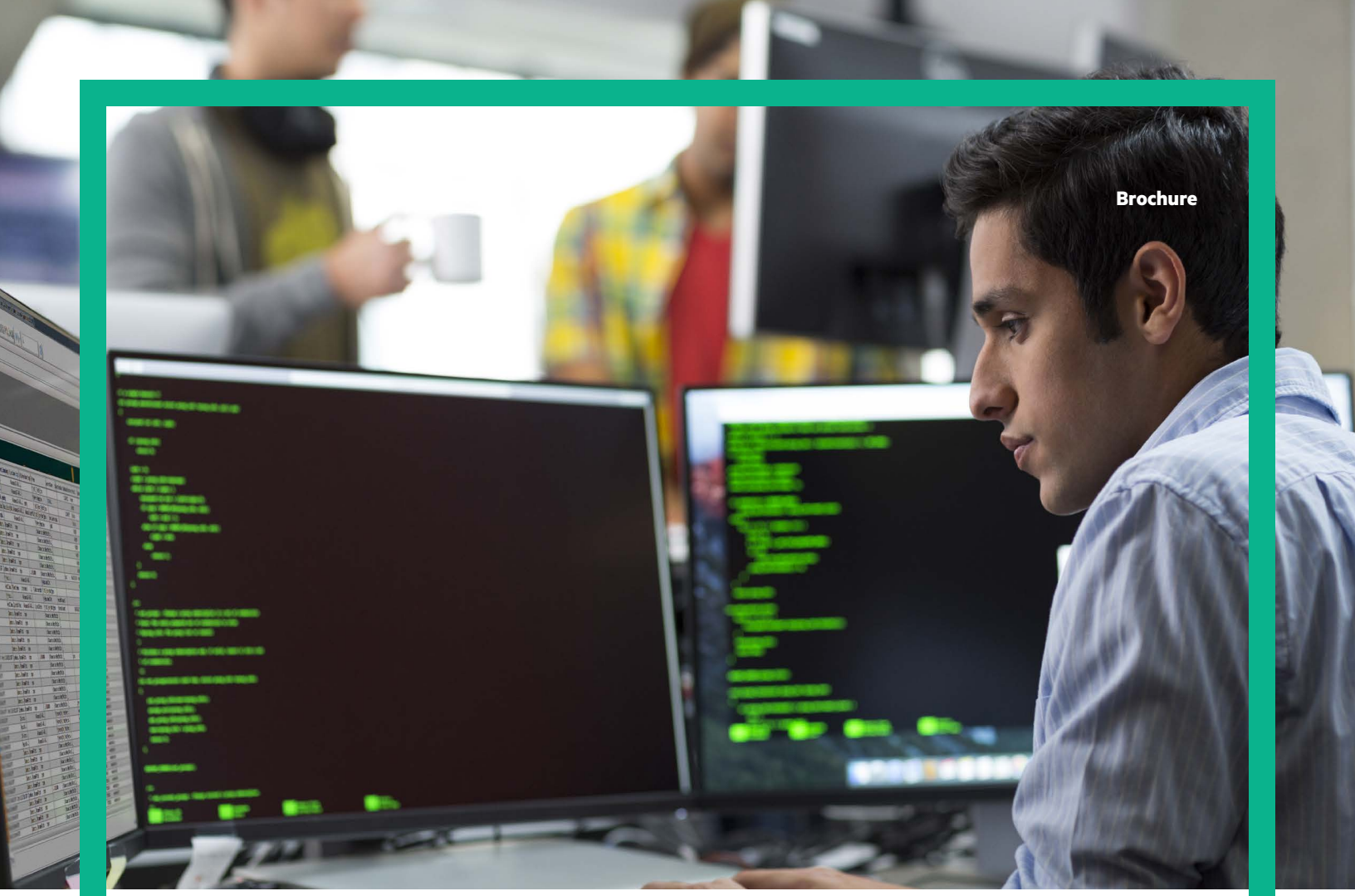

Continuously discover and eliminate security risk in production applications

Hewlett Packard
Enterprise

Continuous Application Monitoring

HPE Security Fortify on Demand

The first step in any application security initiative is to understand where your risk exposure is, particularly in live production environments that may already be vulnerable. While organizations are increasingly addressing security as part of the development process, they struggle to get security visibility into their externally facing apps in production. Network vulnerability assessment and monitoring programs give no actionable insight into application layer vulnerabilities and suffer from the noise of inaccurate signature-based scanning. Finding vulnerabilities during development is essential to securing applications long term, but does little to save the company from attacks targeting live legacy applications today. It is now an imperative to continuously monitor and protect production environments for application security risks from new or rogue applications, risk profile changes, and zero-day vulnerabilities.

Find and protect applications without slowing application delivery

The HPE Security Fortify on Demand Continuous Application Monitoring Service can help close the gap between application deployment and security by combining application discovery with continuous dynamic vulnerability scanning, risk profiling, and runtime protection in a subscription service that provides visibility and insight into the risk facing customers' public web application portfolio. The automated discovery scans identify new external-facing applications on a monthly basis and results are presented in a risk-ranked list with confidence scores. Confirmed applications can then be enrolled in fast, production-safe, continuous vulnerability, and risk profile scanning. Based on scan findings and business factors, deeper dynamic analysis and runtime protection can be added for critical applications. Continuous application monitoring serves as both an ideal first step in launching a software security assurance program and as a complement to dynamic and static testing of applications once they are deployed.

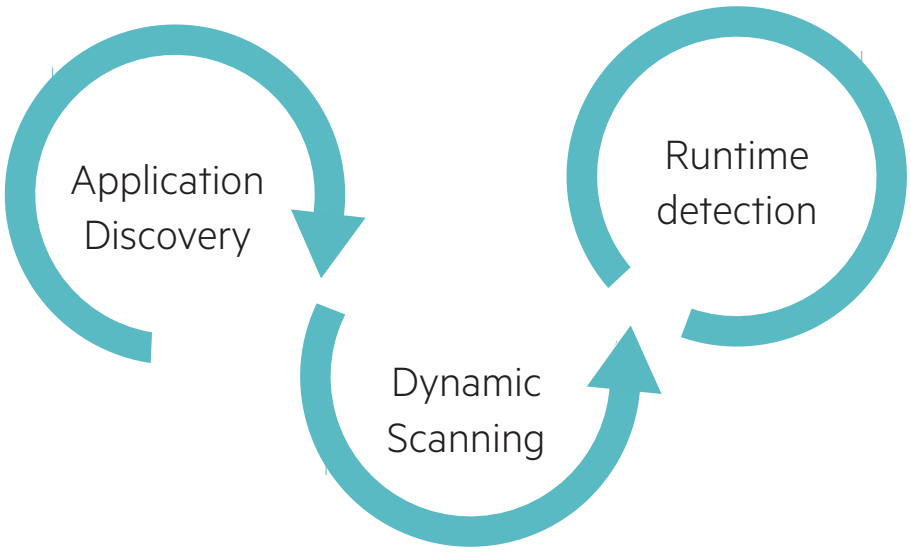

Figure 1. Continuous Application Monitoring

Application discovery and risk profiling

Do you know what's out there? Fortify on Demand Continuous Application Monitoring Service quickly and regularly gives security teams visibility into their external-facing software portfolio. Some are obvious—corporate, division, brand, or regional sites—but others can be hard to keep track of. Marketing and channel campaigns are a common, ongoing source of shadow IT, while mergers and acquisitions can significantly grow your portfolio almost overnight. Application security program managers need an ongoing solution to monitor and assess their company's constantly evolving attack surface.

Application discovery is kicked off monthly as part of the Continuous Application Monitoring service. It starts by identifying your publicly accessible web applications, starting with a few simple inputs: your primary corporate domains and company name at a minimum, with IP address range and keywords optional. Our automated service employs multiple advanced domain and endpoint-based discovery techniques to identify publically accessible web applications. Discovered applications are verified and used as feedback for further iterative discovery.

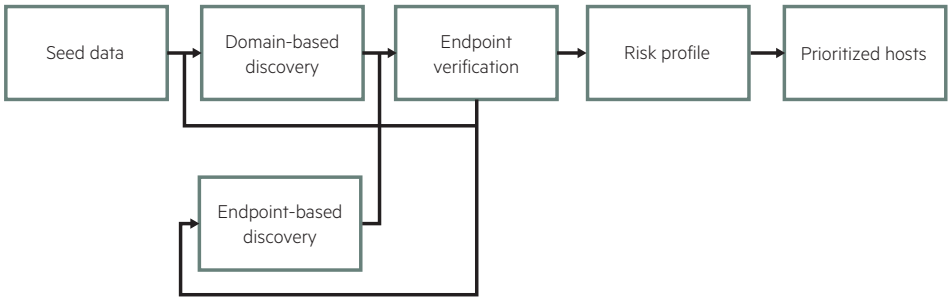

Figure 2. How application discovery works

As part of the discovery process, we look for specific criteria to help us risk profile the applications: site purpose (informational vs ecommerce), collection of personally identifiable information (PII), authentication capability, and web technology information (application server, client-side JavaScript libraries, etc) to name a few. The gathered information is used to generate risk ranking and confidence scores on a user-friendly scale. From the list of discovered and profiled applications, AppSec managers can make decisions about which sites to retire and which to confirm and enroll in their application security program.

Application discovery use cases:

- Cataloging application inventory before starting a software security program
- Establishing the business case for an application security initiative or program growth
- Maintaining visibility across worldwide, constantly evolving medium-to-large application portfolios

What we cover in the OWASP Top 10
A1 Injection

A2 Broken Authentication and Session Management

A3 Cross-Site Scripting (XSS)

A4 Insecure Direct Object References

A5 Security Misconfiguration

A6 Sensitive Data Exposure

A9 Using Components with Known Vulnerabilities

A10 Unvalidated Redirects and Forwards

Dynamic scanning and change detection

Script kiddies are scanning your sites right now, so why aren't you? Once a software portfolio has been scoped, an overwhelming feeling of, "where do we start?", is often a security team's next reaction. For enterprises starting out, Continuous Application Monitoring's powerful, yet fast dynamic and risk profile scanning technology quickly finds and provides recommendations to fix the most glaring vulnerabilities across large numbers of applications, demonstrating value early on. The team can then establish a methodical process for onboarding applications for more comprehensive dynamic and static scanning during development. For organizations with established software security assurance programs that focus on pre-production testing, Continuous Application Monitoring provides a complementary layer of defense in depth where the focus of application security testing has traditionally been on pre-preproduction.

Once an application is enrolled, Continuous Application Monitoring provides continuous lightweight, unauthenticated dynamic scans focused on common critical, highly exploitable vulnerabilities found in the **OWASP Top 10**, with a particular emphasis on common deployment issues, while also re-assessing the application's risk profile. Designed with production-safe principles at the forefront, the scan revalidates previous findings and looks for any changes that might have taken place since the previous scan, which can occur due to frequent or untested patches, new zero-day vulnerabilities or unintended configuration updates. Most recent changes, including new vulnerabilities or risk profile changes, are highlighted in a single dashboard, and a notification is triggered when a new vulnerability is detected or if the risk profile changes. Users can drill into the findings to see vulnerability and risk profile details.

Leveraging information provided by the continuous scans, application security teams managing large portfolios have visibility in between periodic comprehensive dynamic scans and are able to make better decisions on which applications need those deeper dynamic assessments and which may need protecting via runtime detection. This helps allocate resources based on company risk criteria and internal and external security polices and regulations. Information can also be funneled back to threat modeling and development as part of a mature security program.

Dynamic scanning and change detection use cases:

- Complement and prioritize comprehensive dynamic scanning in pre-production for defense in depth
- Quickly identify and remediate low-hanging but critical vulnerabilities
- Cost-effective alternative when not enough resources or budget to test every application during development
- Detect changes to application's threat model introduced by subsequent releases or patches

Comprehensive dynamic scanning

Chances are you are already employing dynamic scanning or penetration tests for those applications you know about. Now, as new information becomes available via application discovery and continuous scanning, security teams can identify at-risk applications and kick off a deeper dynamic scan. Customer-facing websites and mobile apps, or those containing sensitive data, are obvious choices for cyber-attacks. However, even secondary websites and brochure pages within the same network, are at risk and need to be constantly tested and monitored for security flaws.

Dynamic assessments mimic real-world hacking techniques and attacks using both automated and manual techniques to provide comprehensive analysis of complex web applications and services. Featuring **HPE Security Fortify WebInspect** for automated dynamic scanning, Fortify on Demand provides a full-service experience as all scans include macro creation for authentication and a full audit of results by our experts to remove false positives and for overall quality—a level of service you don't get with other providers. Our manual testing focuses on the types of vulnerabilities that skilled hackers exploit, including authentication, access control, input validation, session management, and business logic testing. Simply provide a URL and our team will handle the rest.

Fortify on Demand offers three levels of dynamic assessment types depending on need and business criticality: basic, standard, and premium. Dynamic basic offers an automated scan with a manual audit and false positive removal. Dynamic standard adds manual testing to the basic scan, while Dynamic premium offers an extensive manual component with static code analysis, business logic testing, and web services assessment. Typically, marketing applications are tested at the basic level while those needing to pass strict compliance guidelines are tested with the Dynamic premium assessment.

Comprehensive dynamic scanning use cases:

- Comply with industry compliance standards
- Quickly identify and validate critical security vulnerabilities and misconfigurations in running applications
- Identify application flaws that penetration testing or automated testing alone wouldn't find

Application Defender supports 29 vulnerability categories including:
SQL injection, cross-site scripting, Java deserialization, privacy violations, malformed request, command injection, internal security violations

Runtime detection

Remediating vulnerabilities found in production applications is not an instantaneous process. While it's a best practice to fix all security issues, it's not always possible or practical to disrupt the software development flow. To protect production software, HPE Security Fortify Application Defender offers runtime application self-protection (RASP) that quickly and easily detects and defends against exploits in real time.

The Application Defender solution works from within the application server, quickly instrumenting an application to stops attacks across dozens of vulnerability categories. Contextual insight from within the application data flows and execution logic enables Application Defender to identify and stop even the most sophisticated attacks.

Fortify on Demand integrates with Application Defender, allowing customers to implement smarter monitoring, logging, and protection for applications. While reviewing vulnerabilities identified from static or dynamic scanning within Fortify on Demand, customers can enable protections against identified vulnerability categories or even on a point-related basis for specific request paths. Conversely, by feeding real-time security event data from Application Defender, Fortify on Demand customers can better prioritize remediation efforts on the vulnerabilities where exploits are being attempted.

Runtime detection use cases:

- A greater number of vulnerable applications 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

Continuous Application Monitoring—key features and benefits

- Eliminates production application blind spots
  - Discovers what web applications actually exist on external networks and the risk factors involved
  - Identifies critical vulnerabilities early (before they are exploited)
  - Detects the most recent changes—both risk profile changes and new vulnerabilities—through continuous scanning
- Low to no impact on site load—designed for production safety
- Affordable, per application subscription model
- Fully automated—set up Continuous Monitoring at the tenant level and enroll applications, there's nothing else to do

How we sell it

We recommend customers purchase the Continuous Application Monitoring bundle, which includes monthly application discovery and allows continuous dynamic scanning for a desired number of applications. Additionally, continuous dynamic scanning is included with any dynamic basic, standard, or premium subscription and can also be purchased as a standalone service.

Dynamic Scans are purchased by redeeming HPE Security Fortify on Demand Assessment Units for single scans or application subscriptions.

Runtime Detection from Application Defender is available through an on-premise license or as a service (SaaS). One Application Defender agent license is included with every HPE Security Fortify on Demand Dynamic premium subscription.

For more information

Continuous Application Monitoring is part of a Software Security Assurance program that embeds security at all points in the software development lifecycle (SDLC).

Learn more at
hpe.com/software/FoD
Or contact your HPE representative

Sign up for updates

Hewlett Packard Enterprise

4AA6-7588ENW, September 2016