White Paper

Segurança

# Segurança de aplicativos perfeita: segurança na velocidade de DevOps

MICRO FOCUS

# Índice

página

À medida que o tempo de lançamento no mercado continua a ser crucial para os negócios, as organizações estão adotando DevOps ou metodologias ágeis semelhantes para desenvolvimento rápido. Na verdade, as empresas acreditam que, até 2020, cada aplicativo precisará ser lançado 30 vezes a mais por ano para acompanhar as demandas de clientes e parceiros para interagir com a organização por meio de aplicativos.

## O problema atual de segurança de aplicativos

Nos últimos anos, o software passou de uma função de suporte de negócios para um centro de inovação, tornando-se o diferencial competitivo essencial para a maioria das empresas de todos os setores e tamanhos. Com essa mudança na função do software, as empresas atuais estão aumentando drasticamente o número de aplicativos e a frequência de lançamentos, com pouco investimento nos requisitos não funcionais. Além disso, os aplicativos modernos estão aumentando em complexidade devido à necessidade de velocidade e, como resultado, a dependência dos desenvolvedores em relação à reutilização de código, bem como de componentes de código-fonte aberto e comerciais (COTS) aumentou drasticamente. Isso tem grandes implicações nas equipes de segurança para encontrar e gerenciar vulnerabilidades. Como consequência, algumas das notáveis violações de segurança nos últimos anos foram causadas por vulnerabilidades em componentes de código de terceiros.

Com as necessidades comerciais no comando, os aplicativos estão se proliferando por meio de sites, plataformas de mídia social, como Facebook, aplicativos móveis e em nuvem. Além disso, alguns aplicativos são conduzidos por equipes de marketing e criados com software de terceiros. Esses aplicativos geralmente estão fora dos processos normais de negócios com pouca ou nenhuma governança.

Além de todos os desafios criados pelo aumento do número de aplicativos, o aumento da complexidade e lançamentos mais rápidos, regulamentos como o GDPR e a captura de dados de clientes para fins comerciais tornaram-se a norma. Ter várias instâncias de dados de clientes aumenta a probabilidade e o impacto de uma violação. Isso é especialmente preocupante porque a maioria das violações de segurança atuais se deve a vulnerabilidades de aplicativos. De acordo com o Relatório de risco de segurança de aplicativos de 2018 da Micro Focus® Software Security Research, 80% dos aplicativos contêm pelo menos uma vulnerabilidade crítica ou alta e 90% dos incidentes de segurança são de explorações contra defeitos no design ou código do software.

## Esses problemas só continuarão crescendo

À medida que o tempo de lançamento no mercado continua a ser crucial para os negócios, as organizações adotam DevOps ou metodologias ágeis semelhantes para desenvolvimento rápido. Na verdade, as empresas acreditam que, até 2020, cada aplicativo precisará ser lançado 30 vezes por ano para acompanhar as demandas dos clientes e parceiros. Tudo isso significa que, se a segurança não se tornar uma parte essencial do ciclo de vida do software, as organizações lançarão com mais vulnerabilidades em velocidade inimaginável.

## Por que as práticas tradicionais de segurança de aplicativos não serão bem-sucedidas

Na maioria das organizações, a segurança de aplicativos é limitada a uma equipe específica que se envolve nos estágios finais de desenvolvimento e é considerada um inibidor de velocidade. Essas equipes de segurança não conseguem acompanhar o ritmo, pois as equipes de desenvolvimento estão crescendo a uma taxa de 80:1[1] em relação às equipes de segurança. Quando as vulnerabilidades de segurança são encontradas em estágios posteriores, as organizações enfrentam pressão, o que resulta em atrito entre as equipes, perda de prazos de lançamento ou algo pior. Versões com defeitos de segurança conhecidos também são enviadas à produção para atender aos prazos do projeto, caso em que a empresa e seus clientes correm o risco de serem expostos a invasores.

Além dos prazos não cumpridos e da dinâmica da equipe, ter uma abordagem reativa à segurança de aplicativos custa mais para as organizações. De acordo com o NIST, o custo para corrigir falhas de segurança é 30 vezes mais caro na produção e 10 vezes mais nos testes do que se eles fossem detectados em estágios iniciais de desenvolvimento. Todos esses problemas e riscos em potencial indicam que a única maneira de proteger aplicativos sem comprometer o custo é mudar para um modelo de segurança de aplicativos perfeita.

## O que é a segurança de aplicativos perfeita?

A segurança de aplicativos perfeita tem a ver com tornar a segurança de aplicativos parte integrante do ciclo de vida do software sem gerar carga adicional para os interessados. Seja adotando uma abordagem DevSecOps ou apenas criando um programa de segurança mais eficaz, a necessidade é pensar na segurança desde os primeiros estágios do ciclo de vida. As práticas recomendadas e os testes de segurança de aplicativos devem ser incorporados em todo o processo de ciclo de vida de desenvolvimento de software. Quando executado da maneira correta, isso também significa que você não precisa comprometer a segurança de aplicativos para obter os ciclos de lançamento mais rápidos que estão sendo conduzidos pelo mercado.

## Como tornar a segurança de aplicativos perfeita para sua organização?

O sucesso com a segurança de aplicativos perfeita exige tempo e esforço, mas o maior obstáculo a ser superado é a mudança de cultura necessária para incluir a segurança em todo o ciclo de vida de desenvolvimento de software. É importante remover o atrito entre as equipes de segurança e os desenvolvedores. Assim como em DevOps, as equipes precisam dividir os silos entre elas, adotar a transparência e colaborar. Embora seja mais fácil falar do que fazer isso, ter a adesão de executivos e alguns dos principais campeões dentro da organização pode ajudar a impulsionar essa iniciativa. Além da mudança de cultura necessária, veja algumas etapas importantes para tornar a transição da segurança de aplicativos perfeita bem-sucedida:

A segurança de aplicativos perfeita tem a ver com tornar a segurança de aplicativos parte integrante do ciclo de vida do software sem gerar carga adicional para os interessados.

1 *Fonte: "10 Things to Get Right for Successful DevSecOps", Gartner, Inc., 2017*

Ao encontrar e corrigir defeitos de segurança durante o processo de codificação, os desenvolvedores podem eliminar possíveis vulnerabilidades de segurança antes de chegarem aos testes e à produção, economizando tempo e dinheiro da organização.

## Etapa 1: desenvolver com a segurança em mente

Com a proporção de desenvolvedor para especialista em segurança aumentando em direção a essa proporção de 80:1, é essencial capacitar os desenvolvedores a assumir a responsabilidade por seu próprio código. Ao encontrar e corrigir defeitos de segurança durante o processo de codificação, os desenvolvedores podem eliminar possíveis vulnerabilidades de segurança antes de chegarem aos testes e à produção, economizando tempo e dinheiro da organização. Essa mudança de pensamento exige treinar os desenvolvedores para codificar com a segurança em mente e usar as ferramentas certas para obter feedback em tempo real sobre o código. Há muitas opções para o treinamento de segurança do desenvolvedor, mas ferramentas que fornecem feedback de segurança em tempo real sobre o código (como o Fortify Security Assistant, que funciona de forma muito semelhante a um corretor ortográfico de segurança, fornecendo segurança em tempo real sobre o código à medida que ele é desenvolvido) ou treinamento de desenvolvedor gamificado integrado tornam a adoção mais fácil e aceleram o treinamento. Também é importante que as equipes de segurança ajudem a permitir que os desenvolvedores compartilhem informações sobre ameaças conhecidas, fornecendo feedback e tendo transparência e visibilidade do trabalho. Ter líderes de desenvolvimento treinados em segurança de aplicativos e se juntar a eles como defensores da segurança gera resultados positivos. Dessa forma, os líderes de desenvolvimento trazem a perspectiva de segurança logo no início do ciclo de vida de desenvolvimento, além dos tradicionais aspectos funcionais e de qualidade.

## Etapa 2: teste antecipado, frequente e rápido

Durante o ciclo de vida de desenvolvimento de software, há várias abordagens a serem seguidas para manter a velocidade necessária para acompanhar os lançamentos de hoje. Essas abordagens são testes antecipados, frequentes e rápidos.

**Teste antecipado**

O SAST (Static Application Security Testing, Teste estático de segurança de aplicativos) identifica as causas raiz dos problemas de segurança e ajuda a corrigir as falhas de segurança subjacentes nos estágios iniciais do desenvolvimento. Para manter a velocidade dos lançamentos, os desenvolvedores precisam ser capazes de enviar código de forma rápida e fácil, tendo a inteligência ao alcance dos dedos. O **Fortify Static Code Analyzer** lidera esse método porque:

- Identifica e elimina vulnerabilidades no código-fonte, binário ou byte
- Analisa os resultados da verificação em tempo real com acesso a recomendações, navegação de linha de código para encontrar vulnerabilidades mais rapidamente e permitir auditoria colaborativa.
- Integra-se totalmente aos populares ambientes de desenvolvedores integrados (IDEs)

O **Fortify Security Assistant** leva isso um passo adiante, oferecendo aos desenvolvedores insights em tempo real e recomendações sobre vulnerabilidades de código à medida que o código é escrito. Isso não só funciona como uma "verificação ortográfica" de segurança do desenvolvedor para vulnerabilidades conhecidas comuns, como também permite que ele pare de cometer esses erros para começar.

### Teste com frequência

O Dynamic Application Security Testing (DAST) simula ataques em um aplicativo da Web em execução ou para identificar vulnerabilidades exploráveis. Isso fornece uma visão abrangente da segurança de aplicativos, concentrando-se no que é explorável e cobrindo todos os componentes (servidor, código personalizado, código-fonte aberto, serviços). Ao integrar as ferramentas DAST ao desenvolvimento, à garantia de qualidade e à produção, é possível oferecer uma visão holística contínua. O **Fortify WebInspect** oferece uma solução eficaz ao:

- Identificar rapidamente os riscos em aplicativos existentes
- Automatizar testes dinâmicos de segurança de aplicativos de qualquer tecnologia, desde o desenvolvimento até a produção
- Validar vulnerabilidades nos aplicativos em execução, priorizando os problemas mais críticos para a análise de causa raiz
- Simplificar o processo de correção de vulnerabilidades

### Teste rápido

O teste interativo de segurança de aplicativos (IAST) é uma forma de teste de segurança de aplicativos que combina o teste dinâmico de segurança de aplicativos (DAST) e o feedback de tempo de execução do aplicativo testado à medida que os testes são executados. Mas mesmo com uma abordagem IAST, encontrar vulnerabilidades é apenas 1/3 do esforço. Os outros 2/3 do esforço geralmente podem ser gastos em validação e correção de falsos positivos. Outro contra-argumento do IAST é o fato de que esse método de teste provavelmente perderá verdadeiros positivos devido às limitações técnicas dessa abordagem. Como uma abordagem alternativa e mais eficiente, os algoritmos de aprendizado de máquina aplicados e a automação de auditoria podem economizar tempo e esforço de auditoria, além de melhorar a precisão da análise estática.

O **Fortify Audit Assistant** é nossa tecnologia inovadora de aprendizado de máquina. Oferecido no local e na nuvem, o Assistente de auditoria aproveita os metadados dos resultados de verificação para prever e remover falsos positivos, reduzindo o tempo de correção em até 50%. Um cliente notou que 8000 problemas de Java foram reduzidos para cerca de 3000 com base nessa tecnologia. Nossa versão 18.2 automatiza ainda mais o processo para os clientes adicionando a previsão automática na versão do aplicativo para solicitar automaticamente previsões automatizadas quando novos problemas são adicionados.

O Fortify Audit Assistant simplifica a fase mais demorada dos testes de segurança: a auditoria dos resultados da verificação. O Fortify Audit Assistant aplica amplo conhecimento de segurança e aprendizado de máquina para automatizar a remoção de falsos positivos, priorizar descobertas e identificar as vulnerabilidades de segurança relevantes para a organização. Isso significa que, depois que uma verificação estática é iniciada, os resultados da verificação validada podem ser obtidos em minutos e enviados para o desenvolvimento para obter correções.

Mesmo com uma abordagem IAST, encontrar vulnerabilidades é apenas 1/3 do esforço. Os outros 2/3 do esforço geralmente podem ser gastos em validação e correção de falsos positivos.

A segurança de aplicativos perfeita, integrada ao longo de todo o ciclo de vida de desenvolvimento de software, cria muito menos riscos e processos controlados de forma mensurável, o que resulta em custos reduzidos, tempo de lançamento no mercado aprimorado e esforço otimizado.

# Etapa 3: aproveitar as integrações para tornar a segurança de aplicativos uma parte natural do ciclo de vida

Para tornar a segurança de aplicativos perfeita, é essencial aproveitar as integrações com suas ferramentas atuais durante todo o ciclo de vida de desenvolvimento de software. O **Micro Focus Fortify** é o líder do setor em soluções de segurança de aplicativos e vem com as opções de integração avançadas para todo o ciclo de vida do software, disponibilizando e tornando a segurança de aplicativos consumível por equipes rápidas. Hoje, muitas organizações têm várias equipes em diferentes locais, todas usando diferentes ferramentas de desenvolvimento, QA e monitoramento. Para obter a visibilidade e a percepção necessárias em toda a empresa, é comum utilizar uma ferramenta de gerenciamento do ciclo de vida, como o **Micro Focus ALM Octane**.

Integrados juntos, o ALM Octane e o Fortify oferecem diversos benefícios e necessidades importantes consistentes com a segurança de aplicativos perfeita. As verificações de segurança podem ser iniciadas como parte de compilações e os resultados da verificação podem ser importados automaticamente para o ALM Octane para controle e monitoramento eficientes. Isso exporá todas as vulnerabilidades de segurança logo após serem introduzidas no código e fornecerá à equipe as informações necessárias para rastreá-las e corrigi-las. Além de identificar os riscos logo no início, o processo aumenta a conscientização dos desenvolvedores e os encoraja a evitar a introdução de vulnerabilidades no código em primeiro lugar.

### Implantação de software mais rápida

Com opções de automação para verificações estáticas e dinâmicas e integrações disponíveis para as ferramentas de desenvolvimento mais populares, como Visual Studio, Eclipse e Jenkins, as equipes de desenvolvimento economizam tempo e reduzem o atrito. As integrações com sistemas de gerenciamento de defeitos, como JIRA ou BugZilla, melhoram o tratamento e a correção de problemas de segurança e garantem que eles possam ser tratados da mesma maneira que a organização lida com problemas funcionais. Essa abordagem eficiente resulta em desenvolvimento e implantação de software mais rápidos que atendem às necessidades comerciais de velocidade.

### Redução dos riscos

Ao mudar a segurança para a esquerda e cobrir todo o ciclo de vida de desenvolvimento de software de uma forma perfeita, as organizações reduzem os riscos e custos associados, pois é menos dispendioso corrigir vulnerabilidades no início do processo. O **Fortify Security Assistant** e a automação de verificações de segurança conduzidas pelo ALM Octane ou Jenkins ajudam a organização de desenvolvimento a adotar testes de segurança antecipadamente e durante todo o processo.

### Melhor retorno do investimento

O Fortify trabalha com ferramentas de desenvolvimento existentes para proteger seu investimento existente e permite que as equipes de desenvolvimento continuem usando suas ferramentas favoritas. Com o Assistente de segurança, por exemplo, os desenvolvedores não precisam aprender uma ferramenta diferente para executar verificações de segurança em seu código, pois ele funciona no IDE existente. Ou, com integrações de verificação estática, as verificações de segurança são executadas como parte do processo de criação e os desenvolvedores recebem os problemas de segurança dentro do sistema de gerenciamento de defeitos, sem introduzir nenhuma complexidade nas ferramentas e nos processos existentes.

## Etapa 4: automatizar a segurança como parte dos processos de desenvolvimento e teste

Automatizar o desenvolvimento, os processos, o provisionamento de servidores e a implantação de aplicativos é a chave para ser eficiente com a iniciativa DevOps. A automação permite que as organizações desenvolvam e lancem aplicativos de maior qualidade com mais rapidez. Para uma segurança de aplicativos perfeita, a automação pode ser utilizada da mesma maneira com testes de segurança para manter a mesma qualidade em velocidade mais alta. Ao automatizar os testes de segurança, você pode criar e executar testes de segurança automatizados da mesma forma que faria com testes de unidade ou de integração.

Com a análise automatizada estática ou dinâmica, você pode identificar com eficiência as vulnerabilidades de segurança no código-fonte, minimizando a natureza trabalhosa das avaliações de segurança. Ter uma análise automatizada do código reduz não apenas os tempos de análise, a avaliação e o teste de segurança, mas também reduz os custos de correção ao encontrar vulnerabilidades mais cedo.

## Etapa 5: monitorar e proteger depois de lançar

A primeira etapa em qualquer iniciativa de segurança de aplicativos é entender onde está sua exposição a riscos, especialmente em ambientes de produção que talvez já estejam vulneráveis. Embora tratar da segurança como parte do processo de desenvolvimento seja uma ótima abordagem, também é vital proteger os aplicativos existentes em produção. Agora é essencial monitorar e proteger continuamente ambientes de produção para riscos de segurança de aplicativos novos ou não autorizados, alterações de perfil de risco e vulnerabilidades de dia zero. Isso é feito utilizando a autoproteção do aplicativo de tempo de execução (RASP).

O RASP usa instrumentação de tempo de execução para detectar e bloquear ataques de computadores, aproveitando as informações de dentro do software em execução. O **Fortify Application Defender** pode fornecer mais visibilidade aos ambientes de produção e levantar sinais de alerta para investigação adicional.

## Para começar

A segurança de aplicativos perfeita, integrada ao longo de todo o ciclo de vida de desenvolvimento de software, cria muito menos riscos e processos controlados de forma mensurável, o que resulta em custos reduzidos, tempo de lançamento no mercado aprimorado e esforço otimizado. Ter um caminho claro para a segurança de aplicativos integrada e automatizada com KPIs mensuráveis aumentará a oportunidade de sucesso da sua organização. A segurança de aplicativos fornece retornos que são mais fáceis de demonstrar em comparação com outros investimentos em segurança cibernética. A demonstração do progresso feito e do retorno do investimento garantirá um investimento contínuo na segurança de aplicativos.

Ter um caminho claro para a segurança de aplicativos integrada e automatizada com KPIs mensuráveis aumentará a oportunidade de sucesso da sua organização.

O Fortify fornece uma solução flexível e completa de segurança de aplicativos, com modelos no local, sob demanda e híbridos.

Veja algumas coisas importantes a serem consideradas ao criar o roteiro para essa jornada.

- Identifique os especialistas em segurança de aplicativos perfeita.
- Desenvolva sua estratégia e os principais processos antes de implementar.
- Defina o escopo inicial e as principais métricas, como:
  - Com quais aplicativos e equipes de desenvolvimento começar,
  - Se usar SAST, DAST ou ambos,
  - Quais integrações aproveitar,
  - Se é necessário usar ferramentas de segurança de aplicativos no local, sob demanda ou uma abordagem híbrida,
  - Quais são as melhorias esperadas em 12 meses em comparação com a linha de base.
- Encontre as ferramentas certas para sua organização.

Pessoas, processos e tecnologia são os componentes essenciais da segurança de aplicativos perfeita. O Micro Focus Fortify tem a experiência e os recursos com a tecnologia, as pessoas e os processos (via **Fortify on Demand** e serviços profissionais) para ajudar você em cada etapa do caminho.

O Fortify fornece uma solução flexível e completa de segurança de aplicativos, com modelos no local, sob demanda e híbridos. Com **benefícios mensuráveis**[2] como tempo de lançamento no mercado 30 vezes mais rápido, 95% menos positivos, verificações 10 a 15 vezes mais rápidas, correção 10 vezes mais rápida e o dobro de vulnerabilidades encontradas, o Fortify continua sendo o líder do setor em ferramentas de segurança de aplicativos.

Escolha o Fortify para:

- **Facilidade de começar:** você pode começar em um dia com o**Fortify on Demand**.
- **Facilidade de uso e integração intuitiva aos processos existentes:** o Fortify integra-se facilmente ao que seus desenvolvedores usam e adoram, tornando a segurança uma adição perfeita às ferramentas e processos existentes.
- **Recursos de velocidade, automação e escala:** a maioria das verificações do Fortify é concluída em minutos e você pode obter resultados de auditoria assistida por máquina em minutos para resultados de verificação brutos. As verificações automatizadas podem ser iniciadas como parte de check-ins de código, compilações, versões ou outros componentes do pipeline CI/CD. Os clientes do Fortify podem dimensionar facilmente no local usando técnicas de verificação centralizadas, utilizando o Fortify on Demand ou uma abordagem híbrida.
- **Precisão e cobertura em linguagens de programação:** os clientes do Fortify relatam mais verdadeiros positivos (mais resultados validados) e menos falsos positivos (menos ruído) em comparação com outros produtos. O Fortify oferece a mais ampla cobertura de linguagem de programação com 25 linguagens de programação compatíveis em novembro de 2018.
- **Reconhecimento contínuo do setor:** o Fortify foi reconhecido como líder em segurança de aplicativos nos últimos 13 anos, incluindo o reconhecimento como líder no Quadrante Mágico da Gartner para Segurança de aplicativos pelo 8° ano consecutivo. O Fortify tem sido confiável para as principais empresas em várias indústrias em todo o mundo.

2 *Fonte: "Continuous Delivery of Business Value with Micro Focus Fortify" Mainstay Customer Evidence Research*

Fale conosco:
**www.microfocus.com**

Gostou do que leu? Compartilhe.