Flyer
Security

Application Self-Protection Made Simple

Run-time application self-protection monitors production applications and prevents attacks, stopping threats that alternative technologies cannot even see. Using proven technology, it accurately monitors threats from within the run-time environment, using a prescribed response that you control.

Benefits

- Easy to install and manage
- Point-wise control
- Proven run-time technology
- Minimal performance impact
- Robust back-end architecture
- Secure communication to the cloud
- No code changes, no recompile

The Micro Focus Application Defender Solution

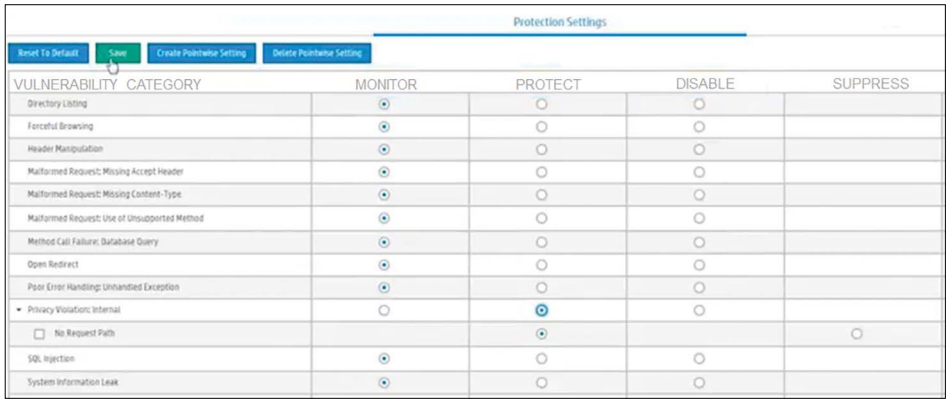

Figure 1. Predictive Settings

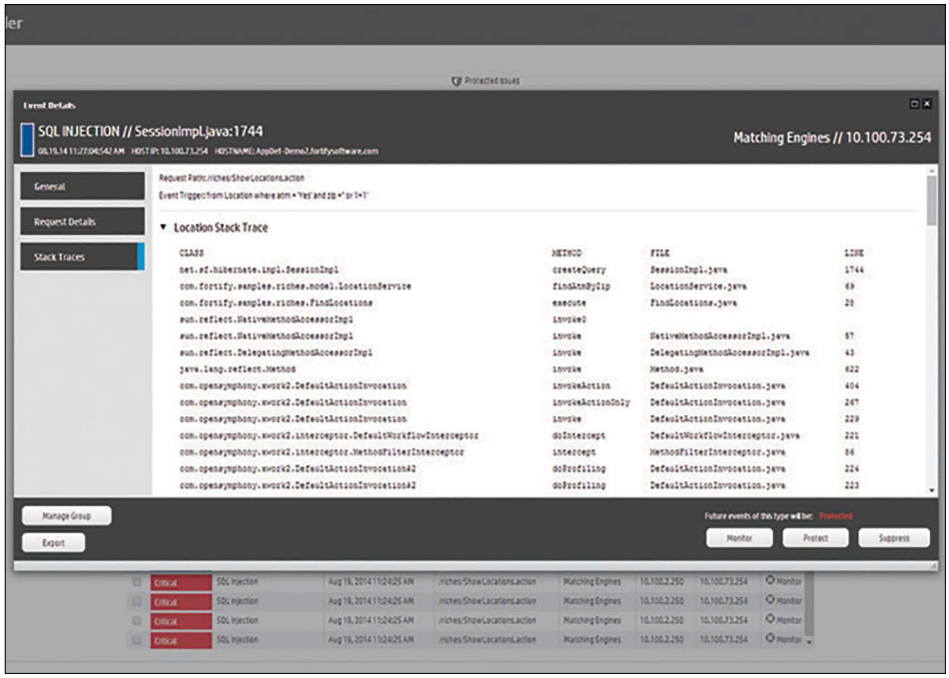

Figure 2. SQL Injection

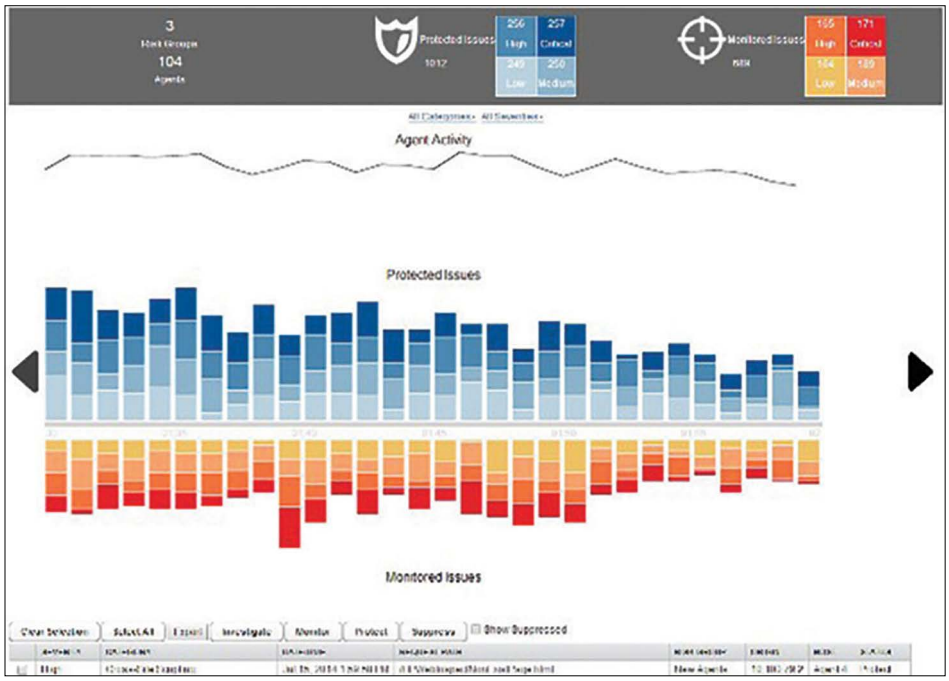

Figure 3. Visualization

A New Kind of Defense with Application Self-Protection

Micro Focus® Application Defender is application self-protection made easy. Managed from the cloud, and pre-configured, the self-protection SaaS offer enables you to defend, in minutes, new and existing software vulnerabilities in production software. Without waiting to change the application's code, you can immediately stop attacks. And with more accurate contextual insight from within the application itself, you can confidently identify and remediate attacks that network security would not see.

Because Application Defender can see everything the application sees, it can analyze actions made by users, data anomalies, and logic flow to distinguish between an actual attack and a legitimate request. Examples of attacks that might otherwise go undetected include cross-site scripting, injection attacks, and sensitive data capture. The full context of malicious activity is understood, and precise action is taken immediately when an attack is identified. Rule packs are pre-configured, and the response taken is flexible and within your control.

Permanent Application Security Defense or an Immediate "Fix"

Today over 80 percent of successful security breaches target application software. Application Defender protects production applications, third-party and in-house, and can be used as either a permanent solution or for immediate protection. Because it fills such a crucial need, Gartner expects the run-time application self-protection category to gain increasing adoption with the prediction that "By 2020, 25% of application run-time environments will have built-in self-protection capabilities."[1]

How It Works

Immediate Protection

If a new threat arises, unforeseen during application testing, or if a known vulnerability is released into production, the production application can be immediately protected. A simple three-step deployment process and pre-configured rules allow you to begin monitoring and protecting production applications in minutes. The central cloud-based administration portal makes it easy to deploy and manage Application Defender throughout your enterprise no matter the scale.

Software-as-a-Service

The Application Defender SaaS solution is a "software-as-a-service" application self-protection solution consisting of two parts:

1. Cloud-based management platform with an interactive dashboard for deployment, management, reporting, and threat management.
2. The proven Micro Focus Security Fortify run-time technology, installed in the application run-time environment, to monitor and protect the associated application in real time.

Simple Deployment

Both parts are seamlessly integrated. You can get started in minutes with three easy steps:

1. **Initiate—**download Application Defender into your Java or .NET application environment

1 *Runtime Application Self-Protection: A Must-Have, Emerging Security Technology, Gartner research G00229122, J.Feiman, 19 May 2014.*

2. **Verify results**—through a simple, cloud-based user interface
3. **Protect**—automatically protect your production applications

Operational Considerations

Easy to Manage

Application Defender is not only easy to install but easy to manage. Agents are grouped into "risk groups" to simplify protection of applications with similar risk profiles. Newly deployed agents are put into a default risk group, which is always set to "monitor." You choose how to group your agents, moving them to the desired risk group using one click. Protection settings (monitor, protect, suppress) apply to the entire risk group, but more granular point-wise protections can be set providing a different response to a specific threat.

Proven Technology

Micro Focus has been using run-time analysis technology for some time now (see Runtime Application Self-Protection: A Must-Have, Emerging Security Technology, Gartner research G00229122, J.Feiman, 19 May 2014). The same run-time technology is used in Micro Focus WebInspect and Micro Focus ArcSight Application View. This proven technology assesses calls to common core libraries. It does not change the application's code nor does it require a recompile.

Minimal Performance Impact

Understanding the performance impact created by a new solution brought in the production environment is invaluable. Application Defender protects applications by monitoring dangerous function calls and validating the corresponding function arguments. These protection guards are triggered only when necessary and most of the guards do not hold any internal states. Because of this, the execution time and memory overhead are low.

In order to measure the performance overhead caused by Application Defender, we tested the application self-protection solution on a well-used open source enterprise automation software. The goal of the test was to determine performance overhead impact on the test application from Application Defender, measuring performance impact on executing time and memory consumption. Our performance lab results show 3.5 percent impact on application response time on average and memory overhead is about two percent.

Java performance white paper
.NET performance white paper
Micro Focus also offers on-premises options. Contact your account manager for more information

Robust Back-End Architecture

Application Defender was designed with a robust back-end architecture to maintain the performance of cloud-based functions as it scales. Architecture goals included:

- Web scale
- Horizontally scalable at each layer
- Distributed compute
- Real-time stream processing/complex event processing
- Reprocessing of event stream
- Post-stream analytics

The resulting Application Defender architecture uses clusters at the Web edge, distributed commit log clusters, distributed real-time compute clusters, and Vertica analytics clusters.

Secure Communication to the Cloud

To provide secure communication between the Application Defender agents and the Web-based management console, secure command/event channel port 443 is used and vulnerability data is encrypted.

Unintrusive Monitoring

The run-time agent is installed in the run-time production environment. However, it requires no code changes and no recompile. Application Defender leverages the existing capabilities of Java and .NET to monitor the application for malicious activity. When the agent is initially deployed, the program must be restarted and then restarted again only when agent binary or protection rule pack updates are installed.

Contact us at:
www.microfocus.com

Like what you read? Share it.

Using Application Defender to protect end-of-life applications where you want to minimize changes, or to protect complex/mission-critical applications, can be a way to reduce the changes required (from coding) while affording instant protection for new and existing threats in a minimally invasive way.

Learn more at
www.microfocus.com/rasp