responds to critical alerts on a 24/7 basis. This enables us to reduce the time it takes to identify issues, understand risks, and make security decisions to remediate issues.

Threat Intelligence Platform

To ensure we can contextualize incoming threat feeds and data as fast as it comes in, we employ a threat intelligence platform (TIP) that has our "single source of truth" for intelligence information. This platform automates many aspects of the data collection processes that are repetitive and time-consuming, allowing security analysts to focus on the threats that require high-level analysis rather than manually investigating every system alert.

Our threat intelligence platform continuously monitors more than 200 intelligence data feeds that are incorporated into our monitoring process. The data

is scored according to relevance and accuracy, then merged with other commercial threat intelligence information from government and commercial sources. Indicators from the TIP are then distributed to endpoint protection—such as next-generation firewalls, anti-malware, anti-spam, and EDR solutions—to provide protection. This context-rich data enables our analysts and engineers to build optimized workflows and refocus efforts on proactive threat hunting and risk mitigation.

Secure Coding

Our security and engineering teams deliver application security by continually working together to ensure all code is reviewed following the guidelines of our secure software development lifecycle.

All RelativityOne developers are required to take courses in security awareness and secure coding, and our coding standards have a strong security component. Each time code is checked into our source repository, it is reviewed by a developer with security as a priority.

As part of our secure software development lifecycle, code for new features goes through a structured review process with the security team. Projects with heightened attention include data storage, authentication, authorization, passwords, cryptography, transmission of data, new product design, use of HTML-enabled fields, and licensing. All custom rich text controls are coded to prevent cross-site scripting as well as SQL injection.

Security reviews and tests are performed for all software developed for Relativity and RelativityOne. For outsourced feature development, the legal team reviews acquisition contracts and incorporates security-related specifications, documentation, and developmental and evaluation requirements.

Role-based security training and awareness programs reinforce our secure-coding principles and procedures. Secure-coding guidelines are maintained on the company intranet.

Vulnerability Scanning

We use a variety of tools to continually scan our source code and enterprise assets to ensure vulnerabilities do not make it into our product. Whether an issue arises internally or externally, our goal is to ensure that we can identify and remediate it as quickly as possible. To mitigate these risks, we employ a variety of scanning approaches to alert us to problems.

Corporate asset vulnerability scanning delivers deep insights into trends, common vulnerabilities, susceptible assets, and other data to give us a better picture of our infrastructure. Microsoft Security Center ensures that we are up to date with all our software and Windows patching. We also scan our code libraries against third-party libraries to search for vulnerabilities identified by other companies. Static and dynamic code analyses enable us to test our own code and even run attack simulations to search for possible weaknesses in our code. With the deep insights gained from these processes, we can reduce the time it takes to identify issues and stop potential attackers from gaining access to our system.

Transparent Operations

We ensure data security and privacy through our aggressive compliance standards paired with a transparent culture, where we share valuable cyber information with customers and the industry to advance security capabilities beyond our organization.

RelativityOne Compliance

We view our information security, risk, and privacy program as a pledge to our customers. Our compliance team conducts ongoing evaluations of control performance and changes in risk profile for RelativityOne. We also engage in multiple annual examinations by third-party accredited examiners.

We are ISO 27001 certified and have achieved SOC 2, Type II attestation. These certifications represent key market-based standards for information security and assure our customers that we have established the required processes necessary to effectively manage information security to global standards. The certifications also substantiate that our processes are being followed across RelativityOne services upon request from our customers.

We continually evaluate RelativityOne processes against other customer and industry-specific standards, such as the Cloud Security Alliance Common Control Matrix, PCI DSS, HIPAA BAA, and FedRAMP. We constantly monitor key ongoing RelativityOne regulatory compliance activities and have a defined roadmap for achieving additional industry and cloud standards. We share our assessments and our roadmap with customers as appropriate.

Microsoft Azure Platform

In addition to our rigorous compliance standards that went into the design and delivery of RelativityOne, our Microsoft Azure infrastructure environment meets more than 70 international and industry-specific compliance standards, such as ISO 27001, SOC 2, Type II, HIPAA, and FedRAMP, as well as country-specific standards like Australia IRAP, UK G-Cloud, and Singapore MTCS.

We optimize the customer's role through a partnered approach to security encompassing data handling, data processing, and data storage. Customers determine what data to put into RelativityOne and control the processes they require for selecting and handling data.

Our RelativityOne cloud service processes this data rapidly and provides powerful options for analyzing and identifying the most critical data. Customers can rely on RelativityOne's compliance credentials for securing data during processing.

We partner with Microsoft Azure for infrastructure services. Our data center structure supports varied country requirements. Customers can rely on Microsoft Azure's extensive credentials for storing data and maintaining data continuity.

Shared Security Insights

In addition to hunting for vulnerabilities, we regularly share insights with customers and frequently work side by side with them to correct critical vulnerabilities in their own environments. We can provide customers access to the relevant security logs from their RelativityOne instance through our security information and event management platform. This enables customers to conduct an independent second-level log review and identify security events unique to their organization and threat model.

Additionally, we present at conferences, produce white papers, write blog posts, and engage with customers to present the latest threat landscape, attack patterns, and mitigation strategies for protecting customer environments. We also collaborate with our threat intelligence providers to share indicators of compromise to further enhance detection in the industry at large.

Security Community Advancement

Through collaboration, sharing of events and indicators of compromise, output of analyses, and regular educational offerings, we are part of a whole community of cybersecurity professionals. This community gives us invaluable insight to threats in the wild and allows us to contribute to increasing the overall security posture of all participants.

We belong to Information Technology – Information Sharing and Analysis Center (IT-ISAC), a forum for managing risks and strengthening IT infrastructure through cyber-information sharing and analysis. IT-ISAC is a community of our peers who see a much larger collection of threats against IT critical infrastructure.

We also adhere to MITRE ATT&CK adversary behavior framework to understand risks, plan, verify defense, and contribute back to the community of organizations involved. This knowledge base of adversary tactics and techniques is generated from commercial organizations, government agencies, and cybersecurity professionals. By mapping indicators to the MITRE ATT&CK matrix, we can share context and provide usable and actionable intelligence to help the community take a proactive defensive stance. This alignment allows us to improve our security posture while helping advance the usable knowledge available to other organizations.

We also partner with the Open Web Application Security Project, an organization that provides unbiased and practical cost-effective information about computer and internet applications, as well as the Cloud Security Alliance, which promotes best practices for securely operating in a cloud environment.

This community of cybersecurity professionals gives us valuable insight to threats in the wild and allows us to contribute to increasing the overall security posture of all participants.

Conclusion

The threat landscape will continue to grow more complex as cyber criminals search for new ways to gain access to valuable information. It's up to each organization to keep client data safe, and there are no shortcuts to get there.

The fully integrated, comprehensive security program wrapped around RelativityOne focuses on just that—protecting customers' most sensitive data. We've established preventative defense strategies, fueled by advanced threat intelligence analytics and automated processes, to identify vulnerabilities and stop attacks before they happen. We are dedicated to continuing to meet aggressive compliance standards and maintaining a security-aware culture. Lastly, we believe in working hand in hand with the security community to share actionable intelligence, elevate security practices, and create a united front against threat actors.

You can count on Relativity to work tirelessly to protect your data and ensure your reputation remains a reflection of the services you provide your customers. If you're interested in learning more about Relativity's security program, please contact us and we'll connect you with one of our security experts.

Relativity Trust

Relativity Trust is a fully integrated and comprehensive security program that goes far beyond standard data security and privacy certifications. We've established an entire culture of security, centered around preventative defense, threat intelligence, automated processes, and transparency. When you work with Relativity, you can trust that your data is secure.

CALDER7

Calder7 is Relativity's internal security team. The team's cybersecurity, product security, compliance, and risk specialists are united under one mission: anticipate threats and stay ahead of the adversaries. By leveraging threat intelligence, cloud security, and software engineering, Calder7 makes Relativity and our products safer every day.

Relativity®

231 South LaSalle Street | 8th Floor
Chicago, Illinois 60604
+1 (312) 263-1177 | relativity.com