# Zero Trust Vendors to Watch, Know, Understand: ZT Applications - API Gateways

Michael O'Neil, Alex Banghart,
Rob Forbes, Joseph Karpenko,
Michael Wilcox, Cheryl Rodenfels, Chris
Hudson, Aaron Smith

stratascale
An SHI Company

# Executive Summary & Featured Companies

Applications are the focus of a great deal of attention within zero trust (ZT), and within cybersecurity strategy as a whole. Applications – especially proprietary applications that help an organization to build competitive advantage – represent critical IP, and need to be protected via the ZT framework.

Applications also represent the point at which security is visible to the business as a whole, because all internal users (and in many organizations, external users such as suppliers, customers, and other stakeholders) rely on applications to access and work with needed data. This visibility significantly raises the stakes for the security organization.

Users who find security measures overly restrictive will look for (shadow IT) workarounds, increasing overall organizational IT costs and decreasing visibility into potential vulnerabilities and threats. Measures that imperil critical business processes –for example, a security control that ends up preventing a single quarter-end deal from being processed – will destroy months' worth of good will generated by frictionless ZT security approaches.

A second complicating factor with applications is that they tend to enter the organization from two distinctly-different sources: every major business uses a mix of commercial offthe-shelf software (COTS) and internally-developed software, which in today's industry, is the product of a DevOps "software supply chain." Security professionals need to deploy technologies and management practices that are capable of addressing both COTS and internally-developed applications.

After considering these factors, Stratascale SMEs identified seven critical ZT application capabilities and technologies:

- Application inventory
- Least privilege access to data
- Workload monitoring
- Application data flow mapping and dependency mapping
- Secrets management
- API gateways
- User experience

### API gateways

API traffic represents an enormous subset of total traffic – and an enormous potential vulnerability for the businesses that use APIs to connect applications. It is essential that API traffic be managed effectively and consistently. As one contributor to this document noted, "you shouldn't be running APIs out of every single application. You should have an API gateway implemented where you're making calls and every app is using the same API call" – and not coding APIs for common applications like Salesforce into every 3 OF 10 application that feeds into or takes data from the CRM system. An API gateway provides a single point to control API calls, across both COTS and internally-developed software.

A series of meetings involving SMEs from Stratascale's security practice, Office of the CISO, Office of the CTO, and Innovation Labs assessed 12 vendors, resulting in a list of five vendors as a starting point for firms looking to enhance API gateway capabilities as part of a broader zero trust applications strategy. Vendors listed here share two characteristics: they are familiar to our team of experts from our work with clients, and are considered relevant to both API gateway and zero trust applications strategies.

Please note that no recommendation or warranty is implied by the inclusion of any vendor within this report.

## FEATURED COMPANIES


### Drilling down

Stratascale assembled a cross-functional group of security and application experts to create this report. This group included eight Stratascale SMEs:

- Stratascale Director of Zero Trust and Identity Services Rob Forbes
- Stratascale Director of Software Security Services Aaron Smith
- Senior Technical Advisor for DevOps and Automation Chris Hudson
- Field CTO Cheryl Rodenfels
- Field CISO Joseph Karpenko
- Vice President - Office of the CISO Michael Wilcox
- Cybersecurity Research Analyst Alex Banghart
- Lead Cybersecurity Research Analyst Michael O'Neil

Stratascale launched this vendor analysis by setting out guidelines for assessing and highlighting vendors: we considered for inclusion firms that are actively supplying API gateway solutions that support zero trust applications strategies to enterprise customers. The group also drew a distinction between vendors who are broadly applicable in the enterprise environments that Stratascale addresses (generally, Fortune 1000 businesses), and those which are relevant in specific niches, but not across all potential enterprise use cases. For ZT API gateways, the list is as follows:

- 42Crunch
- Cequence Security
- Salt Security
- StackHawk
- Traceable Inc

Please note that this list is subject to change over time, as new vendors and capabilities become available.

*Stratascale brings a unique combination of expertise, solution depth and vendor relationships and insight to the cybersecurity market. Readers seeking support in developing zero trust strategies are encouraged to contact their Stratascale Client Advisor or to connect with us at stratascale.com/contact-us/*

# 42Crunch

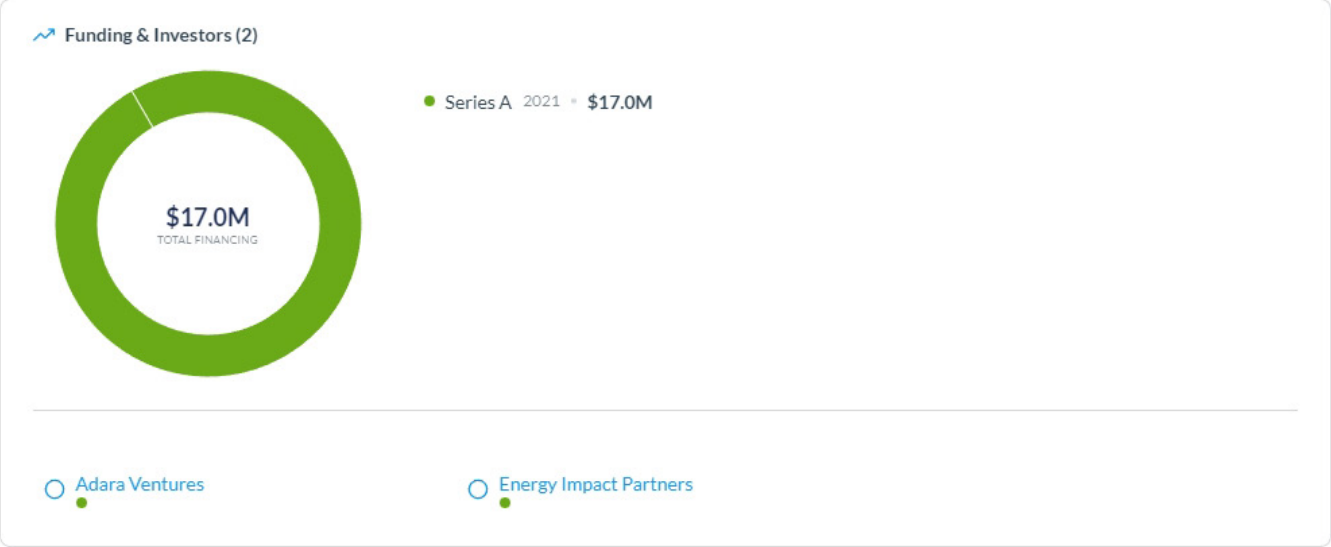
http://www.42crunch.com/

**KNOWN FOR:** 42Crunch provides continuous API security to protect the digital business.

## DESCRIPTION

APIs are the nervous system of the digital enterprise. Enterprises are marching full steam ahead, building new agile applications based on APIs to increase reach and foster innovation, connecting with their customers, employees, partners and developers. These new applications are often built on orchestrations of existing internal APIs, partners APIs and public (SaaS) APIs. While every company is pursuing the gold rush and deploys new applications at speed, the security requirements are often overlooked, taken as an afterthought. At best, security is limited to authentication and authorization, but this is not enough to fully address the API security spectrum. 42Crunch is the only enterprise grade, full-fledged API Security platform, addressing the development, testing and deployment security requirements of an API infrastructure.

## FUNDING & INVESTORS




## EXECUTIVE TEAM

**Jacques Declas**
CEO & Co-Founder

**Philippe Leothaud**
CTO & Co-Founder

# Cequence Security

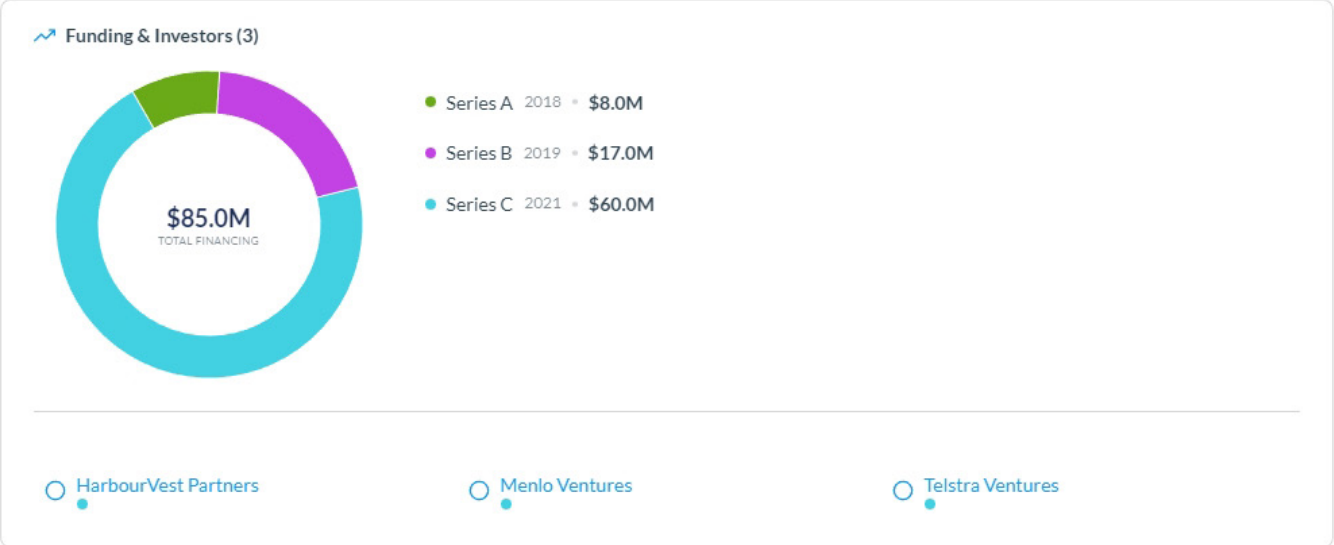
https://www.cequence.ai/

**KNOWN FOR:** Cequence secures web, mobile, and API applications. We discover all apps, detect malicious bots, and stop attacks with an AI-integrated security platform.

## DESCRIPTION

Organizations that increasingly rely on APIs to power their businesses trust Cequence Security to deliver the most effective and adaptive defense against online fraud, business logic attacks, exploits and unintended data leakage, which enables them to remain resilient in today's ever-changing business and threat landscape. Cequence is the only Web and API Protection Platform vendor that provides runtime API visibility, security risk monitoring, and patented behavioral fingerprinting technology to consistently detect and protect against ever evolving online attacks without the development and deployment friction associated with alternative offerings. Customers include F500 organizations across multiple vertical markets, and our solution has earned numerous industry accolades.

## FUNDING & INVESTORS




## EXECUTIVE TEAM

**Larry Link**
President and CEO

**Ameya Talwalkar**
Co-Founder and CPO

# Salt Security

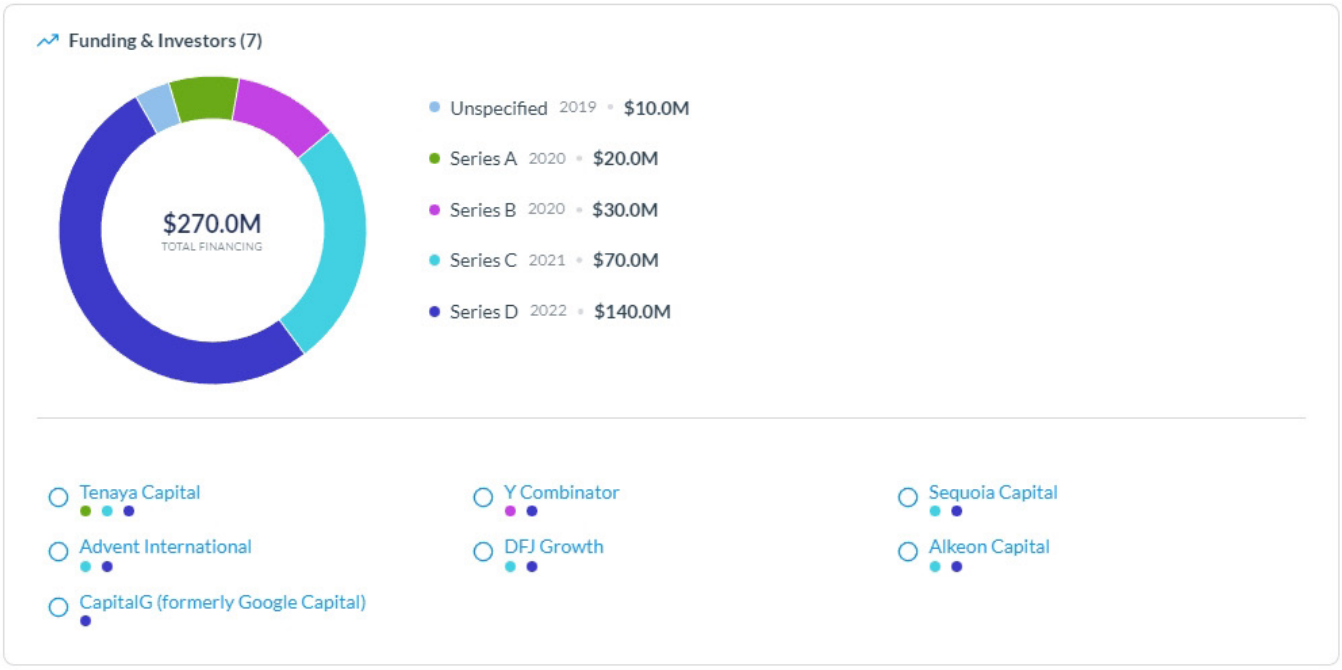
https://salt.security/

**KNOWN FOR:** At Salt, our sole mission is to protect the APIs that are the core of every SaaS, web, mobile, microservices and IoT application.

## DESCRIPTION

With the next generation of API attacks hitting the headlines, we created the first patented solution to prevent these imminent threats using behavioral protection. Deployed in minutes, our AI-powered solution automatically and continuously discovers and learns the granular behavior of any company's APIs and requires no configuration or customization to help ensure protection. The Salt team consists of engineers from elite intelligence units. Coming from a background in offensive cybersecurity, we think like attackers every step of the way when building our products. We believe in products that simplify processes, and save you time, rather than introduce additional load. We believe in precise solutions. We are reimagining what API security should be. With no other solution in the market today defending against attacks that exploit API logic and vulnerabilities unique to each company and application, Salt leads the way with innovative next-generation API protection.

## FUNDING & INVESTORS




## EXECUTIVE TEAM

**Roey Eliyahu**
Chief Executive Officer & Co-Founder

**Michael Nicosia**
Chief Operation Officer & Co-Founder

# StackHawk

https://www.stackhawk.com/

**KNOWN FOR:** StackHawk, a software-as-a-service (SaaS) company focused on security software for businesses. The company is headquartered in Denver, Colorado.

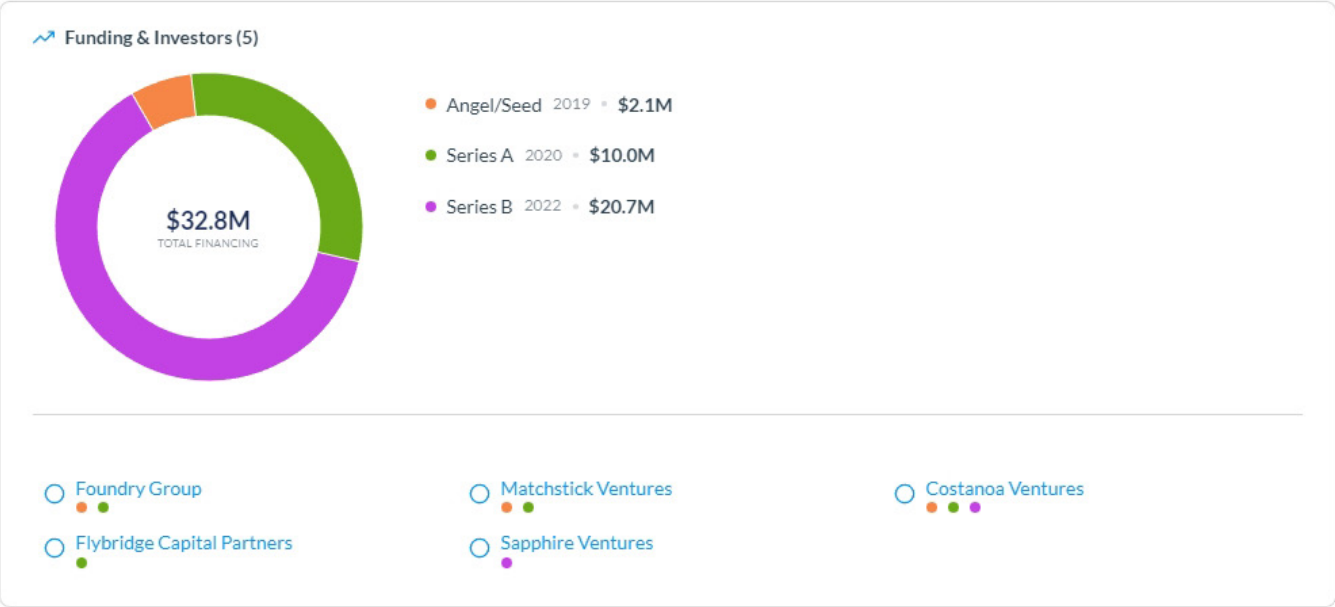
## DESCRIPTION

We believe that application security belongs in the hands of the engineers who write code. It should be automated within current workflows, simplifying the process of building secure software.

Built for developers is not just a recent addition to our marketing site. It is the reason we exist.

- **More than a dev tool:** StackHawk is more than a dev tool. StackHawk is confidence and security, closer to the keyboard than ever.
- **This is not security for "security people":** Developers should own security, but existing AppSec tools are built for antiquated security teams. StackHawk is AppSec *truly* built for modern engineering teams.
- **Right where security matters:** Security bugs are best caught pre-production, with the context of the code currently being worked on.

## FUNDING & INVESTORS



## EXECUTIVE TEAM

**Joni Klippert**
CEO & Founder

**Ryan Severns**
COO & Co-Founder

# Traceable

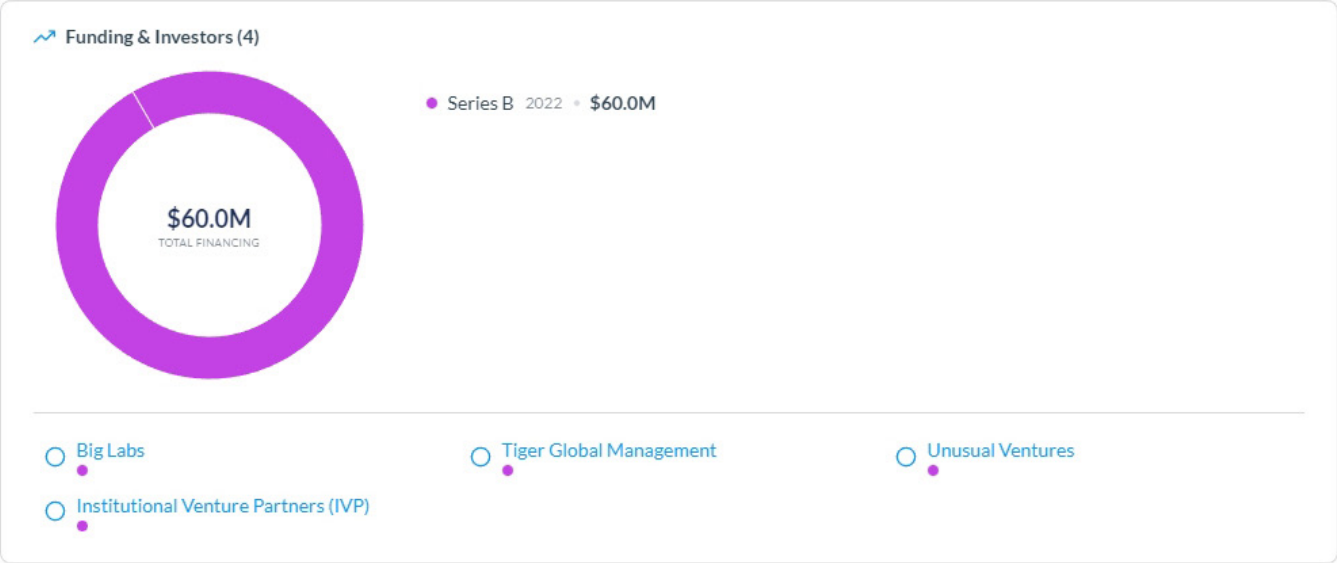
https://www.traceable.ai/

**KNOWN FOR:** Modern applications are extremely hard to secure and protect. Microservices, APIs, and cloud services are complex and continuously change. Traceable enables security to keep up with engineering and the continuous pace of change and protect modern applications from modern threats.

## DESCRIPTION

Traceable was founded by third-time entrepreneur Jyoti Bansal and Sanjay Nagaraj. Bansal and Nagaraj saw the massive adoption of cloud-native architectures firsthand during their time at AppDynamics and founded Traceable as a result to protect applications from next-generation attacks. Traceable applies the power of machine learning and distributed tracing to understand the DNA of the application, how it is changing, and where there are anomalies in order to detect and block threats, making businesses more secure and resilient. Our team has decades of experience in designing and operating industry-leading products to help modern DevOps, SRE and engineering teams. Our founding team included founders and key executives at AppDynamics and Harness, leading companies in the DevOps space. We have seen first hand transition to micro services and cloud-native architectures, and we have clearly seen how application security has become a major bottleneck for many companies. We are bringing our expertise with DevOps and managing large-scale distributed systems to rethink how modern applications and APIs can be secured.

## FUNDING & INVESTORS




## EXECUTIVE TEAM

**Jyoti Bansal**
CEO & Co-Founder

**Sanjay Nagaraj**
CTO & Co-Founder