VERACODE

WHITE PAPER

Addressing the Scalability Challenge with Cloud-Based Application Security

TABLE OF CONTENTS

I. Executive Overview 3

II. The threat to software applications is growing. 4

III. Application security has evolved. 5

IV. Legacy security testing tools slow innovation. 5

V. There is a simpler, more scalable way. 6

Veracode's centralized platform:

A. Multiple analysis techniques 6

B. Platform core capabilities 8

VI. Every enterprise has its unique challenge. What's yours? 8

A. Developing software with security and agility 9

B. Protecting web applications in a fast, scalable way 9

C. Streamlining compliance processes with automation 11

D. Reducing risk from third-party software 11

E. Securing mobile apps whether built, bought or downloaded 12

VII. Conclusion 13

EXECUTIVE OVERVIEW

Every enterprise is now a technology company. Business trends driven by mobile, cloud, social media and Big Data technologies are dramatically changing the way global organizations deliver innovation. Time-to-market is as important as ever, exposing some information security approaches as woefully deficient.

Many enterprises are not adequately protecting the software that runs their business. Ad-hoc application security programs and regimens have led to inconsistent policies across organizational business units and software development teams. Traditional on premise solutions have proven difficult for IT staff to correctly configure. The result: enterprises end up with a fragmented approach to application-layer security. Millions are spent on one-off or manual testing and tools, but they end up covering only a fraction of the organization's global application threat surface.

Yet cyber threats to global commerce only continue to proliferate. Cyber-attackers continue to improve their tactics at an alarming rate. New attacks and exploits look for the paths of least resistance – such as ignored or unprotected websites and applications on the enterprise perimeter. A determined criminal, hacktivist or cyberspy will search every nook and cranny of a target enterprise's software supply chain to find its weakest link.

It's the job of every Chief Information Security Officer to ensure that the software that runs the business doesn't introduce unnecessary risk. The risks of a significant data breach are well understood, threatening intellectual property, future revenue, market valuation and brand reputation. Protecting the entire software supply chain – from cloud to mobile to vendor-supplied apps in a sustained and systematic way – requires specialized expertise.

Veracode offers a simpler and more scalable approach to application security. Its powerful, cloud-based platform offers on-demand protection to secure a global organization's entire application infrastructure. Veracode combines deep security knowledge with proven best practices for managing enterprise-wide software governance programs for its global blue chip customers.

Application security, at its best, is a collaborative effort. Robust programs involve the active participation of representatives from application development, IT operations, GRC audit, legal and even vendor procurement. IT security teams need to address the unique needs of these groups to justify increased investment in securing the software that runs the business.

The threat to software applications is growing.

IT security professionals are well aware of the kinds of cyber threats targeting their organizations. Data breaches from cyber-attacks are the single biggest threat to enterprise security today. The quantity and frequency of significant breach incidents are only growing – and well-documented. To mitigate this threat, organizations must secure all three fundamental access points to their digital data: the network; the hardware… and the *software* that support their business operations.

Existing security measures create a false sense of security. Most enterprises have widely adopted IT security tools such as firewalls and intrusion detection to protect their networks as well as antivirus, access control and physical security measures to secure their hardware. However, what many businesses still lack is adequate investment in the protection of their critical software. Simply put, software applications have become the most vulnerable entry point for attacks targeting an organization's sensitive, protected or confidential data. If network and hardware infrastructure is the "back door" to the network, then business applications are the front door. Very few people leave their front door unlocked these days.

Professional attackers and cyber criminals know to exploit the weakest link in an organization's IT infrastructure – vulnerable software – to get at valuable data. Cyber-attackers located anywhere in the world easily scan business applications for common vulnerabilities using freely-available tools — as often as they like. Consider these sobering statistics:

- **93%** of companies suffered a data breach in 2013. (source: U.K. BIS report)
- **75%** of attacks are financially motived cybercrime, with **92%** perpetrated by malicious outsiders. **52%** of data breaches are caused by attackers hacking applications. (source: Verizon)
- The National Vulnerability Database – the U.S. government's repository of standards based vulnerability management data – publishes at a rate of **13** new vulnerabilities each and every day. In 2013, **75%** of flaws found were software related. (source: NIST)
- When 12,000 security professionals were asked to name the number one security threat to their organization, **69%** said application-layer vulnerabilities. (source: Booz Allen Hamilton)
- Only **10%** of enterprises test *all* their critical applications for resilience against cyber-attacks. (source: SANS)
- The costs of a single data breach are daunting: **$188** per compromised record or an average **$5.4M** per incident, and as high as **$277/record** when recovering from criminal attacks. (source: Symantec)
- For public companies, data breaches can hammer their valuation. Big box retailer Target estimates its widely publicized data breach cost them as much as **$61 million** during the 2013 holiday shopping season. Its stock plummeted **-10.5%** in a single month. (source: CNN)

Compliance pressures only intensify the requirement for a multi-layered security approach to strengthening data privacy and protection. Government and industry regulatory bodies, alarmed by the potential for widespread social and commercial damage, have been strengthening mandates in the area of application security.

Application security has evolved.

Software is everywhere. It is increasingly plentiful, accessible, painless and profitable for malicious parties to attack. The practice of application security protects an organization's critical data from external threats by ensuring the security of all of the software utilized to run the business. Just as Quality Assurance (QA) is the operational solution to the problem of product quality, application security is the operational solution to the problem of software risk. As a best practice, application security employs proactive, preventative methods to manage software risk, and aligns an organization's security investments with the reality of today's threats.

It has three distinct elements:

1) Measurable reduction of risk in existing applications.
2) Prevention of introduction of new risks.
3) Ensuring compliance with software security mandates.

Ultimately, it is the Chief Information Security Officer (CISO) or equivalent's responsibility to mitigate the enterprise's level of software risk as part of a comprehensive approach. When undertaken correctly, application security is a systematic process of reducing the risks associated with developing and running business-critical software. It moves the organization from a state of unmanaged risk to effective risk mitigation.

Application security is growing in complexity because the variety of business software continues to proliferate. Today's enterprises manage an increasingly complex software environment:

- ✓ Applications are heterogeneous – developed in a seemingly endless variety of programming languages: Java, .NET, C++, PHP, mobile OS and more.
- ✓ Applications are platform-agnostic, and deployed across myriad platforms – operating locally, over virtual servers and networks, accessed as SaaS in the cloud, or running on mobile devices.
- ✓ Applications are sourced in a supply chain – in-house development teams, commercial vendors, outsourced development, legacy applications and open source.

Each of these software development and deployment options, indeed each new wave of computing innovation, introduces new application security vulnerabilities. Enterprises concerned with application security need to help (not hinder) business innovation by promoting security in a simpler, more scalable way than past approaches.

Legacy security testing tools slow innovation.

Because traditional, ad hoc and manual solutions for application security actually *slow down* business innovation. The last generation of tools suites, installed on premise, imposed unnecessary complexity on today's fast-moving software development processes (e.g. agile). These heavy application security suites have proven difficult to configure, often requiring specialized expertise. Hiring more consultants or installing more servers is often necessary to scale them. The heartache: it can take months or even years to bring a global application infrastructure into corporate compliance using legacy approaches to application security.

On the other hand, ad-hoc and manual software testing tools are based on a decentralized model, making it challenging for CISOs to apply an enterprise-wide software security governance model. This leads to inconsistent policies, reporting and metrics across an enterprise's business units and development teams. As a result, enterprises that rely on ad hoc or manual solutions end up taking a fragmented approach to application-layer security. A large global organization may spend millions on with ad-hoc testing vendors or manual penetration testing consultants, but cover only a fraction of their application threat surface. This is no way to combat pervasive business risk.

There is a simpler, more scalable way.

Veracode offers a simpler and more scalable approach to reducing application-layer risk across an enterprise's entire global software infrastructure — including web, mobile and third-party applications. Enterprises can secure their entire in-house portfolio as well as their software supply chain using Veracode's single, centralized platform.

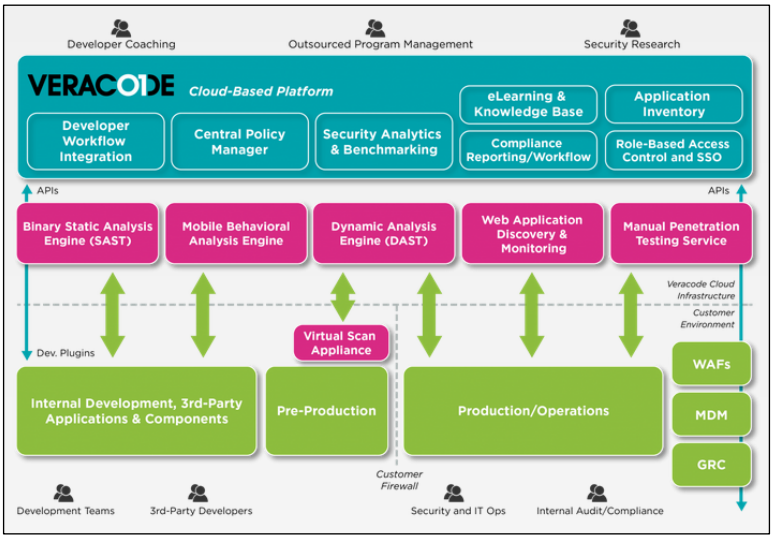
It's Smart. Veracode was designed by world-class experts in application security. It learns continuously with every new scan, combining multiple analysis techniques for optimum accuracy. This deep software security intelligence helps organizations address emerging and rapidly-evolving threats.

It's Cloud-Based. Veracode's SaaS platform was purpose-built to be hosted in the cloud and delivered as an on-demand service. Teams can start securing software immediately, without installing more servers and tools. The cloud simplifies information sharing across the enterprise. It's massively scalable to secure the largest enterprise's entire application infrastructure.

It's Programmatic. Veracode's program management services implement a centralized, policy-based approach proven with the world's largest companies. Our expert coaching accelerates adoption and helps rapidly remediate vulnerabilities using agile processes. Ongoing security governance and reporting is managed across global business units and disparate development teams.

Veracode's unified, cloud-based platform empowers consistent policies, metrics and reporting across multiple business units and disparate development teams. It aggregates the results of multiple analysis techniques (e.g. static, dynamic and manual) and allows test results to be shared with all stakeholders in a single dashboard.

Figure 1: Veracode's centralized platform delivers application security on demand.



Regardless of software development environment, the Veracode platform offers a centralized way to systematically reduce application-layer risk across an enterprise's **entire application infrastructure** *(Figure 1, in green)*. Veracode supports the entire software development life cycle (SDLC) from internal and third-party software to pre-production (Quality Assurance) testing and production/operations. Veracode's SOC-2 certification ensures that rigorous controls are applied to ensure sensitive data remains secure.

For optimum accuracy in identifying application-layer threats, the Veracode platform combines **multiple analysis techniques** *(Fig. 1, in pink)* including:

Static Analysis (SAST)
Static Application Security Testing tests applications from the "inside out", finding common vulnerabilities by performing a deep analysis of applications without actually executing them. Unique in the industry, Veracode's patented SAST technology analyzes all static binaries without requiring access to source code. It identifies common code vulnerabilities (e.g. SQL injection), unhandled error conditions and potential back-doors – even in custom and third-party code.

SAST supplements threat modeling and code reviews performed by developers, using automation to find coding errors and omissions more quickly and at lower cost. It's typically run in the early phases of SDLC because it's easier and less expensive to fix problems before going into production. SAST delivers actionable information that prioritizes flaws according to severity and provides detailed remediation information to help developers address them quickly.

Dynamic Analysis (DAST)
Dynamic Application Security Testing tests applications already in production from the "outside in", probing their exposed web interfaces. DAST looks for code vulnerabilities as well as architectural weaknesses that only surface when the application is running, such as authentication issues and server misconfiguration errors.

DAST takes the same approach as cyber criminals when probing the attack surface, such as deliberately supplying malicious data to input fields of web forms and shopping carts. It finds runtime issues that can't easily be found by looking at code in its offline state via SAST. Web applications can even be tested in pre-production staging—using Veracode's Virtual Scan Appliance (VSA) for local scanning. VSA is a pre-configured, software-based appliance that is locally-installed to probe web applications behind the firewall. VSA provides full DAST capabilities and then uploads results to the core cloud-based platform.

Web Application Perimeter Monitoring
This end-to-end dynamic testing solution starts with application discovery, proceeds to baseline scanning of 1000s of applications in parallel, and concludes with deep scanning to enable continuous, ongoing monitoring of the web perimeter. Veracode's massively parallel, cloud-based discovery provides visibility into all websites in a domain including unknown sites outside a corporate IP range. Unlike network IP scanners, it uses a combination of advanced search techniques – such as DNS keyword searches, production-safe crawling, analyzing page redirects and machine learning – to quickly identify unknown sites that network IP scanners miss.

Web application perimeters are constantly expanding as enterprises spin-up new websites for new marketing campaigns or geographies, create web portals for customers and partners, and acquire companies. Most organizations also have legacy and old marketing sites they're not even aware of. To reduce a global application threat surface that's growing all the time, Veracode's massively parallel cloud infrastructure rapidly discovers all public-facing applications and identifies the most exploitable vulnerabilities. Teams can take immediate action on identified risks and feed security intelligence to your existing Web Application Firewalls (WAFs) for rapid mitigation.

Mobile Application Security
This dynamic analysis offering quantifies mobile app risk by inspecting its real-time behavior in a controlled sandbox, which is compared against millions of known applications both malicious and safe to determine a risk rating. Static analysis is also employed to identify risky behavior such as hidden malware and coding errors such as buffer overflows.

When combined with Veracode's mobile app reputation knowledgebase, enterprises can secure their entire mobile software footprint. Gartner now recommends mandatory security testing and remediation of all enterprise mobile apps – whether bought, built or downloaded. Mobile application security testing provides the intelligence needed to protect against attacks and verify compliance with corporate risk and privacy policies.

Manual Penetration Testing Service
Veracode's world-class security experts find exploitable vulnerabilities with the benefit of specialized, real-world experience using the same methodologies cyber-criminals employ. Certain design, business logic and compound flaws such as cross-site request forgery — an OWASP Top 10 vulnerability — are only detectable via manual penetration testing. Combining manual with SAST and DAST automated techniques reduces false negative rates when evaluating the enterprise's most critical applications.

This collection of powerful analysis tools integrates testing results via application program interfaces (APIs) with the **Veracode Platform's core capabilities** (Figure 1, in blue) which include:

Developer Workflow Integration: Powerful APIs and plugins maximize developer productivity by seamlessly embedding security analysis into agile and continuous deployment workflows. Seamless integration with existing build and test processes encourages wide developer adoption. Enforce BYOD (Bring-Your-Own Device) policies with app behavioral intelligence fed to mobile management solutions.

Central Policy Manager: Custom security policies can be defined and uniformly enforced for web, third-party and mobile applications across all business units and distributed development teams.

Security Analytics & Peer Benchmarking: A suite of analytical dashboards deliver key metrics and benchmarks that give executives a clear and comprehensive way to measure the progress of global application security programs. Security teams can better understand the threat landscape and quantitatively compare their organization's security posture against industry peers.

eLearning: On-demand, cloud-based training codifies secure coding practices with all development teams. Formal training helps organizations comply with regulations and mandates such as ISO, PCI-DSS (Requirement 6.5) and SANS procurement policies.

Compliance Workflow Automation: Automated, pre-configured reporting and approval workflows simplify collaboration and application security compliance attestation for IT teams and internal audit committees. Veracode helps address PCI, SOX, HIPAA and NIST 800-53, among others.

Application Inventory: Veracode's platform tracks every application you are working on, all in one place. It consolidates internally developed, outsourced, open source and all software in the enterprise portfolio into a comprehensive view of the organization's security posture.

Role-based Access Control: Everyone has a stake in application security — from developers and auditors to executives and third-party vendors. A total of eleven distinct user roles are offered with pre-defined permissions. Cross-functional global teams can easily and securely collaborate with each other with unique rights and responsibilities.

Every enterprise has its unique challenge. What's yours?

Application security, at its best, is a collaborative effort. Robust programs involve the active participation of representatives from application development, IT operations, GRC audits, legal and even vendor procurement. Application security teams need to address the unique needs of these constituents to justify increased investment in securing the software that runs the business.

Here are five common application security challenges that global organizations confront:

1. We need to secure our software development, but not slow our SDLC.
2. We need to discover and protect *all* of our web apps, but in a fast and scalable way.
3. We need to comply with regulations and industry mandates, but streamline the process with automation.
4. We need to reduce the risk from third-party software – whether vendor, open source or outsourced.
5. We need to control mobile security risk whether we build, buy or download the apps our users demand.

Let's examine each of these solution requirements.

1. We need to secure our software development, but not slow our SDLC.

IT organizations need a better way to automate their secure development efforts so they can scale to protect the entire application infrastructure in a cost-effective manner — without hiring more consultants or installing more servers and tools. In today's agile development environment, the challenge is to protect the most applications without slowing the pace of software innovation with needless security gates. Being secure and agile need not be mutually exclusive.

With Veracode, testing occurs as a standard part of the nightly build cycle, delivering fast, short iterations to support continuous delivery. Both application upload and flaw ingestion are automated as well as automatic, policy-based flagging of release blockers. Developers are more productive because they never have to exit their IDE. Veracode allows development teams to secure applications from initial code design and development through pre-production testing and quality assurance (QA).

During initial development: Veracode experts recommend code-level analysis using SAST, in addition to security best practices such as secure architectural design and threat modeling. Addressing security during these early stages of the SDLC produces stronger application security at lower cost. Because SAST doesn't require source code access, third-party software such as commercial applications, outsourced code, third-party libraries and open source can also be covered.

During the pre-production QA phase: Veracode recommends using both SAST and DAST analyses. For highly critical applications, manual penetration testing is also recommended. Our solutions integrate with widely-used WAFs such as Imperva so you can quickly mitigate vulnerabilities via virtual patching. Since pre-production environments are usually located behind the firewall, Veracode's Virtual Scanning Appliance (VSA) allows full DAST capabilities to be locally installed.

Our multiple analysis techniques deliver a holistic, policy-based view of application layer threats across your infrastructure. Results of all three testing types are managed via a single set of policies and reports to maximize accuracy. Analysis is optimized for low false positives and prioritized based on standard measures of severity (e.g. OWASP Top 10 for web applications, CWE/SANS Top 25 for non-web applications), so development teams don't waste their time or remediation efforts.

To protect software across the entire Software Development Lifecycle (SDLC), application security solutions must integrate tightly with the developer's environment. Veracode supports all widely-used languages for desktop, web and mobile applications. Our scalable cloud-based platform works with agile development processes and tools including:

- ✓ IDEs such as Eclipse and Visual Studio.
- ✓ Build servers such as Jenkins, Ant, Maven and Team Foundation Server.
- ✓ Issue tracking systems such as JIRA, Bugzilla and RSA Archer GRC.

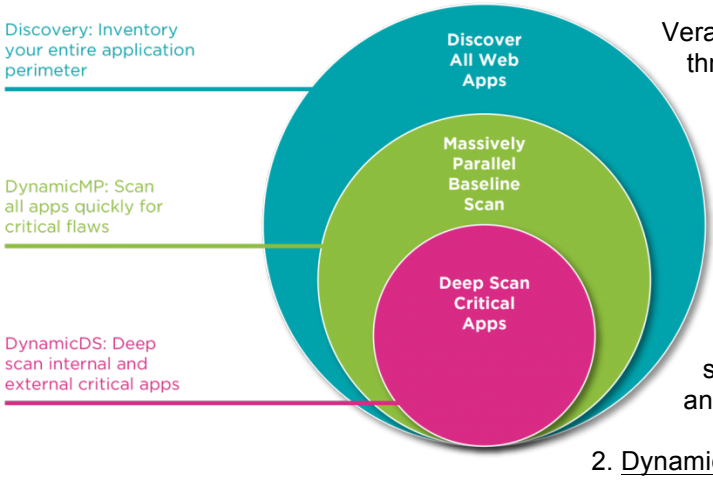
For more information on: Veracode for secure development.

2. We need to discover and protect *all* of our web apps, but in a fast and scalable way.

More than half of all data breaches involve web applications, yet most are not security tested before going into production. Many enterprises don't even know how many public-facing applications they have. Applications have become the path of least resistance for cyber-attackers because software is:

- ✓ Constantly exposed to the Internet and easy to probe by outside attackers using freely available tools that look for common vulnerabilities such as SQL Injection.

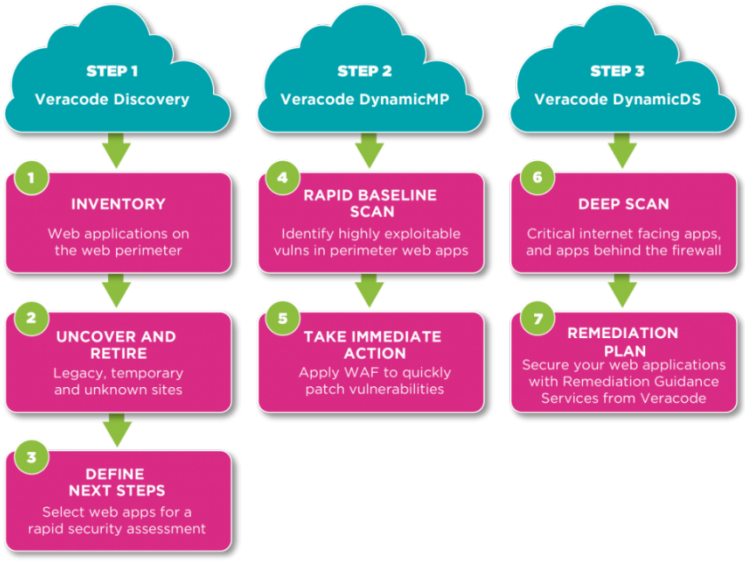
- ✓ Easier to attack than traditional targets such as network/host operating systems which have been hardened over time and walled off using next-generation firewalls and IDS/IPS systems.
- ✓ Driven by short development cycles that increase the probability of design and coding errors because security is often overlooked when the key objective is rapid time-to-market.
- ✓ Assembled from hybrid code obtained from a mix of sources including in-house, outsourced, third-party and open source — without visibility into which components contain critical vulnerabilities.
- ✓ Likely to present a larger attack surface with Web 2.0 technologies that incorporate complex client-side logic such as JavaScript (AJAX) and Adobe Flash.



Veracode addresses web application security in three steps:

1. Discovery: closes the visibility gap by creating a global inventory of all public-facing web applications leveraging Veracode's massively parallel, auto-scaling infrastructure to discover 1000s of applications per day. Safely identify production assets such as corporate sites, temporary marketing sites, portals, mobile sites, international domains, acquired sites and even related sites (info, mail).

2. DynamicMP (Massively Parallel): baselines application risk by inspecting 1000s of web applications simultaneously with lightweight, non-authenticated dynamic scans. It quickly identifies highly exploitable vulnerabilities with actionable feedback for developers.



3. DynamicDS (Deep Scan): performs a comprehensive deep scan that identifies web application vulnerabilities using both authenticated and non-authenticated scans, looking for attack vectors, insufficiently protected credentials and information leakage.

These approaches can be combined with Veracode's VSA to examine web applications behind the firewall. This secures them from insider attacks or attacks by malicious outsiders who gain access to user credentials.

At each step, Veracode's dynamic analysis feeds security intelligence to WAFs and consolidates what it finds with the core platform. Teams can take immediate action such as virtual patching and shutting down legacy sites.

Dynamic scanning complements other techniques such as SAST and manual penetration testing to find vulnerabilities in web applications at runtime. Veracode's end-to-end dynamic application security solution enables continuous, ongoing monitoring to maintain your security posture.

Your web application threat surface grows all the time. Security teams can replace fragmented ad hoc or manual testing approaches with a dynamic program to protect the perimeter. Go from having blind spots in your web application inventory to mitigating the most exploitable vulnerabilities across thousands of apps — in days not weeks.

For more information on: Veracode for web application security.

3. We need to comply with regulations and industry mandates, but streamline the process with automation.

Government and industry regulatory bodies, alarmed by the potential for widespread social and commercial damage, have been strengthening mandates in the area of application security. Many organizations are now required to address the risk posed by their applications, perform scheduled risk assessments and compliance audits, and then demonstrate compliance.

PCI, FISMA, HIPAA and FFIEC – these are only a few of the many regulations which specifically require a multi-layer security approach to strengthen data privacy and protection. Taking PCI-DSS as an example, 84 percent of organizations that suffered a data breach were out of compliance with application-layer security controls (Requirement 6) in 2014, compared to an average of only 47 percent of all organizations assessed a year earlier.[1] This suggests a strong correlation between the likelihood of suffering a data breach and non-compliance with PCI's application security controls.

Veracode's cloud-based platform assesses applications for compliance with standard controls such as PCI, OWASP and CWE/SANS. Policies can easily be customized to support specific corporate audit requirements as well as compliance requirements for SOX, HIPAA, NIST 800-53, MAS and other mandates. With automation, centralization and comprehensive controls, Veracode helps the largest global enterprises:

1. Achieve compliance. Strategic organizations understand that compliance does not equate to security. By implementing best practices for ongoing security, organizations can demonstrate compliance while at the same time preventing data breaches, loss of intellectual property, and fraud – which can all lead to business disruption, downtime and other material impacts.

2. Simplify compliance. Veracode helps simplify and lower the cost of compliance by maintaining a secure audit trail while automating common workflow processes such as notifications, approvals, policy changes and reporting. Enterprise-wide compliance status can be shared and tracked by business unit, development team and network operations — across your global application infrastructure.

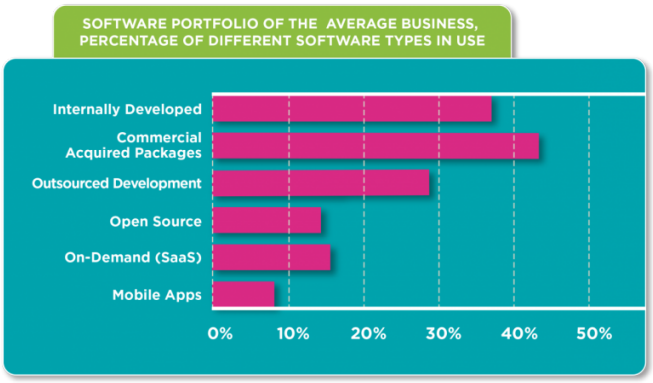
3. Maintain compliance. Security and compliance professionals understand that these are not periodic one-time events but rather ongoing activities. Veracode helps deliver continuous compliance by ensuring that application discovery, web perimeter monitoring, threat intelligence and automatic testing of new pre-production software occur as part of a frictionless application security compliance program.

For more information on: Veracode for compliance.

4. We need to reduce the risk from third-party software – whether vendor, open source or outsourced.

If you're like most businesses, more than two-thirds of your enterprise software portfolio is provided by third-parties — including commercial and outsourced applications, SaaS, third-party libraries and open source code.

[1] Source: 2014 Verizon PCI Compliance Report <link>



Source: Quocirca

Enterprises want to make sure all their vendor-supplied software is secure. Independent Software Vendors (ISVs) often need to prove to enterprise customers that their applications comply with security standards. Veracode helps both parties trust in their level of application security with our Vendor Application Security Testing (VAST) solution. More.

Software Supply Chain Security for Enterprises
Get all your vendor-supplied code up to internal security standards by letting Veracode work with your vendors to assess and remediate their code, and by helping you implement an application security governance process for third-party software based on industry best practices. Our SAST binary testing spots vulnerabilities even in third-party frameworks and components.

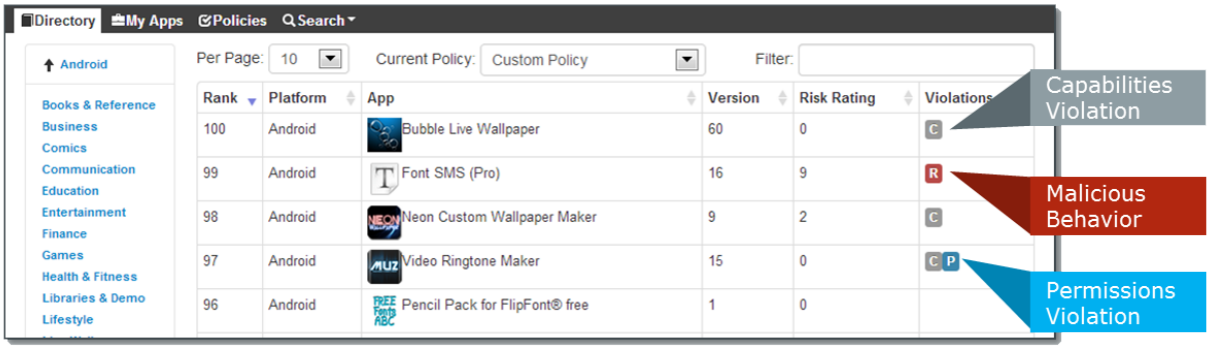
Independent Security Audits for ISVs
Customers asking you to prove that your applications are secure? Take the time, money and effort out of proving it. As a trusted, independent party, Veracode provides an unbiased audit and an alternative to self-attestation. Your development team gets detailed test results and step-by step remediation assistance, and doesn't share the results until you tell us to. Veracode lists your bulletproofed offerings in our VerAfied Directory so you can gain competitive advantage in the marketplace.

For more information on: Veracode for third-party security.

5. We need to control mobile security risk whether we build, buy or download the apps our users demand.

Mobile applications are some of the most innovative technologies being deployed by enterprises large and small. Apps may be developed to bring legacy enterprise applications to a new platform, respond to user demands for greater information access and collaboration, and support new business initiatives. However, they also expose the enterprise to new and little understood threats to business data and user privacy. It is estimated that *90 percent* of the top mobile apps have access to local files on the device. In your zeal to go mobile, don't neglect to effectively manage the security risks posed by mobile apps you build, apps you buy or apps downloaded by employees through BYOD programs. Veracode helps mobile teams strike the correct balance between innovation and control.

Veracode's mobile security solution is a combination of automated analysis and program services that enable IT teams to secure mobile applications during development, without slowing the pace of innovation. Veracode's behavioral analysis of mobile apps exposes risky and malicious app behaviors. It provides intelligence and controls to help you detect which apps violate your enterprise policies for security and privacy — and why.



Acting on mobile app behavioral intelligence, it's easier to mitigate those risks and enforce corporate BYOD policies. Assess apps before you buy or upload them to your enterprise app stores or secure application containers. Leverage our searchable directory of the most popular Android and iOS apps available from public app stores, including detailed ratings of each application. Set or change central policies for various employee groups. Developers can secure builds with app wrapping or choose more secure third-party component libraries. Veracode's mobile security intelligence integrates via APIs with leading MDM solutions including IBM/Fiberlink, VMware/AirWatch, Good Technology and MobileIron.

For more information on: Veracode for mobile security.

CONCLUSION

Past enterprise investment in information security solutions that protect only the network and end-point layers has proven ineffective against cyber attacks that increasingly exploit flaws at the application layer.

Today's CISOs are looking for pragmatic solutions that reduce application-layer security risk across their global software infrastructures – and across web, mobile and third-party applications.

Veracode's cloud-based platform and smart, programmatic approach provide enterprises with a simpler and more scalable way to reduce application-layer risk – so they can speed their innovations to market without sacrificing security.

ABOUT VERACODE

Recognized as a Gartner Magic Quadrant Leader since 2010, Veracode secures hundreds of the world's largest global enterprises – across web, mobile and third-party applications – including 3 of the top 4 banks in the Fortune 100 and 25 of the world's top 100 brands.