[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@179f4f4a545c42339b6997e31046a8f7?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view#main)

Reference <https://www.rapid7.com/blog/post/2018/01/11/the-4-big-differences-between-network-security-and-web-application-security/>

**The 4 Big Differences Between Network Security and Web Application Security**

* Jan 11, 2018
* [Alfred Chung](https://www.rapid7.com/blog/author/alfred-chung/)

Tomato, tom*ato*, potato, pot*ato*, network security and [web application security](https://www.rapid7.com/solutions/application-security/). Two things that may seem similar, they are actually quite different. Network security (also known as vulnerability assessment or [vulnerability management](https://www.rapid7.com/solutions/vulnerability-management/)) has been around for quite some time and is something most security practitioners today know well. Web application security, however, is still not widely understood and has many scratching their heads.

While both seek out weaknesses in a company’s security posture, there are important differences you should know. Network security should lie at the heart of pretty much every [security program](https://www.rapid7.com/fundamentals/security-program-basics/). However, companies that develop and manage their own web applications, or for their customers, need to approach security in a slightly different manner. This is where application security comes in.

In this post, we’ll explain the main differences between network security and web application security and why you need both for a multi-layered and comprehensive vulnerability management program.

**It starts with CVEs and CWEs**

Chances are, if you’re trained in network security or vulnerability assessment, you use a CVE, or Common Vulnerabilities and Exposures list. CVEs are a list of known issues that can lie at the network, operating system, or software layer. If found by your security tool, they should be removed in due time. This is great when it comes to spotting concrete, known, and documented issues within your infrastructure, but what about unknown issues and behaviors? This is where CWEs, or Common Weakness Enumeration, are most useful.

Especially when it comes to dynamic application security testing, or DAST ([a practice we recommend](https://information.rapid7.com/dast-is-anything-but-static.html)), CWEs can be used to spot behaviors at the application layer that appear to be vulnerabilities based on a community-generated list of the latest security weaknesses. You see, most applications reside on the internet where they’re much more likely to be exposed to the latest threats, so in order to protect your apps, you need to look at security differently, which is where CWEs come in. CWEs offer security pros a common baseline standard from which to identify, mitigate, and prevent potential application security issues.

To be effective at securing your web applications, you need to be able to detect both the known and the unknown, which is why CVEs alone are not enough and why CWEs must be leveraged, too.

**Know what you are scanning**

Another big difference that determines when it’s better to use network security versus web application security is the surface area that you’re scanning. Network security tools are designed to scan infrastructure like networks and application security tools are designed to scan… well... applications. Like trying to fit a square peg in a round hole, one is not like the other. Many security teams, when they begin to learn the basics of application security, attempt to monitor their applications with a network security tool only to find out later on that certain issues weren’t caught due to the nature of what needed to be scanned and how it needed to be scanned.

DAST solutions like [InsightAppSec](https://www.rapid7.com/products/insightappsec/) are designed for the dynamic nature of today’s web applications, able to look for unknown threats like zero-day, whereas tools like [InsightVM](https://www.rapid7.com/products/insightvm/) are built to look for vulnerabilities and known threats. This is why it’s important to have both tools on hand and to make sure you’re using each in the right way.

**Consistent versus dynamic environments**

Infrastructure like networks and operating systems, generally speaking, are static and consistent in nature. Built with similar standards in mind, they generally function the same. Not only that, but since most are internal, they’re typically protected from the security issues we find on the internet, meaning vulnerabilities don’t evolve as rapidly. This makes it easier to report, share, and detect vulnerabilities as a community. This, again, is where CVEs come in.

Applications, on the other hand, can be built on everything from Ruby on Rails, to node.js and html. Because systems and code can look and operate differently depending on how and where they were built, [web application security scanning](https://www.rapid7.com/fundamentals/web-application-security/) needs to be done differently. A feature within our dynamic application security solution InsightAppSec called [Universal Translator](https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7-insightappsec-appspider-feature-brief-universal-translator.pdf) does just this. Leveraging advanced testing scripts, it can cover any type of application, old and new alike, with out-of-the-box functionality.

Using a solution built for the type of infrastructure and applications you have, you can be sure you’re catching both every day and net-new issues. That’s why having tools like InsightAppSec and InsightVM in your toolbox can save you a great deal of time, as they’re designed to accommodate a large range of technologies, vulnerabilities, and complexities.

**Addressing traditional vs. web-based threats**

[Web application attacks](https://www.rapid7.com/fundamentals/web-application-vulnerabilities/) are the #1 source of breaches today according to the Verizon Data Breach Report because most every app is exposed to the internet where potent security vulnerabilities lurk. This has led to application security being the [fastest growing segment in the security space](https://www.gartner.com/doc/3780266/forecast-information-security-worldwide-), and no company with a web application should be without it today.

While network security is ideal for detecting known vulnerabilities on the network, to keep pace with today’s web-based threats, companies with web applications need the ability to detect and address issues within the application. However, what often holds back security pros today is a lack of know-how about what to do with the results of a web application security scan. While solutions like InsightAppSec make this as straightforward as possible, for teams that don’t have the resources internally to run a tool like InsightAppSec and then act on the results, Rapid7 offers a [managed application security service](https://www.rapid7.com/services/vulnerability-management-services/managed-appsec/) to run scans and prioritize the issues for you. Because application security simply cannot be ignored today, it’s important you dedicate personnel to this big and growing area of security — whether it’s internal or external.

**A look ahead at the state of security**

Application security is a hot and growing field of focus, but it is still quite new for most security teams, unlike its counterpart, network security. Today, we’re already faced with a massive security talent gap that is only continuing to grow. This means that not only are companies having trouble keeping up with basic security hygiene due to this shortage, but they’re unable to capitalize on new security needs, like application security. Here at Rapid7, it’s our aim to make [application security testing](https://www.rapid7.com/fundamentals/web-application-security-testing/) available to everyone. Intuitive and deployed in the cloud, [InsightAppSec](https://www.rapid7.com/products/insightappsec/) walks you through the entire process from setup to scanning so that even if you don’t have an application security background, you can benefit from it just the same.