ZERONORTH™

The ZeroNorth™ Platform

Orchestrate Software and Infrastructure Risk Management from a Single Pane of Glass

Today every organization is in the software business. Software and the infrastructure it runs on are critical assets and continuous deployment is essential – but not at the expense of security. Traditionally, organizations rely on multiple scanning tools to identify vulnerabilities in different phases of development, deployment and operation. However, each tool classifies vulnerabilities differently, has its own console and requires a dedicated employee to manage it. Among the many challenges to this approach, it does not allow for a single, full-stack view of the constantly-changing risks inherent in continuous deployment. In addition, relying on disconnected tools becomes expensive and difficult to staff amid a widening talent gap in cybersecurity.

ZeroNorth™ transforms these manual and siloed efforts. The ZeroNorth platform accelerates and scales proactive software and infrastructure risk management by continuously orchestrating the discovery and remediation of vulnerabilities. Our "mission-control" orchestration platform enables organizations to construct and

manage an automated and consistent software security program. As a result, the platform directly provides board-level visibility into business risk, the assurance of better security, continuous proof of compliance and a more cost-effective risk management program.

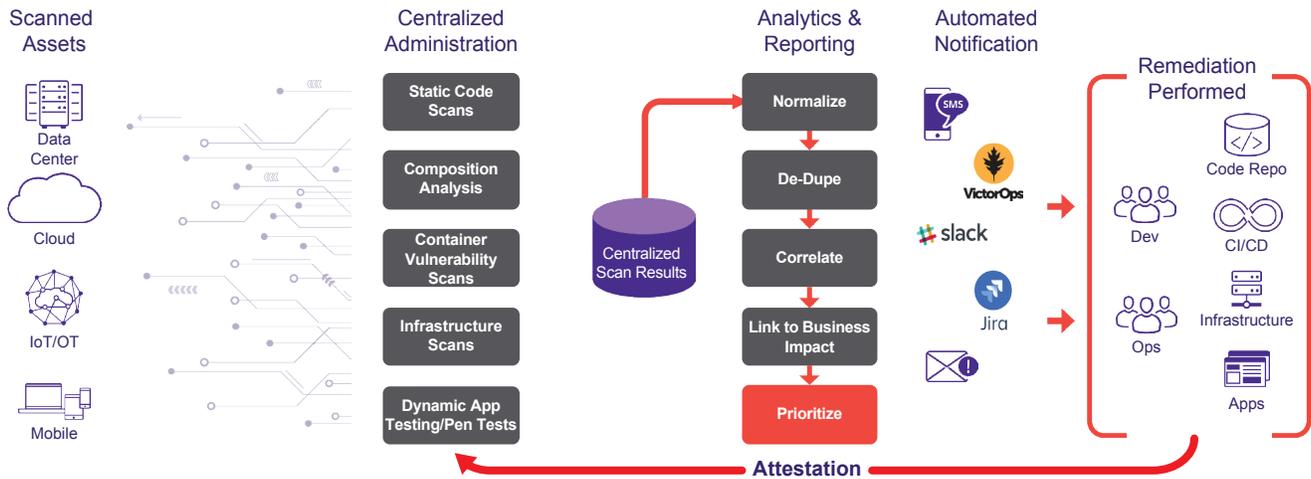## A Single View into the Application Security Lifecycle

ZeroNorth's adaptive policy-driven platform orchestrates and automates security testing from code commit to application delivery for complete visibility. By seamlessly and continuously weaving security into the application development process the ZeroNorth platform ensures security will no longer be an obstacle to development velocity.

Integrating with security and DevOps tools across the development lifecycle, ZeroNorth provides continuous visibility and assurance across all code repositories, application deployments and cloud infrastructure. ZeroNorth detects any changes and automatically adapts to elastic development environments and associated risk.

Working with Best-of-Breed Tools

Working with open source tools and commercial products, the ZeroNorth platform supports an organization's code and application security ecosystem across all levels of maturity. Through these integrations, ZeroNorth provides a 360-degree view across the application testing landscape, helping rationalize investments and understand the efficacy of current and future tools.

With ZeroNorth, organizations no longer need to rely on periodic point-in-time testing or limited visibility into the true risk of an application. ZeroNorth automates and orchestrates what many organizations address manually or through costly integrations and will continue to leave security out of step with development and the speed required for application delivery. The ZeroNorth platform also provides vulnerability assessment, notification and prioritization by polling the top threat and vulnerability feeds and correlating them with repositories and associated libraries and packages.

Scanned Assets
- Data Center
- Cloud
- IoT/OT
- Mobile

Centralized Administration
- Static Code Scans
- Composition Analysis
- Container Vulnerability Scans
- Infrastructure Scans
- Dynamic App Testing/Pen Tests

Centralized Scan Results

Analytics & Reporting
- Normalize
- De-Dupe
- Correlate
- Link to Business Impact
- Prioritize

Automated Notification
- SMS
- VictorOps
- slack
- Jira

Remediation Performed
- Dev
- Ops
- Code Repo
- CI/CD
- Infrastructure
- Apps

Attestation

With ZeroNorth, organizations have a closed-loop, "discovery and remediation" process across their organization.

How It Works

The ZeroNorth platform orchestrates and automates security testing across the software development lifecycle. The platform integrates with scanning tools to provide comprehensive visibility and software assurance across code, applications and infrastructures.

The platform rapidly creates exact replicas of code repositories and application environments, then aggressively scans for security vulnerabilities by containerizing and automating security solutions. Predictive analytics are applied to the consolidated security scan results providing proactive remediation through a single dashboard.

Current approaches to code and application security have been focused on disparate, vertical tools instead of unifying security and developers' needs across the horizontal CI/CD pipeline. Further, organizations require tools and visibility across on-premise, cloud and hybrid infrastructures. The ZeroNorth platform addresses both of these challenges by seamlessly integrating existing tools into the software development lifecycle, supports application security scanning regardless of environments and continually monitors infrastructures for new server and code instances.

The data derived from the orchestration and automation of the security tool chain is presented via ZeroNorth rich analytics. The correlated data provides an accurate, continuous view of security posture with critical risks prioritized and integrated into IT solutions to track and speed remediation. Additionally, Security Operation Centers are often overwhelmed with both responding to incidents as well as monitoring multiple threat feeds. ZeroNorth solves this by offering vulnerability analytics as a core part of the platform. The platform continually polls the CVE Details and NIST's National Vulnerability Database feeds and correlates with the target application to provide real-time alerts to the security team.

ZeroNorth enables a closed-loop "discovery and remediation" process across organizations because it seamlessly communicates remediation requirements with developers and operations and delivers automatic, scheduled attestation.

Easy to Configure and Manage for Complete Visibility

ZeroNorth is designed for fast set-up and management. Administrators can define testing policies in minutes and start seeing results immediately. ZeroNorth's intuitive user interface allows administrators to discover all code repositories across all environments and providers and integrate with notification services.

Once configured, administrators can create and automate policies to enforce scanning, scheduling and remediation. A company's entire security posture and key performance indicators can be viewed from ZeroNorth, as well as scan results, remediation plans, overall key metrics and real-time correlation of aggregated threat feeds from external sources.

If you are interested in learning more or seeing a demo, please contact us at **secure@zeronorth.io**