Vendor Profile

ZeroNorth, Bringing End-to-End Clarity to Application Security

Jim Mercer Christina Richmond

IDC OPINION

IDC forecasts that by 2023, more than 500 million digital applications and services will have been developed and deployed using cloud-native approaches (see *IDC FutureScape: Worldwide IT Industry 2020 Predictions,* IDC #US45599219, October 2019). Software applications are now ubiquitous and power everything from our phones and laptops to the cars we drive, and these new applications require continuous updates. This explosion in software applications is producing an exponential increase in the overall application attack surface. Applications are now the favored attack vector for bad actors, who typically choose the path of least resistance. Hackers, cybercriminals, and nation states are increasingly exploiting vulnerabilities or application weaknesses as a means of entry into an organization and gaining access to corporate assets and confidential personally identifiable information (PII) data. They are doing this using readily accessible tools such as bots, Nmap, and Wireshark to locate applications with known vulnerabilities or susceptible code. And sometimes, access is gained through good old phishing attacks aimed at untrained or unaware employees. Virtually all these new applications will be cloud native and composed of multiple third-party and open source libraries. According to IDC's recent *U.S. DevOps Survey,* by 2021, some 25–34% of new applications will be composed of 30% third-party open source software. Further, the proliferation of sharing data via APIs is creating a growing collection of new potential ingress points for attackers. Increasing application vulnerabilities has led to an array of security tools used across diverse security domains provided by an assortment of vendors. Security complexity can cause application development and DevOps teams to suffer from information overload and a lack of visibility into their true security risk exposure. Organizations are being forced to string together a host of tools to reduce security exposure requiring in-house experts to sift through the results to uncover and prioritize security vulnerabilities. Overwhelming numbers of alerts and the lack of appropriate staffing can inevitably leave vulnerabilities unaddressed resulting in breaches to the organization.

This is essentially the problem that the ZeroNorth platform is designed to address. The company brings clarity to this problem by offering a risk-based approach to application security tool orchestration and management. Using a risk-based approach, ZeroNorth aims to help organizations secure their software products, integrate security into DevOps, and accelerate their application security programs while being able to assess the business impact of application security risks.

IN THIS VENDOR PROFILE

This IDC Vendor Profile provides a perspective on ZeroNorth and its SaaS-based DevOps application security automation platform. With increasing number of applications composed of multiple third-party and open source libraries, there has been a proliferation of security threats and new application security tools to find them. These tools all look at various aspects of security exposures and come from a variety of different vendors. This has added unintended complexity to application security and has caused DevOps teams adopting DevSecOps practices to struggle with too many different sources of security information generating a lack of overall visibility into the true security risk exposure. ZeroNorth is trying to bring clarity to this problem by offering a risk-based methodology to application security tool management.

SITUATION OVERVIEW

As DevOps and rapid application development practices have found their way into the enterprise, there has been a growing concern about how the increased speed of software delivery can cause application development teams to overlook security due diligence. Security has long been an obstacle and an impediment to the efficiency of the software development life cycle (SDLC). Those organizations that have recognized the critical nature of securing all their applications software across the entire development life cycle adopted a myriad of new security tools and DevSecOps practices. IDC defines DevSecOps as a methodology that asserts that security needs to be prioritized at the beginning and applied throughout the DevOps delivery pipeline.

This focus on application security has led to increased complexity and a cacophony of different DevSecOps tools across domains such as static application security testing (SAST), dynamic application security testing (DAST), software composition analysis (SCA), container scanning, and penetration testing. Often, however, weak coding practices or application vulnerabilities are missed, and the adversary finds a foothold into the targeted organization.

While DevSecOps security tools provide valuable insights, each tool focuses on a particular area; even within a specific security category, disparate vendors offer different strengths and insights. Some of the security findings turn out to be duplicates that are reported by multiple tools at various stages of the application life cycle. This makes it difficult for DevOps teams, who are generally not security experts, to effectively inject security and compliance into their DevOps pipelines.

In a recent IDC survey, 69% of DevOps teams indicated that security, compliance, and governance was still their top technology bottleneck (see *U.S. DevOps Survey of Large Enterprise Organizations, 2019,* IDC #US45688619, December 2019). So, despite the investments in modern security tools, DevOps teams are still struggling to get an accurate picture of their security risk exposure when releasing software updates.

Company Overview

Founded in April 2015, ZeroNorth provides a SaaS-based DevOps application security automation platform. In April 2019, the company received a $10 million Series A round of funding, and in August, John Worrall, former CMO at CyberArk, took over as CEO. In March 2020, the company obtained a second $10 million boost as part of a Series A+ funding round from ClearSky, Crosslink Capital, Rally Ventures, and Petrillo Capital. Most recently, ZeroNorth asserted a 300% ARR growth, two times growth in the company's customer base, and 300% growth in employee head count.

The ZeroNorth platform provides organizations with a risk-based approach to application security management. The platform orchestrates your application security scanning tools throughout the entire software life cycle and provides a continuous view of risk. Moreover, ZeroNorth normalizes scanning data into a common risk framework and dedupes and aggregates repetitive-related issues to minimize noise (such as false positives) and provide streamlined data to developers. Security configuration can be done centrally using policies within the ZeroNorth platform rather than across a collection of dissimilar tools.

This consolidated technique can reduce the resources required to implement a comprehensive software security program while giving organizations a more complete and consistent view of risk. Having a holistic, comprehensive view can ease reporting for corporate and board-level audits, regulatory compliance, and customer assurance as well as reduce the costs associated with managing disparate security tools. The ZeroNorth platform can be integrated into a DevOps CI/CD pipeline and used to schedule subordinate scans. This enables DevOps teams to proactively monitor and understand the risks posed to their software updates and digital infrastructures within their existing processes. This can also shorten the time DevOps teams spend trying to find and neutralize an identified security vulnerability and ultimately increase their development efficiency and ability to scale application security. Security thus becomes an enabling part of application development rather than the obstacle.

The key benefits of the ZeroNorth platform include:

- Optimization of investments in application security scanning tools
- Consistent, efficient application security scanning through orchestration
- Business-level metrics on application risk
- Contextual insights into application security vulnerabilities and risk
- Actionable, prioritized application scanning data for developers
- Integration of security into DevOps process workflows
- Reports and risk dashboards
- Overall, reduction of manual work and resources required to identify, correlate, and remediate vulnerabilities and understand risk

Company Strategy

The company's mission is "to provide security and risk leaders with innovation in application security orchestration and analytics that accelerates security, delivers continuous risk visibility, and powers secure digital transformation." Tying the corporate direction to digital transformation is timely, given the acceleration in this direction.

In 2019, the company clearly stated its strategic growth goals in press releases announcing Worrall as CEO and Karen Higgins as CFO. A seasoned CFO was formerly engaged with the start-up Resilient Systems, which ultimately was acquired by IBM, and Worrall states that she is "a perfect match for our team."

ZeroNorth claims that it is the first company to deliver risk-based application security management. Its platform aims to empower customers to rapidly scale application and infrastructure security while integrating seamlessly into developer environments to simplify and verify remediation. Both tenets are a clear depiction of the company's product strategy and align well with its corporate mission.

Further building out a senior leadership team, ZeroNorth hired Chris Riley in May 2020 as its SVP of Sales. In addition to Sales, Riley will lead the company's channel vision. IDC believes that ZeroNorth will continue direct engagement with its customers and build out strategic relationships with partners to gain access into verticals and customer segments not readily accessible to it. ZeroNorth continued to expand the company's leadership team in 2020 with the addition of Christian van den Branden as SVP of Engineering. Branden brings significant security and DevOps experience to the team; he was previously SVP of Product at Digital.ai and chief product officer at XebiaLabs.

FUTURE OUTLOOK

The future is bright for companies that truly provide visibility into security vulnerabilities and reduce workflow challenges for DevOps teams required to remediate security risks. Security teams struggle to keep pace with development, and historically, DevOps teams have neglected security to their peril. With disparate tools clouding the landscape, organizations have left themselves open to attack because of the lack of integration and scant visibility across hybrid environments. And the tools themselves have posed their own risks as well. IDC believes that ZeroNorth is well positioned in a critical intersection between development and security.

While ZeroNorth is the first to try and address application security risk and complexity using an autonomous approach not tethered to a specific security tool or platform, other larger competitors and global systems integrators (GSI) have also recognized this problem and are architecting their own solutions.

ESSENTIAL GUIDANCE

Organizations that are currently wrangling with DevSecOps or considering DevSecOps as a future state should consider the end-to-end application security and risk management capabilities the ZeroNorth platform offers. The platform provides a compelling value proposition to help DevOps teams optimize their DevSecOps effectiveness while improving velocity and reducing risk.

While the ZeroNorth platform concept addresses real problems and provides unique value, there are some areas that need to be considered. Furthermore:

- Although ZeroNorth has about 37 different technology integrations consisting of both commercial software vendors and open source solutions, use of the platform is largely constrained by the available integrations or ZeroNorth integration agents. ZeroNorth states that the company is continuing to add integrations to its portfolio on an ongoing basis. Data for unsupported security tools can be ingested using the company's generic endpoint or via JSON uploader. ZeroNorth can also support new integrations during the onboarding of a new customer or via a services arrangement.
- While ZeroNorth has been actively investing in out-of-the-box dashboards, some organizations still find that they need to create their own custom dashboards leveraging the available ZeroNorth APIs.
- While the platform integrates with tools such as Tenable and Qualys, the strength of the ZeroNorth platform is on the development side rather than runtime security operations. It is also important to understand that the ZeroNorth platform is not intended to be a security information and event management (SIEM) platform.

Advice for ZeroNorth

- Continue to build out cloud infrastructure visibility and management beyond AWS, Red Hat's OpenShift, and VMware to include Microsoft Azure and Google Cloud Platform (GCP).
- Continue to expand available integration agents and offer a software development kit (SDK) that can be used by partners and ISVs to build integration agents with the potential for creating a community of contributors.

- Consider partnerships with large security systems integrators and managed security service providers to further DevSecOps enablement for a broader set of customers and to increase awareness and revenue.
- Add dashboards for specific compliance areas such as PCI DSS (Payment Card Industry Data Security Standard).
- Remain tool and vendor independent and focused on innovation to fully exploit the company's first-mover advantage.

LEARN MORE

Related Research

- *Ongoing Demand Will Drive Solid Growth for Security Products and Services, According to New IDC Spending Guide* (IDC #prUS46773220, August 2020)
- *BT Announces Managed Security Services for Azure Sentinel* (IDC #lcUS46744720, July 2020)
- *Accenture Announces Strategic Relationship with Vodafone*, (IDC #lcUS46735620, July 2020)
- *Top Technologies for Cybersecurity Engineers* (IDC #US46648120, June 2020)
- *IT Vendors Step Back from Facial Recognition Software Considering Racial Inequity* (IDC #lcUS46610020, June 2020)
- *IDC TechBrief: Software Composition Analysis of Open Source Software* (IDC #US46133920, March 2020)
- *Developers: Driving the Future of Digital Innovation* (IDC #US45723719, January 2020)
- *U.S. DevOps Survey of Large Enterprise Organizations, 2019* (IDC #US45688619, December 2019)
- *IDC FutureScape: Worldwide IT Industry 2020 Predictions* (IDC #US45599219, October 2019)

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com