Especificações técnicas

HP Fortify on Demand

Teste de segurança de software na nuvem

Segurança de software contratada como um serviço sob demanda

O HP Fortify on Demand é uma solução de segurança como um serviço (SaaS) que permite a qualquer empresa testar a segurança do software que suporta os seus negócios com rapidez, precisão, a um preço acessível e sem qualquer software que precise ser instalado ou gerenciado. Esse serviço sob demanda ajuda as empresas em dois desafios principais:

– Garantir a segurança de aplicativos de software criados para propósitos específicos, e aplicativos de outros fornecedores.

– Aumentar a velocidade e a eficiência ao estabelecer a segurança de software em um ciclo de desenvolvimento.

O HP Fortify on Demand age como um sistema independente para análise de segurança em software, conduzindo avaliações consistentes e imparciais através de análises estáticas, dinâmicas e híbridas. Os resultados são apresentados em uma interface web detalhada ou em relatórios gerados em diversos formatos. O processo é extremamente simples, onde os usuários precisam somente carregar o código-fonte do software no web site da HP – no caso de uma análise estática – ou apontar a URL onde a aplicação web esteja publicada – no caso de uma análise dinâmica.

O ambiente está hospedado em data centers de segurança máxima, provendo aos nossos clientes uma solução completa de testes sem que haja a necessidade de aquisição de hardware, software ou a contratação de equipes especializadas.

Como o HP Fortify on Demand funciona

1. Inicie
Carregue seu código fonte ou indique a URL e receba um teste para análise de segurança no software, o que pode incluir análise estática e dinâmica, em um modelo que pode ser utilizado para o software originado em qualquer fonte:

- Localmente - colabore com seus desenvolvedores analisando a segurança do software localmente antes de implementá-los na produção.
- Comercialmente - proteja seus investimentos ao se assegurar de que todo software comercial é seguro antes de adquirir licenças.
- Terceirizado - tenha a certeza de que todo código terceirizado é escrito de forma segura.
- Código aberto - garanta que qualquer software de código aberto é compatível com suas expectativas de segurança.

2. Teste
Nossa equipe especializada em SaaS conduzirá uma auditoria dos seus aplicativos para identificar vulnerabilidades de segurança.

- Análise estática - os usuários simplesmente carregam bytecodes ou códigos fonte, e o HP Fortify on Demand realiza uma análise completa.
- Análise dinâmica - os usuários fornecem o URL de qualquer aplicativo em ambiente de homologação ou produção, e o HP Fortify on Demand pode ser programado para realizar testes automaticamente em um dos três níveis de serviço.
- Revisão especializada - todos os resultados são revisados manualmente por um especialista em segurança de software para garantir o mais alto nível de precisão.

"Praticamente metade dos aplicativos testados em 2012 eram vulneráveis a Cross-Site Scripting."

-HP 2012 Cyber Security Risk Report

Figura 1. Painel executivo do HP Fortify on Demand
O painel executivo do HP Fortify on Demand mostra os principais resultados para os projetos de teste do seu aplicativo em uma única tela.

Figura 2. Relatório detalhado: o relatório do HP Fortify on Demand pode correlacionar os resultados de diferentes formatos de teste e priorizá-los por severidade para fornecer a representação mais realista dos riscos do aplicativo.

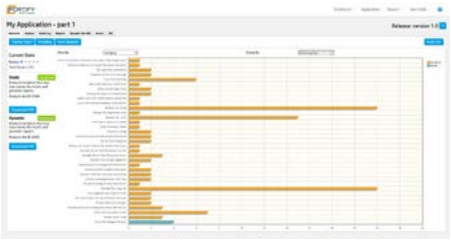

Figura 1. Ilustração das três etapas do processo do HP Fortify on Demand.

O cliente faz upload do software para a nuvem ou fornece a URL do aplicativo.

O HP Fortify on Demand conduz um teste de segurança completo (dinâmico ou estático) do aplicativo

O cliente revisa e analisa os resultados do teste do aplicativo apresentados como um painel ou relatório detalhado

3. Revisão
Revisão dos resultados correlacionados de forma detalhada.

- Painel executivo - monitore e gerencie todos os seus projetos de teste de segurança em software de um único ponto. As equipes de desenvolvimento e segurança podem economizar tempo e esforço graças à comunicação e colaboração por meio de um local central.
- Painel técnico - visualize os cinco projetos com pior desempenho, tendências da categoria OWASP Top 10, projetos de correção pendentes das últimas 4 semanas e atribuição vs. cancelamento de atribuição de problemas.
- Geração de relatórios detalhados - as avaliações são fornecidas em um relatório que conta com um sistema de classificação de cinco estrelas consistente, geralmente em apenas um dia. Os resultados são correlacionados e priorizados de acordo com a severidade e o grau de risco. Os problemas identificados incluem detalhes no nível do código de linha, com sugestões de como corrigi-los.

Casos de uso do HP Fortify on Demand

O HP Fortify on Demand pode proteger qualquer aplicativo, seja ele desenvolvido internamente ou por terceiros. Geralmente, ele é utilizado nestes cenários:

Testes de segurança de aplicativos internos
Isso permite que qualquer empresa teste a segurança de todos os softwares localmente - durante o desenvolvimento e em ambiente de produção. O HP Fortify on Demand estabelece um parâmetro de segurança em todo o portfólio de software sem a necessidade de implementar ou manter hardware e software, os clientes podem testar mais aplicativos — centenas ou até milhares — com eficiência. Falta de pessoal? Nossa equipe de especialistas oferece todos os testes e triagem necessários. Com uma assinatura anual, os usuários do HP Fortify on Demand podem desfrutar de avaliações ilimitadas.

Testes de segurança de aplicativos de outros fornecedores
O HP Fortify on Demand oferece uma análise independente de aplicativos de outros fornecedores, permitindo que as empresas testem o software antes de adquiri-lo e também que os fornecedores do software demonstrem a segurança do seu produto. Os fornecedores podem carregar o código fonte e/ou fornecer um URL para a análise de resultados e, posteriormente, disponibilizar um relatório para seus clientes. Esse serviço obriga fabricantes comerciais a agir proativamente no intuito de corrigir vulnerabilidades, além de permitir que eles mantenham controle de seus aplicativos. Os profissionais de segurança podem exigir que problemas de alta prioridade sejam corrigidos e verificados durante os processos de aquisição ou atualização, antes da aceitação.

Escolha a solução certa para você

Como optar entre uma solução local ou sob demanda?

O HP Fortify não restringe você em seu investimento. Oferecemos tanto uma solução local como sob demanda.

- Algumas empresas começam com o HP Fortify on Demand devido ao baixo custo de propriedade e à facilidade de iniciar rapidamente os testes para a segurança do software. Posteriormente, assim que o processo atingir o nível de maturidade esperado, eles podem optar pela tecnologia local.
- Outras empresas optam por um modelo híbrido, com alguns aplicativos enviados para a nuvem para teste e outros analisados localmente durante o desenvolvimento.
- As empresas também concordam que o HP Fortify on Demand é incrivelmente fácil de usar e descobrem que o ROI é superior ao utilizá-lo para todos seus aplicativos.

Nossas soluções sob demanda e local aproveitam as mesmas técnicas de análise, classificações de vulnerabilidade e sistemas de categorização de aplicativos. A HP é a única empresa que oferece essa flexibilidade na implantação.

Sobre o HP Fortify on Demand

O HP Fortify on Demand oferece

- A melhor análise
  - Recursos estáticos e dinâmicos líderes de mercado
  - Recursos de análise testados nos clientes do HP Fortify desde 2001
  - A maior e mais experiente equipe de pesquisa de segurança
- Resultados estáticos e dinâmicos correlacionados, com diretrizes de prioridade detalhadas
- Resultados precisos, específicos para cada aplicativo
- Suporte para aplicativos móveis, da Web e thick client
- Todos os resultados são manualmente analisados por especialistas em segurança de aplicativo
- Gerenciamento centralizado do programa de testes para todos os aplicativos

Benefícios do HP Fortify on Demand

- Fácil gerenciamento: sem hardware, software ou manutenção
- Rápido: geralmente, os resultados são obtidos em menos de 24 horas no caso de avaliações estáticas
- Flexibilidade para migrar de forma rápida e fácil para a solução HP Fortify local, e vice-versa
- Início de uso imediato - sem necessidade de aguardar aquisições, aprovações ou implementações demoradas
- Rápida conformidade com PCI, HIPAA, FISMA e muitos outros padrões
- Soluções personalizadas que se adequam a qualquer tamanho de empresa
- Geração de relatórios detalhados, incluindo resultados correlacionados priorizados por severidade para fornecer a imagem precisa de risco do software.

Especificações do HP Fortify on Demand

- Análise estática - bytecode ou código fonte para 21 linguagens diferentes
- Análise dinâmica - todas as linguagens da Web
- Análise móvel - Android, Apple iOS, Blackberry e Microsoft

"Houve um aumento de 68% nas vulnerabilidade de aplicativos de 2011 para 2012"

-HP 2012 Cyber Security Risk Report

Integrações do HP Fortify on Demand

- HP Application Lifecycle Management (ALM) - os resultados do HP Fortify on Demand podem ser importados no ALM, permitindo que as empresas rastreiem as vulnerabilidades de segurança como outros defeitos do software.
- Archer - os resultados do HP Fortify on Demand podem ser exportados automaticamente para o Archer para ajudar a melhorar a conformidade.
- Build server - os clientes podem definir um processo automático para carregar aplicativos a partir de um build server.

Linguagens estáticas

Linguagens compatíveis

ABAP/BSP	COBOL	Python
ASP.NET	JavaScript/Ajax	Ruby
C	Java (com Android)	T-SQL
C#	JSP	VB6
C++	Objective C	VBScript
Classic ASP	PHP	VB.NET
ColdFusion	PL/SQL	XML/HTML

HP Fortify on Demand Dynamic

O HP Fortify on Demand oferece três níveis para avaliações dinâmicas, onde a maioria dos clientes escolhe o tipo de avaliação com base no perfil de risco do aplicativo que está sendo testado. Normalmente, aplicativos de marketing são testados com a opção Basic, enquanto que aplicativos que sustentam diretamente os negócios são testados com a avaliação Premium.

Basic	• Uma solução automatizada para testes de segurança em Web • Inclui uma avaliação via scanner de segurança HP WebInspect • Todos os resultados são analisados manualmente por especialistas de segurança para remover falsos positivos.
Standard	• Uma solução automatizada para aplicativos Web que representam itens permanentes na experiência on-line do cliente e oferecem processos baseados em formulário, com várias etapas, mas não são necessariamente de missão crítica. • Testes manuais para vulnerabilidades técnicas • O padrão inclui o uso de várias soluções de teste manual e automatizado. • Todos os resultados são analisados manualmente por especialistas de segurança para remover falsos positivos.
Premium	• Uma solução de teste manual e automatizado de segurança para aplicativos Web que são permanentes ou de missão crítica, apresentam requisitos rigorosos de conformidade, dos quais os clientes dependem ou parceiros comerciais e que apresentam processos baseados em formulários, com várias etapas • A opção Premium inclui testes para vulnerabilidades técnicas e da lógica de negócios. • A descoberta de vulnerabilidades na lógica de negócios exige a análise manual pelos especialistas em segurança em site da Web, pois eles são capazes de compreender questões como as estruturas da conta e a lógica contextual presente nos aplicativos Web. • Inclui serviços Web para até 10 endpoints • A opção Premium inclui uma avaliação estática, se o cliente tiver acesso ao código fonte ou bytecode do aplicativo que está sendo avaliado. Isso é opcional. • Todos os resultados são analisados manualmente por especialistas de segurança para remover falsos positivos.

Ofertas de avaliação para software móvel

Análise móvel	Básico	Padrão	Premium
Nível risco aplic.	Baixo Aplic. marketing	Médio Identificação pessoal	Alto Cartão de crédito/CPF
Camada cliente - Fonte	√	√	√
Camada cliente - Dinâmica		√	√
Camada cliente - Binário			√
Camada de rede - Dinâmica		√	√
Camada do servidor - Estática e dinâmica			√
Verific. de correção	√	√	√

Sobre a HP Enterprise Security

HP é a fornecedora líder em soluções em compliance e segurança para as organizações que buscam mitigar os riscos em ambientes híbridos e estarem protegidas de ameaças avançadas. Baseada nos produtos líderes de HP ArcSight, HP Fortify e HP TippingPoint, a plataforma HP Security Intelligence é única na entrega de correlacionamentos avançados de eventos, segurança para software e defesa para os perímetros digitais e redes de dados, fornecendo soluções que efetivamente protegem a infraestrutura tecnológica de nossos clientes das mais sofisticadas ameaças cibernéticas.

Sobre o HP Fortify

O HP Fortify oferece soluções completas de SSA, incluindo a linha mais completa de produtos e serviços disponível atualmente no mercado. As soluções HP Fortify ajudam você a confiar no software do qual depende ao ajudá-lo a localizar, corrigir e fortalecer os aplicativos em menos tempo e com menor custo se comparado às estratégias centralizadas na ferramenta.

Saiba mais em
hp.com/go/Fortify

Inscreva-se para obter atualizações
hp.com/go/getupdated

Compartilhe com colegas

Avalie este documento

4AA4-0664PTL, setembro de 2013, Rev. 1