CSO
FROM IDG
April 29, 2020 www.csoonline.com

REVIEW

ZeroNorth orchestrates and tames enterprise scanner sprawl

The ZeroNorth platform makes scanners more effective and reduces cybersecurity fatigue by consolidating both scan results and fixes.

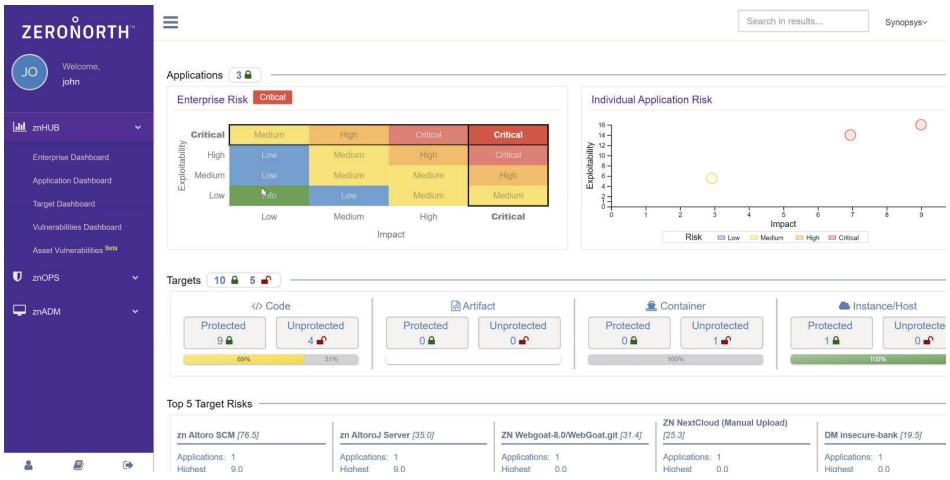
By John Breeden II

Almost every network these days will have one or more scanning tools designed to look for everything from malware and viruses to vulnerabilities inside developing code. They can be quite effective in that role and can improve detection rates, but they can also contribute to cybersecurity fatigue and force security teams to waste time chasing down false alarms.

The ZeroNorth platform brings various scanning tools together in one place so rules and preferences can be created globally and applied to whatever scanners an administrator wants to deploy. It's also adept at ingesting scan results from multiple sources and consolidating them into prioritized alerts. In our testing, ZeroNorth was able to take, on average, about 50 alerts generated by scanners and consolidate them down to just five or six problems that needed to be addressed. Fixing those core issues also eliminated the peripheral and overlapping problems.

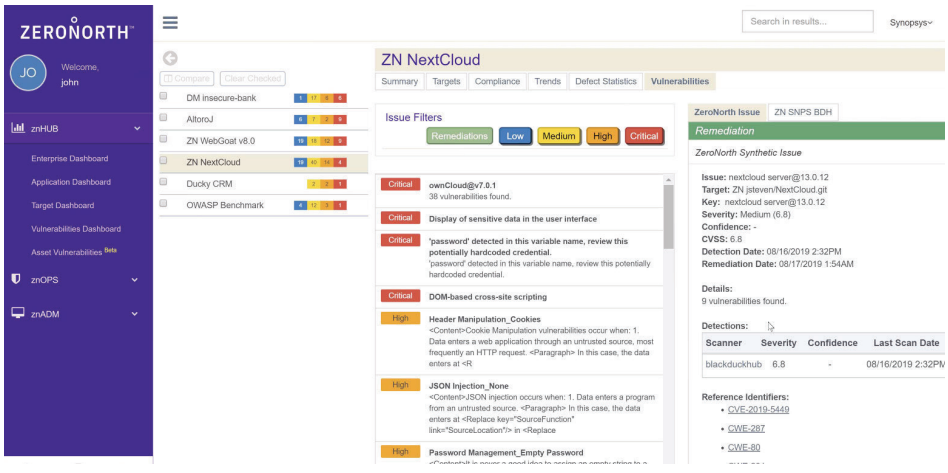
ZeroNorth is offered through a software as a service platform with users logging into the cloud-based portal to get reports and make changes to their scanning tools. A series of agents are needed to connect scanning tools to the platform, though the footprint within a protected network is extremely small given that ZeroNorth is using existing scanning programs. Extremely security conscious organizations can install the platform locally, though this is a special setup that the company does not normally implement.

Pricing for ZeroNorth is based on the number of entities scanned, which can include hardware elements like servers as well as virtual objects like containers within



CSO

When logging in, users are first taken to the main dashboard that shows the results and configurations of every scanning tool operating inside a protected network. The program can also be run "headless" using APIs and a console interface.



CSO

ZeroNorth tracks who created applications and who is responsible for them. When a problem is found by a scanner, ZeroNorth knows who should be notified so that it can quickly get worked on and fixed.

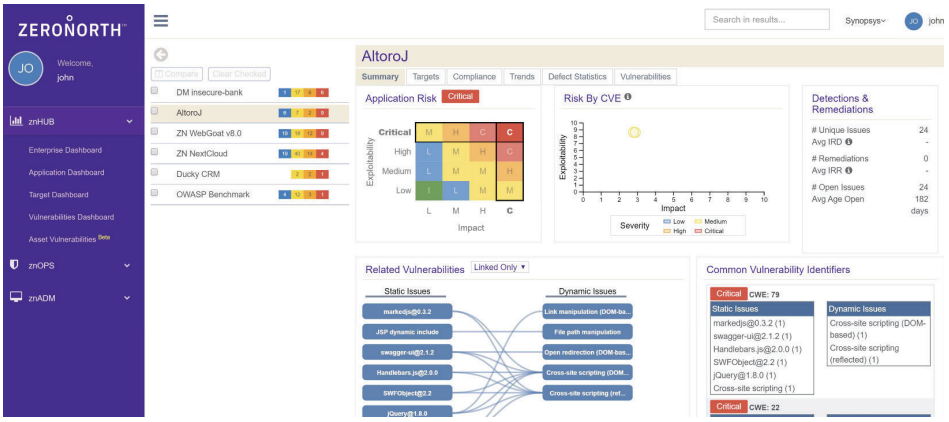
the cloud and also things like IP addresses.

The platform has a very nice user interface where everything is clickable, including consolidated alerts from scanners. And unlike security platforms that simply track event data like most security information and event management (SIEM) tools, ZeroNorth is able to track the ownership of applications or resources that are pegged by scanners as having security flaws or vulnerabilities. It can even be set to automatically notify those owners of scan results in addition to security teams. That way, people at an organization who are the most invested in fixing a specific problem can get to work on it right away.

Working with alerts

One of the most compelling reasons we found to invest in ZeroNorth is its ability to consolidate or compress alerts generated by individual or even multiple scanners. For example, ZeroNorth was able to look at a specific set of vulnerabilities found in a coding library. Scanners had identified almost 100 issues; ZeroNorth consolidated them and showed how specific vulnerabilities were related. By fixing one overall aspect of the vulnerability, we were able to clear 14 other specific alerts.

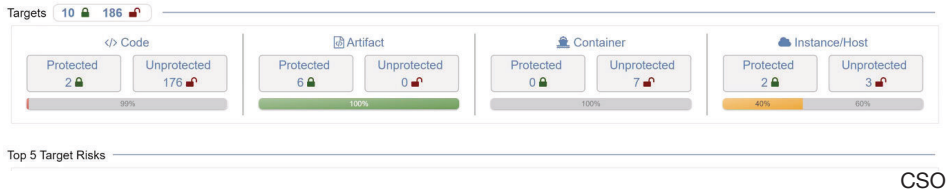
Because of this, ZeroNorth administrators are shown a list of consolidated alerts so that they can fix one thing and resolve multiple issues instead of wasting time patching related but individual problems. You can always drill down into alerts to see how they relate to one another, but you won't be inundated with overlapping alarms. This consolidation process worked with results that came from individual scanners as well as those flagged by multiple scan platforms. In our testing, the maximum number of alerts that were consolidated down into a single fix was 56, though it was common to see the compression of up to 20 problems at a time.



CSO

ZeroNorth can take the results from multiple scanning tools and consolidate the biggest threats to an enterprise network. Users can also tweak the logic used by ZeroNorth to favor or discount certain scanners in specific situations.

In addition to working directly with scan alerts, ZeroNorth provided a snapshot showing where and when problems within a test network were being caught and fixed. This would be especially helpful for organizations that are coding their own applications since the ZeroNorth report covers both the development and production environment. If the current set of scanning tools being used are weak in a specific area, such as not catching problems while apps are being developed or when vulnerabilities are hiding in containerized clouds, then it's probably a good idea to find a new scanner that can beef up security within that blind spot.



CSO

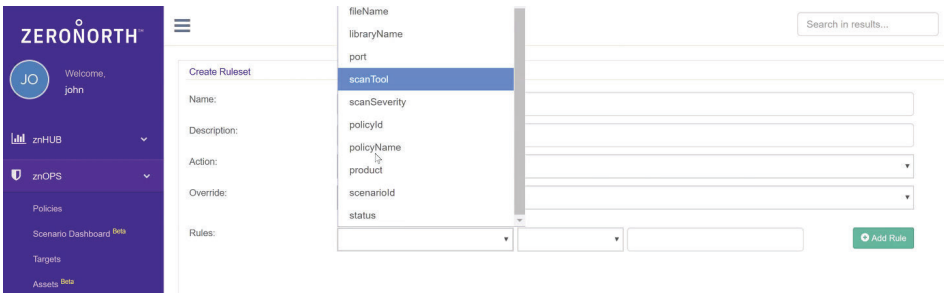
This section shows where various scanners are catching problems. In this example from the test network, almost nothing is being caught while application code is being written to the so-called left side of the software development process. Armed with this information, administrators could bring in a new scan tool designed for developers and then use ZeroNorth to test its effectiveness.

Adding new scanners

ZeroNorth makes it very easy to add new scanners to a network. The platform comes with a whole set of open source scanners that can be activated right from the user interface. For example, if you are not getting good scans in your containerized environment, you can add the Docker Content Trust program. If you want to look for vulnerabilities in open source software, you can install Black Duck Hub.

You have two options for adding new scanners. The first is to install them inside the local environment. ZeroNorth will work with users and its platform's agents to automatically provision scanners and get them up and running. The second option is to run a scanner from the ZeroNorth cloud. This is an interesting configuration because ZeroNorth does not currently charge for this service but is willing to support the infrastructure for their customers' new scanning tools. In either case, once installed, you can use ZeroNorth to configure the scanners and monitor their results.

In addition to open source scanning tools, some commercial scanner offerings are available. The only difference is that users will need to purchase and provide a license from those companies to make use of a commercial scanner. With either open source or

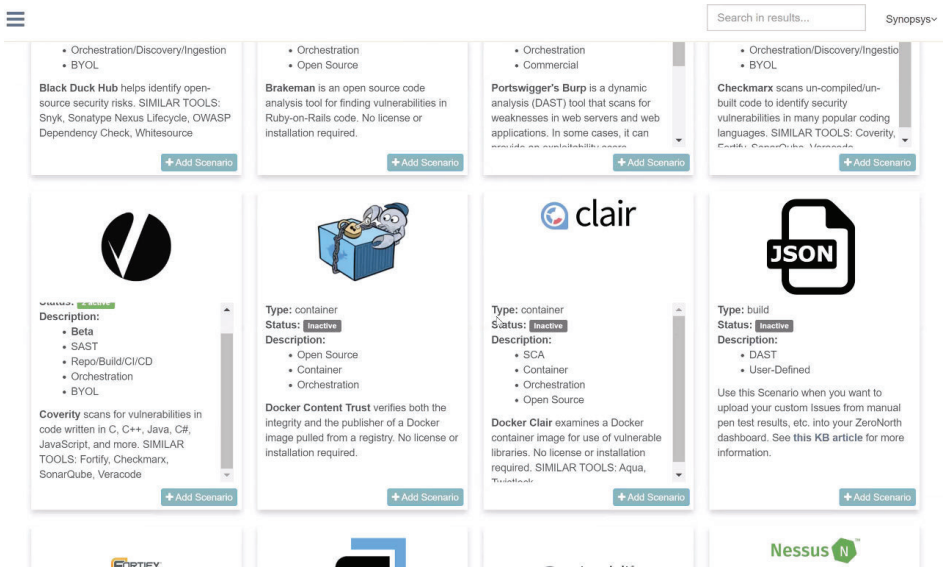


CSO

Most scanning tools allow users to configure policies regarding how they operate. But ZeroNorth can act as a repository for all rules from all scanners, which eliminates the dependency on specific vendors. This also allows users to easily swap out scanning tools.

commercial tools, ZeroNorth can be used to push out global rules and consolidate scan results. And because rules are kept inside the ZeroNorth platform, it eliminates vendor lock-in. If you don't like a scanning tool or aren't getting good results, it's easy to swap it out for another without losing a lot of time spent with individual configurations.

Once you have the new scanner tools in place, you can go back to the ZeroNorth dashboard and see if those previously discovered blind spots have been eliminated. Software developers could theoretically use ZeroNorth to install scan tools to help shift security toward the so-called left side of the development pipeline.



CSO

The ZeroNorth platform makes it easy to add new scanning tools. Several open source scanners are available from the main interface. They can be installed in the local environment or run from the ZeroNorth cloud.

The bottom line

Every organization uses scanners these days. They are practically ubiquitous cybersecurity elements in most networks. But with numerous scanners pinging multiple results to overworked security personnel, they quickly lose both their value and reputation. ZeroNorth can help by not only consolidating both scan results and fixes, but by evaluating the tools themselves to make sure they are doing their jobs and not ignoring critical sections of the enterprise environment. ZeroNorth would be a highly valuable addition for any organization trying to tame the deluge of scanner sprawl, or to improve their scanning accuracy with either new policies or tools.