MICRO FOCUS

Data Sheet
Security

Security Fortify Application Defender

See threats to your application's security. Micro Focus® Security Fortify Application Defender is a runtime application self-protection (RASP) solution that helps you manage and mitigate risk from homegrown or third-party applications. It provides centralized visibility into application use and abuse while protecting from software vulnerability exploits and other violations in real time.

Product Highlights

Without changing your application's source code, you can quickly instrument your apps to immediately and consistently report to security operations activity on applications and their users, at enterprise scale, without creating custom log parsers. In real time, Application Defender accurately detects and safely prevents exploits of software vulnerabilities in Java and .NET applications while providing line-of-code vulnerability details to accelerate remediation. The application self-protection solution—available both "as a service" and "on-premise"—is based on mature Security Fortify runtime technology.

Application Defender quickly instruments applications to capture application and user activity logs. It also detects and stops attacks across

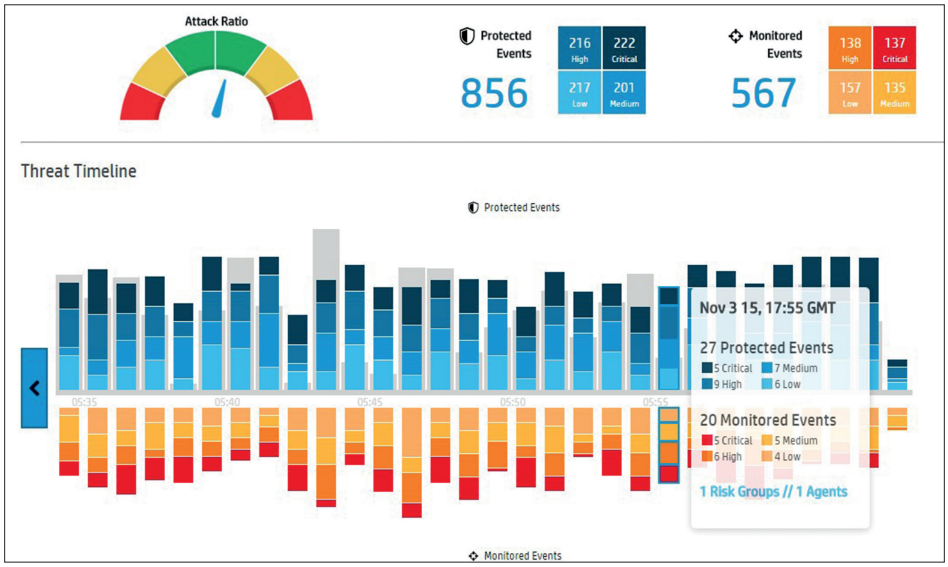

Figure 1. Accurately identify and instantly defend against threats to production applications

Key Features

- Consistent and systematic logging of application activity without editing code nor recompiling
- Real-time protection from known and unknown vulnerabilities with a click of a button
- Flexible event output in industry-standard formats for visualization, analysis, and alerting in any SIEM or log management solution
- Event details with fully reconstructed attack strings and line-of-code details for efficient triage and remediation
- Configurable alerting and reporting for risk prioritization and communication across the organization
- Mature, proven runtime application self-protection (RASP) technology
- When you perform security testing with Fortify on Demand, many of the vulnerabilities can be protected seamlessly with the click of a button without leaving FoD

dozens of vulnerability categories such as SQL injection (SQLi) and cross-site scripting. Both logging and exploiting data can be provided to security information and event management (SIEM) or log management for compliance and broader application security visibility. Contextual insight from within the application data flows and execution logic enables visibility of fully reconstructed malicious queries, allowing Application Defender to identify and stop attacks confidently, including those that network-based security cannot see.

Key Benefits

Visibility

- Instantly see software vulnerability exploits in production applications and continuously monitor actual attacks to pinpoint vulnerabilities for protection or remediation.
- Get automatic and consistent visibility into the activity of applications and their users.
- Send log data to your SIEM or any log manager for compliance, correlation, visualization, analysis, and alerting even if your app was not instrumented to create a log.
- Remediate vulnerabilities faster with line-of-code detail for developers.

Protection

- Detect and protect, in real time, known and unknown application security vulnerabilities at enterprise scale, without the need to alter or recompile source.
- Stop attacks invisible to network-based security solutions.
- Accurately distinguish between an actual attack and a legitimate request.
- Reduce the risk of false negatives via robust scope of coverage.
- Protect from zero days in homegrown or commercial applications or their underlying platforms.

Simplicity

- Deploy as you wish: on-premise or software as a service (SaaS).
- Protect an application quickly and easily in minutes with simplified installation and pre-configured vulnerability detection rules.
- Protect vulnerabilities discovered in Fortify on Demand (FoD) with a click of a button.
- Efficiently manage, report, and scale.

Why Use Application Self-Protection?

- **Centralized and configurable visibility into application use and abuse:** Applications continue to be a popular target for cyber-attacks, but often a Security Operations Center (SOC) lacks visibility into an application's behavior and exploits. Using Application Defender, you can instrument applications, even if they are not developed to create logs. Without changing source code, you can send log and exploit events to any SIEM or log manager for greater visibility.
- **Mitigating control for vulnerable homegrown or third-party applications:** Security teams have begun to shift their focus and budgets to address application security. But limited resources and new vulnerabilities continue to be a challenge. With Application Defender, if a new vulnerability arises, unforeseen during application testing, or if a known vulnerability is moved into production, the production application can be immediately protected. This protection can remain in place until the vulnerability is remediated—or indefinitely—in the case of legacy or third-party applications. There are several cases where mitigating control is needed:
  - Apps with more vulnerabilities than resources or time to fix
  - Third-party or legacy applications where you cannot remediate the underlying vulnerability
  - Zero-day vulnerabilities in applications or underlying platforms
- **Simple deployment and use:** The Security Fortify Application Defender solution makes it easy to deploy, configure, and manage agents, as well as application security policies throughout your enterprise no matter the scale. The proven Security Fortify runtime technology is installed in the application's runtime environment to monitor and protect the associated application in real time. Centralized management and analytics enable rapidly scalable deployments of additional agents across any Java or .NET application.
- **Defense in depth:** Network security remains an important layer of defense, but signature-based defenses rely on filters, inference, and statistics to look for known exploits. For example, an attacker can still exploit an SQLi vulnerability by changing the encoding for the malicious query. Network and perimeter defenses may only see parts of the malicious query if at all.

  Only within the application is the entire query constructed into its fully executable form. Because Application Defender can see the application program flow and attempted usage in real time, it can analyze requests made by users to distinguish between an actual attack and a legitimate request, greatly improving the accuracy of the application self-protection solution. And, the response taken is specific for the attack and within your control, so non-malicious activity is not impacted while attacks are stopped in real time.

Key Features

- Consistent and systematic logging of application activity without editing code nor recompiling
- Real-time protection from known and unknown vulnerabilities with a click of a button
- Flexible event output in industry-standard formats for visualization, analysis, and alerting in any SIEM or log management solution
- Event details with fully reconstructed attack strings and line-of-code details for efficient triage and remediation
- Configurable alerting and reporting for risk prioritization and communication across the organization
- Mature, proven runtime application self-protection (RASP) technology
- When you perform security testing with Fortify on Demand, many of the vulnerabilities can be protected seamlessly with the click of a button without leaving FoD

Why Security Fortify Application Defender?

- Proven application self-protection technology from an application security leader (Gartner MQ)
- End-to-end application security capabilities with integration across tools
- Comprehensive vulnerability categories backed by industry leading security research
- Thorough and accurate insight from within the application immediately available
- Policy management at the agent (not dependent upon a cloud connection to execute policy)
- Flexible deployment: on-premise or as a service

About Security Fortify

Security Fortify offers the most comprehensive static and dynamic application security testing technologies, along with runtime application monitoring and protection, backed by industry-leading security research. Solutions can be deployed in-house or as a service to build a scalable, nimble Software Security Assurance program that meets the evolving needs of today's IT organizations.

Learn More At
https://software.microfocus.com/en-us/products/application-defender/overview

Contact us at:
www.microfocus.com