The Seven Habits Of Rugged DevOps

Strengthen Cybersecurity Using DevOps Culture, Organization, Process, And Automation

by Amy DeMartine and Kurt Bittner

October 15, 2015

Why Read This Report

DevOps practices can only increase speed and quality up to a point without security and risk (S&R) pros' expertise. Old application security practices hinder speedy releases, and security vulnerabilities represent defects that can leave a company open to cyberattacks. But DevOps practitioners can leap forward with both increased speed and quality by including S&R pros in DevOps feedback loops and including security practices in the automated life cycle. These new practices are called rugged DevOps. This report presents the seven main principles of rugged DevOps so I&O pros and developers can break down barriers with S&R pros and achieve faster releases with stronger application security.

Key Takeaways

Rugged DevOps Takes DevOps To New Heights

A partnership between developers and I&O pros can still leave S&R pros on the outside looking in. Developers and I&O pros will not achieve the highest levels of speed and quality until they include S&R pros in the automated life cycle.

Break Down Barriers To Utilize S&R Expertise

As with DevOps transformation, rugged DevOps practices require cultural transformation with S&R pros. Understand and empathize with S&R's goals, and then make incremental changes to include security assessment and remediation automation.

Don't Leave Your Application Open To Cyberattacks

Developers and I&O pros engaging in poor practices can leave applications open to cyberattacks. Engage in seven habits to create good security practices and build cybersecurity into applications and the systems that support them.

The Seven Habits Of Rugged DevOps

Strengthen Cybersecurity Using DevOps Culture, Organization, Process, And Automation

by Amy DeMartine and Kurt Bittner
with Stephanie Balaouras, Tyler Shields, Eveline Oehrlich, and Megan Doerr

October 15, 2015

Table Of Contents

Notes & Resources

Forrester interviewed five industry thought leaders for this report: Joshua Corman, Jez Humble, Gene Kim, Matt Konda, and James Wickett; as well as representatives from Blackboard, Dell, Disney, Intuit, nVisium, and Orbitz.

Related Research Documents

Five Steps To Reinforce And Harden Application Security

Improve Cybersecurity With DevOps

The Seven Habits Of Highly Effective DevOps

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

DevOps Pros Can Undermine Cybersecurity With Poor Practices

Anthem, Home Depot, the IRS, the Office Of Personnel Management . . . not a month goes by without news of a massive breach that costs millions and exposes the personal information of tens of millions of customers.[1] Additionally, Fortune 100 firms have had a material loss of intellectual property trade secrets and sensitive organizational data in the past two years.[2] These events highlight the clear and present danger of malicious attackers and insiders. Any web presence, but especially eCommerce websites and mobile applications, expose yet another attack vector that hackers are ready and willing to exploit. I&O pros and application developers are often only vaguely aware of the threats and lack knowledge about the proper methods for securing these applications. Too often they:

- **Integrate third-party software with known latent vulnerabilities.** Approximately 90% of modern applications consist of third-party software and open source software.[3] Developers can easily integrate third-party software that includes known and unknown vulnerabilities.[4] Even when developers are diligent about using secure third-party libraries, many times these libraries use other libraries of their own, resulting in latent unknown vulnerabilities that expose themselves at a later date.
- **Use unsafe development methods.** Developers can inadvertently use unsafe coding practices, creating security defects such as injection flaws, insecure direct object references, sensitive data exposure, cross-site scripting, and missing or malfunctioning authorization. Without proper code reviews, testing, identification, and remediation, these defects can slip into the production environment, where they lay waiting for exploitation.
- **Can't fix security issues as they arise.** Attacks will happen; the ability to respond to them quickly separates the high performers from the rest. Developers, S&R pros, and I&O pros need to work as a team to quickly identify and patch newly discovered vulnerabilities found in their own code as well as third-party software including open source components. When I&O pros don't have an easy way to understand the bill of materials for every application, long delays in remediating the vulnerabilities are the result.
- **Misconfigure application supporting systems.** Without consistent modeling, testing, and deployment in place, application components can be inconsistent, running unnecessary services, maintaining default users and passwords, or running vulnerable software. When a security breach occurs, I&O pros will have a difficult time identifying the sources of the problems in each uniquely configured application supporting system.

Improve Cybersecurity: Practice The Seven Habits Of Rugged DevOps

Application volume and complexity is exploding. As Joshua Corman, CTO of Sonatype and founder of rugged software/rugged DevOps, said, "Connected systems are expanding faster than we are able to secure them." Unfortunately, as organizations strive toward faster releases, they exacerbate the security problem by creating more of them.

> "Organizations are often understaffed for security and cannot protect against existing vulnerabilities, let alone new ones introduced by DevOps and continuous delivery practices that drive toward faster releases. Little security teams can have a big impact on reducing risk by embracing rugged DevOps and evolving their security programs to meet the needs of full-stack engineering at speed and scale." (Shannon Lietz, DevSecOps leader and senior manager of cloud security engineering, Intuit)

It is time for I&O pros and application developers to unite with S&R pros to limit the exposure that these application vulnerabilities present. Rugged DevOps is a new movement that's gaining momentum and that includes S&R pros on the integrated product team.[5] There are many definitions for rugged DevOps, but Forrester defines it as:

> *A method that includes security practices as early in the continuous delivery pipeline as possible to increase cybersecurity, speed, and quality of releases beyond what DevOps practices can yield alone.*

Rugged DevOps requires I&O pros, developers, and S&R pros to practice seven habits that make use of the continuous delivery pipeline — a series of tools that automates and orchestrates the application delivery life cycle — already established by DevOps practices (see Figure 1).[6] By practicing these habits, I&O pros will:

- **Left-shift security.** In traditional waterfall release cycles, security testing was often the last step before deployment and had a dedicated time for completion; that is, when organizations actually had time and resources for security testing. When organizations use DevOps and continuous delivery practices to deliver in very fast cycles, there isn't time for long security testing cycles. However, this new model of continuous delivery offers a great benefit to S&R pros by left-shifting security and embedding it into the application delivery cycle, giving developers and I&O pros faster feedback with which to fix security defects, and rugged DevOps mandates the inclusion of these embedded security practices.

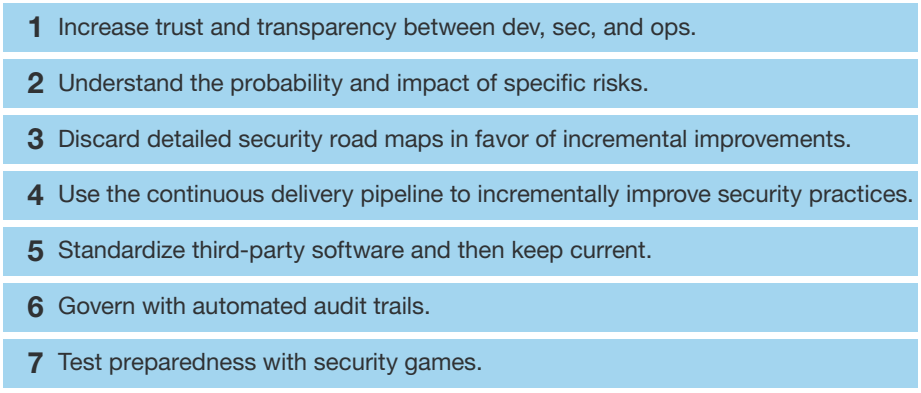
> "Security's biggest fear is being left behind because DevOps is going on with or without them. It's actually a great opportunity for security because developers and operations now have tools that allow them to address issues earlier. Everyone feels more accountable and more empowered to make security improvements." (Ed Bellis, CTO and co-founder, Kenna Security)

- **Automate audit trails.** Part of doing rugged DevOps well is automating a change tracking audit trail through the continuous delivery pipeline. This audit trail includes data such as a bill of materials that lists which software components are included in each application, which you can use to determine what changes other I&O pros have made to hardware and software components and if software or hardware configuration has drifted from its intended state. This information, combined with S&R pros' expertise, enables developers and I&O pros to identify and remediate security fixes faster. As Bellis said, "Security issues get fixed quickly through greater visibility into what is going into production and its security state."

› **Increase speed and quality of releases.** The premise of DevOps and continuous delivery is that throughput and stability increases through automation, smaller batch sizes, and shortened cycle times. Security vulnerabilities are defects and as such represent a decrease in the stability of a product. Without the injection of security measures in the development life cycle, developers and I&O pros will only be able to increase the speed and reliability of releases so far. For example, as Corman said, "When DevOps folks have done everything and yet are no longer accelerating, they will realize that to get to an even faster gear will require rugged software supply chain practices included in the life cycle."

› **Decrease mean-time-to-repair (MTTR).** You can't close every vulnerability or prevent every attack. When attacks occur, organizations that respond rapidly are more secure than their slower peers. Rugged DevOps practices provide organizations with the means to respond quickly with reliable patches and countermeasures that do not add further vulnerabilities.

FIGURE 1 Practice Seven Habits To Achieve Highly Effective Rugged DevOps



Habit 1: Increase Trust And Transparency Between Dev, Sec, And Ops

No matter where you are in your DevOps journey, you must immediately include security pros on the integrated product team and learn to be empathetic to each other's challenges and goals.[7] John Allspaw, senior vice president of technical operations at Etsy, said that "getting people to feel empathy for the pains that another group or challenges another group has to face is a good place to start."[8] Or as Corman said, "Either evolve to be empathetic or remain pathetic." To be empathetic, realize that:

- **Developers don't like unplanned or unscheduled work.** The firm measures developers on delivery of new features; fixing security defects can represent unplanned, unscheduled work. Developers are able to write more secure code when they get early, in-context feedback. As David Mortman, distinguished engineer and Dell chief security architect, said, "Security issues are product quality issues, and no one wants to write buggy code."

> Begin rugged DevOps habits by understanding what motivates developers, S&R pros, and I&O pros.

- **S&R pros don't like security breaches or vulnerabilities.** The firm tasks S&R pros with decreasing the exposure of the company and its customers to the loss of data and intellectual property. One way they do this is to reduce the attack surface, or the points at which hackers can gain entry into an environment, gain unauthorized access to apps, and steal data. S&R pros are the go-to resource for developers and I&O pros for the latest information on security vulnerabilities and remediation strategies.
- **I&O pros don't like outages or performance glitches.** I&O pros pride themselves on understanding the interconnectedness of the hardware and software environment, and they are unnerved by complexities that poorly governed delivery practices create because the firm rates I&O pros on their ability to improve the performance and stability of the production environment. To maintain the environment, they must reduce the chances of an outage or interruption of service, and they must reduce the MTTR when an issue does occur. Security breaches represent an interruption of service, but I&O pros struggle to understand what environment conditions create vulnerabilities and how to remediate them.

Habit 2: Understand The Probability And Impact Of Specific Risks

While developers and I&O pros do not need to become security experts, they do need to know how cybercriminals exploit application vulnerabilities, how their decisions affect security, and how they can work with S&R pros to decrease the attack surface and respond quickly to attacks. For example, third-party and open source components are a particular source of risk, as attackers exploiting a single vulnerable component can affect all applications that use it. Considering that 90% of code in modern

applications is open source and 31% of companies have had or suspect a breach in an open source component, gaining control over open source risks is essential to improving security.[9] To help educate developers and I&O professionals on the probability and impact of risk:

- **Make developers and I&O pros part of the solution.** S&R pros can help developers and I&O pros learn how to build security into applications by working with them to add security scanning tools that identify vulnerabilities into the continuous delivery pipeline. This enables them to identify and remediate vulnerabilities as early as possible.

"A developer comes to me and says what they think an issue is and the potential solution to the problem. This starts the conversation and education on issues and their priorities. No one likes their stuff broken. They have a pride in their work and want to do it well. They take it personally." (Mortman)

- **Use real-life examples of breaches.** Examples from current headlines abound, such as security breaches at Chase and Target. Use these to discuss real-life threats and vulnerabilities and prevention and detection methods you can take to stop or mitigate similar cases. Ken Johnson, chief technology officer at nVisium, told us that "everybody cares about security because they know that the threats are real. Developers and operations know what they didn't know before."

Habit 3: Discard Detailed Security Road Maps In Favor Of Incremental Improvements

The current approach to app security puts S&R pros in the role of gatekeeper or nag who only points out vulnerabilities or errors but doesn't have the bandwidth or opportunity to resolve them. To change this paradigm, S&R pros need to focus on how they can embed security into existing continuous delivery processes. Letting go of the old approach allows S&R pros to embrace the opportunities that new life-cycle automation enables. Doing so enables S&R pros to collaborate with developers and I&O pros to create ways to develop and deliver secure applications while increasing delivery speed. As Bellis said, "Security measures can't be outside of the continuous delivery process. If you try to add security processes outside, you will fail." However, DevOps practices emphasize making small, incremental changes that you can release and test quickly. As such, old security programs that include detailed road maps for improvements will no longer work. Instead, S&R pros must define security goals rather than cling to old processes.

> Let go of old security road maps and embrace new security goals that incrementally embed security assessment and remediation automation into the life cycle.

"In some ways, it is more helpful to have a vision rather than detailed long-term plans. The vision needs to be that we are going to get much better than we are today and here's generally how we can get there through controls and the ability to change. We are going to solve a good number of issues, but we don't always know which ones or at which times. Security in DevOps needs to embrace change." (Matt Konda, founder of Jemurai and OWASP Global Board member)

Your new security goals should be to:

› **Make incremental improvements.** Every organization and application is different in its security needs. S&R pros need to prioritize improvement opportunities based on reducing the most risk exposure for the least amount of effort. For example, a possible quick win is to identify coding practices that inadvertently insert vulnerabilities by adding appropriate dynamic testing to the continuous delivery pipeline automation.

"You get big favors in small incremental improvements. Look to see what's next for improvement, such as scans in production, peer code review, or static analysis as part of the life cycle. Even if you take a few steps back, you will be trending where you want to be." (Bellis)

› **Make security a part of the continuous delivery pipeline to free up S&R pros.** Organizations need S&R pros to identify new vulnerabilities and effective remediation practices; they need them to constantly adapt the organization's security practices to address new threats. To keep pace, I&O pros and developers need to become more responsible for application and operational security by building security testing inside the continuous delivery pipeline. Mortman told us that "automation frees up [S&R pros] to do the hard part, such as measuring what kinds of bugs and vulnerabilities are being generated to find out where better training is needed."

Habit 4: Use The Continuous Delivery Pipeline To Incrementally Improve Security Practices

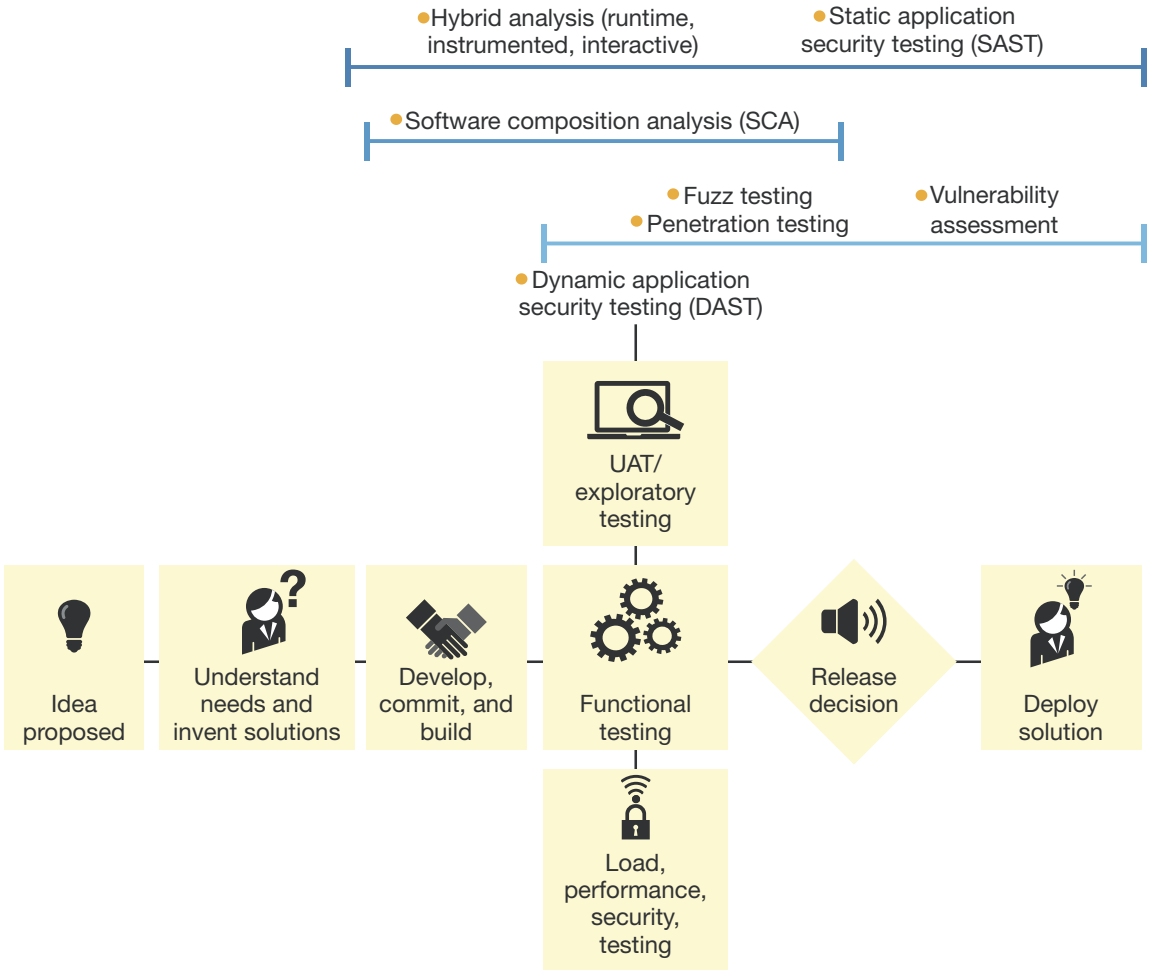
Overall, S&R pros are not satisfied with current app security processes. While some parts are effective, holes still remain in comprehensive app security programs. Konda told us that "no one thinks their security processes are consistently working. We still aren't able to produce positive results in a reproducible way. That's one reason why we want to keep learning and embrace change." The continuous delivery pipeline allows S&R pros to insert automated scans and tests at various stages of the delivery process. This gives S&R pros unprecedented opportunities to test while making it easy for developers and I&O pros to incorporate feedback in context, leading to higher release quality. S&R pros, developers, and I&O pros need to cooperatively develop an app security program. To do this, you must:

› **Augment the existing continuous delivery pipeline.** Developers, I&O pros, and S&R pros must augment existing automated tests across the life cycle with security tests based on a particular application's attack surface and risk profile (see Figure 2). For example, when developers check in code, they can perform static analysis to check for vulnerable coding practices so that developers can immediately remedy the vulnerability while the code change is still fresh in their minds.

"We used the continuous delivery pipeline to combat our biggest issues. We were able to build tests, get notification emails when there was a problem, and notification when new releases were deployed into production. We couldn't miss when an important event occurred." (Johnson)

› **Incrementally grow and modify automated security tests.** As hackers get smarter and faster, organizations have to find and fix new vulnerabilities faster, too. S&R pros, developers, and I&O pros need to respond by continuously changing the testing and tool mix. As Mortman said, "One of the great improvements is the automated continuous delivery pipeline and increasingly putting automatic security quality assurance into their processes."

FIGURE 2 Apply Security Tools Across The Application Life Cycle



Habit 5: Standardize Third-Party Software And Then Keep Current

Standardizing third-party software reduces license fees, education costs, and maintenance costs while also reducing risk. Developers, I&O pros, and S&R pros should use a single version of a third-party software component or tool to perform a task. Lack of version standardization can lead to bloated software and unpatched vulnerabilities when developers choose old versions of open source components, or when they don't patch applications when newer versions become available. Rugged DevOps teams must:

- **Pay close attention to open source software . . .** Today, one out of every 16 open source component download request is for a component with a known vulnerability.[10] In addition, 97% of the successfully exploited vulnerabilities in 2014 trace back to 10 common vulnerabilities and exposures, eight of which have been patched for 10 to 12 years.[11]
- **. . . while also considering all third-party software.** I&O pros, developers, and S&R pros not only need to focus on the risk presented from open source software but also from all third-party software, such as middleware, OS, network, database, and performance management tools.[12] You even must standardize and keep current security tools applied across the continuous development pipeline.

Habit 6: Govern With Automated Audit Trails

One out of every 16 downloads of open source component requests are for a component with a known vulnerability.

Continuous delivery pipeline automation enables S&R pros to view audit trails through logs, versioning tools, and content management tools that track environment, application, and third-party software and security configuration changes without cumbersome manual change management or quality reviews.[13] Through this automation, all these changes are logged and traced to a particular time and owner. To ensure that governance through the continuous delivery pipeline is working properly, I&O pros, developers, and S&R pros need to:

- **Create appropriate security alerts.** S&R pros need to use this transparency to work with I&O pros to create thresholds and alerts and corresponding notifications when anomalies occur that indicate a potential malicious attack. For example, a spike in login attempts may indicate a denial of service attack. Bellis told us that "with automatic alerts based on metrics and log files, your ability to detect anomalies is much greater and faster. You know exactly what has changed and how to react to fix that change in real time."
- **Use the continuous delivery pipeline for high-risk changes.** You should use an augmented life cycle that includes additional security for high-risk changes, or those that have a great probability of having a high customer impact. You must flag these changes when an integrated product team

member creates the requirement to indicate that the broader integrated product team needs to be aware when the integrated product team member makes the change and when the continuous delivery pipeline deploys the change.

- **Enable proper authentication and authorization on all systems.** Lock out all but critical personnel on application systems and supporting systems. Remove all direct calls from applications with user names and passwords and use a service that can be queried to provide access. Ensure that proper logging of any authentication or authorization changes happen automatically or increase security around authentication and authorization by making use of privileged identity management (PIM) solutions.[14] No matter what steps you take, you need a judicious role-based access policy to the production systems including full auditing and accountability.
- **Track drift across development, testing, and production environments.** Track any change from the model or "drift" of the application systems and supporting systems. For any drift you find, either modify the model using configuration management or application release automation tools, for example, or remove the change.
- **Define quality gates as a part of the continuous delivery pipeline.** Use output data from security tools along with other testing tools as inputs to automatic quality gates in the application life cycle. S&R pros need to define what to look for from the security tools that will indicate a vulnerability that I&O pros or developers must fix before release.

Habit 7: Test Preparedness With Security Games

You can use penetration tools and destructive testing to test an application by trying to break application security or the security of the supporting systems of an application, such as the network, database, and OS. Some common packaged application penetration tools are Rapid7 Metasploit and Burp Suite, while common open source destructive testing tools include Chaos Monkey, Chaos Gorilla, and Chaos Kong. However, to get the full value out of these penetration and destructive testing tools, red team-blue team (red teaming) games should involve developers, I&O pros, and S&R pros. Red teaming has roots in military exercises to test preparedness. The red team attacks something while the blue team tries to defend it.[15] In the case of rugged DevOps, a group of I&O pros, developers, and S&R pros are split into a red team and a blue team. All members of an integrated product team are rotated into the games to get equal exposure. Red teaming can be intermittent or scheduled regularly. I&O pros, S&R pros, and developers use red teaming to:

> Test your security preparedness, build security knowledge, and strengthen team relationships with red teaming games.

› **Speed identification.** The defending blue team uses monitoring and reporting tools to identify how the red team is attacking. If the blue team is unable to detect the attack, they are helpless to try to remediate. Developers and I&O pros can use blue team experiences to close any gaps in monitoring and reporting.

"When the red team attacks, the blue team acts quickly to determine if the attack can be discovered, tune event monitoring, and contain the incident quickly. Developers and operations staff are an extension of the blue team and included so that they can become aware of unknown unknowns that cannot be discovered by tools alone. From this, everyone can work collaboratively to improve the safety of workloads through direct and actionable testing, measurement, and reporting." (Lietz)

› **Improve response time.** Once the blue team identifies the red team vulnerability, it tries to remediate through methods such as rolling back to previous application releases, rolling forward to new application releases, or making configuration changes or an entirely new stack of the application and its supporting systems. This process tests how fast they can create, build, test, and deploy changes. Developers and I&O pros can use these tests to determine improvements to the release life cycle. "Be mean to your code, do it a lot, and use the information to reduce your release [technical, process, and security] debt," said Corman.

› **Create better testing.** I&O pros and developers can use found vulnerabilities from red teaming and create better testing to harden future releases. Red teaming is eye-opening for developers and I&O pros who may have a hard time understanding the persona of a malicious attacker and how that persona might take advantage of vulnerabilities. As Konda told us, "It's hard to prepare for the unknown and to see your applications from the perspective of a malicious attacker. When developers and operations start to think about applications from this perspective, it helps them rationalize that it's not easy to test for and spend extra time consciously working on that."

What It Means

The Future Is Secure, Adaptive Applications

Threats are constantly evolving; the way organizations and applications respond needs to constantly evolve and improve as well. Current security measures are trying to not make anything worse while incrementally fixing what is broken through the use of automated detection of potential vulnerabilities. Remediation of vulnerabilities often requires the manual intervention of developers, I&O pros, and/or S&R pros. The tools of today will evolve to eliminate this manual step. In the future, tools will first be able to make suggested fixes to identified vulnerabilities and then progress to being able to remediate under certain conditions to full self-healing. The continuous delivery pipeline will enable this self-healing by allowing these security tools to automatically create, build, test, and deploy fixes to the application and its supporting systems.

Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

Analyst Inquiry

Ask a question related to our research; a Forrester analyst will help you put it into practice and take the next step. Schedule a 30-minute phone session with the analyst or opt for a response via email.

Learn more about inquiry, including tips for getting the most out of your discussion.

Analyst Advisory

Put research into practice with in-depth analysis of your specific business and technology challenges. Engagements include custom advisory calls, strategy days, workshops, speeches, and webinars.

Learn about interactive advisory sessions and how we can support your initiatives.

Supplemental Material

Companies And Thought Leaders Interviewed For This Report

Blackboard
Joshua Corman
Dell
Disney
Gene Kim
Jez Humble
Intuit
Matt Konda
nVisium
Orbitz
James Wickett

Endnotes

[1] For more information on the cost of cyberattacks and other security incidents, see the "The Cybercriminal's Prize: Your Customer Data And Intellectual Property" Forrester report.

[2] Source: AppSec EU15, "Continuous Acceleration: Why Continuous Everything Requires A Supply Chain Approach," OWASP's YouTube channel, June 8, 2015 (https://www.youtube.com/watch?v=0mUN3RppEHE).

[3] Source: AppSec EU15, "Continuous Acceleration: Why Continuous Everything Requires A Supply Chain Approach," OWASP's YouTube channel, June 8, 2015 (https://www.youtube.com/watch?v=0mUN3RppEHE).

[4] For more information about how software composition analytics (SCA) tools can find vulnerabilities in third party source software, please see the "Vendor Landscape: Software Composition Analysis" Forrester report.

[5] For more information about how to create an integrated product team, see the "Playing Musical Chairs For Staffing Modern Service Delivery" Forrester report.

Forrester has recommended including S&R pros into the integrated product team; however, adoption of this model has lagged due to a misalignment of S&R goals with DevOps goals.

[6] For more information about how to create a continuous delivery pipeline of the application life cycle, see the "Gear Up For Modern Service Delivery" Forrester report.

[7] For more information about how to create an integrated product team, see the "Playing Musical Chairs For Staffing Modern Service Delivery" Forrester report.

[8] Source: "John Allspaw Discusses Devops and Continuous Delivery," Continuous Delivery, September 25, 2012 (http://continuousdelivery.com/2012/09/john-allspaw-discusses-devops/).

[9] Source: AppSec EU15, "Continuous Acceleration: Why Continuous Everything Requires A Supply Chain Approach," OWASP's YouTube channel, June 8, 2015 (https://www.youtube.com/watch?v=0mUN3RppEHE).

[10] Source: "2015 State of the Software Supply Chain Report," Sonatype (http://www.sonatype.com/resources/whitepapers/2015-state-of-the-software-supply-chain-report-hidden-speed-bumps-on-the-road-to-continuous).

[11] Source: AppSec EU15, "Continuous Acceleration: Why Continuous Everything Requires A Supply Chain Approach," OWASP's YouTube channel, June 8, 2015 (https://www.youtube.com/watch?v=0mUN3RppEHE).

[12] Source: Bruce Schneier, "Oracle CSO Rant Against Security Experts," Schneier on Security, August 17, 2015 (https://www.schneier.com/blog/archives/2015/08/oracle_ciso_ran.html).

[13] For more information on tools required for the continuous delivery pipeline, see the "Gear Up For Modern Service Delivery" Forrester report.

[14] For a list of the most influential PIM vendors and how they stack up, see the "The Forrester Wave™: Privileged Identity Management, Q1 2014" Forrester report.

[15] Source: Robin Mejia, "Red Team Versus Blue Team: How to Run an Effective Simulation," CSO Online, March 25, 2008 (http://www.csoonline.com/article/2122440/emergency-preparedness/red-team-versus-blue-team--how-to-run-an-effective-simulation.html).

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
- Infrastructure & Operations

Security & Risk
Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.