# Layer Your Security Defense with Real-Time Application Self-Protection

Is your security program able to address today's most relevant threats? Network security has been the focus, but attackers are shifting their efforts toward applications.

**Insight:**

84 percent of breaches target the application (Gartner 2014)

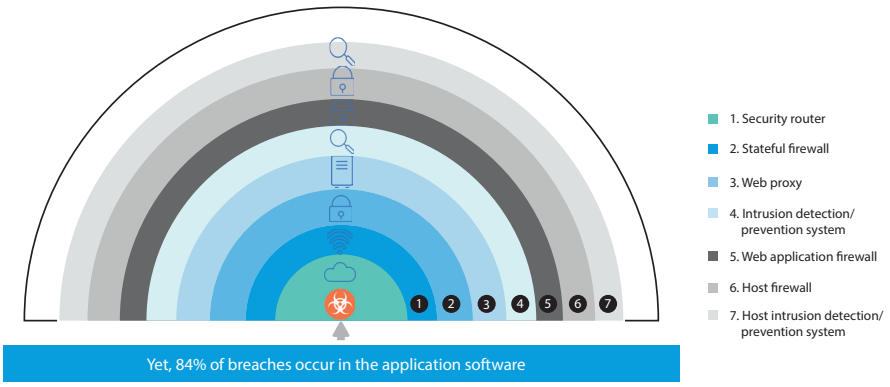


**Figure 1.** Network security accounts for the majority of security technology spending

## How Do You Affect This Shift without Breaking the Bank?

### Focus on Application Security via SaaS

The best practice is to make application security an integral part of your software development lifecycle. A key step in this practice is to scan your applications for vulnerabilities and fix what is identified. Micro Focus® Fortify on Demand allows you to accomplish this without capital outlay. Your team uploads the application code, Fortify scans it, provides a report with precise feedback on the severity of each vulnerability along with where and how to correct them.

### Avoid Panaceas

It may not be practical to fix every application due to resources, time-to-market, or investment priorities. And with the growing use of cloud applications, you may not have access to the code. In order to protect existing vulnerabilities in production applications, a popular practice is to monitor the network traffic and try to interpret what is happening within the application using tools such as Web application firewalls (WAFs). These approaches excel at detecting network-based attacks such as Distributed Denial of Service (DDoS) and can sometimes see first-order SQL injections, but they fall short at detecting more sophisticated application-based attacks.


**Figure 2.** Partner with a market leader

**Micro Focus is a leading provider of application security and has leveraged proven technologies for Application Defender.**

Gartner once again named Fortify a leader in the Magic Quadrant for Application Security Testing in 2017.

Fortify, the most broadly adopted SAST tool in the market, continues to deliver compelling innovations with DAST, IAST, and RASP technologies.

2017 Gartner Magic Quadrant for Application Security Testing

To learn more about Micro Focus Application Security, visit:
**www.microfocus.com/appsecurity**

### The Right Tool for the Job—Protect Deployed Applications with RASP

Runtime application self-protection (RASP) is a security technology that is capable of detecting and preventing real-time attacks. To protect deployed software, Application Defender offers application self-protection that quickly and easily defends software vulnerabilities in production software. By seeing everything the application sees, Application Defender can protect your applications from targeted, often more damaging second-order SQL injections and other sophisticated attacks, which helps you manage risks to which network security, even WAFs, would be blind.

## Where to Get "Bang for Your Buck"

There are many scenarios where Application Defender can simplify application protection.

- Do you have applications that are business critical but are either too complex, too fragile, or ill supported to risk changing the code to remove security flaws?
- How about applications that are not business critical, but with known flaws that could be points of entry for an attacker to reach more business-critical environments or personally identifiable data?
- A lack of developer resources may have your enterprise buried in a backlog of application changes. What do you do in the meantime?
- What about end-of-life applications? You don't want to "waste" precious resources to remediate code that will soon be retired. But how do you defend known (or even unknown) vulnerabilities while it is still being used?
- Are you just beginning your application security program and need protection for key applications, while you ramp your scanning and testing capabilities?
- Do you have a mature application security program but need to provide more information to the developers, so their remediation efforts can be more efficient and effective?
- For all of these reasons and more, Application Defender can help you defend your applications either as a permanent solution or as an immediate "fix."

## Reduce Risk with an Established Technology

### Real-Time Detection and Protection

Application Defender provides compliance and risk reduction through continuous monitoring of production applications. But it goes a step further in that it can also take action and stop threats real time. Application Defender distinguishes between an actual attack and a legitimate request and protects production applications from zero-day threats. Why wait for a security analyst to review a suspicious issue or for application development to remediate code? Let Application Defender stop threats before they can do damage or extract critical information.

Contact us at:
**www.microfocus.com**

### Rely on Proven Technology

With Application Defender, the capabilities to identify and stop attacks on production applications are simplified with pre-configured rules and with deployment and management through the cloud. Application Defender has robust application security with 31 protection rule categories against application security attacks, exploit attempts and other security violations such as SQL injection, cross-site scripting, and privacy violation. Application Defender has logging visibility for Java or .NET web apps, and can remediate vulnerabilities faster with line-of-code detail for developers.

### A Simplified Approach

With Application Defender, you can get started in minutes with run-time application self-protection (RASP). Application Defender does not require that you change production code nor recompile in order to protect it. Unlike WAF, there is no training necessary. You can augment or replace your WAF with always-on protection against both the vulnerabilities you know about, and the ones you don't.

### Easily Scale without Capital Expenditure

Application Defender is available On-Premise, as a Service, or as Hybrid so you can start quickly and scale as needed.

### Learn More At

**https://software.microfocus.com/en-us/software/application-defender**