radware

EVOLVE AND ADAPT: WHY DEVOPS IS RAISING THE BAR FOR SECURITY SOLUTIONS

Agile software development practices are like a double-edged sword. On the upside: they fuel tighter collaboration between IT and business, enable frequent changes to systems and processes, and allow organizations to more quickly capitalize on emerging opportunities and challenges. The downside: it's harder than ever to keep these systems secure. In an environment where change is the only constant, how is security expected to keep pace?

As organizations work to drive higher IT and organizational performance, many are embracing agile and DevOps methodologies. These approaches emphasize strong connection between IT and the business and focus on continual improvements. They also strive to speed up delivery while improving quality, security and business outcomes.

For its 2016 State of DevOps Report, Puppet Labs surveyed 4,600 technical professionals. In analyzing the results, Puppet identified three types of organizations:

- High IT performers, which complete multiple deployments per day
- Medium IT performers, which deploy between once a week and once a month
- Low IT performers, which deploy once per month or less frequently

The study found that high IT performers deploy 200 times more frequently than low IT performers. Further, their lead times are 2,555 times faster and recovery times are 24 times faster than their low-performing counterparts. It would be tempting to assume that frequent deployments could lead to higher failure rates. However, one of the study's surprising findings is that high IT performers have three times lower failure rates. These high IT performers also spend 22% less time on unplanned work and rework—reflecting a high level of quality.[1]

According to another industry study, 20% of organizations emerged as advanced adopters of DevOps.[2] Similarly, according to Radware's *2016-2017 Global Application & Network Security Report*, 18% of respondents told us they deploy application changes to production at least once a day, suggesting that they are high IT performers.

The trend is clear: agile development practices and DevOps have become mainstream. What does it mean for security?

Bridging the Gap

While DevOps offers tangible advantages in terms of improved quality and speed to market, it introduces complications for implementing and auditing security controls. Among the issues: constantly changing assets, continuous deployments and a breakdown in traditional segmentation of duties. Indeed, how best to integrate security into DevOps remains a pressing challenge for all stakeholders. And while security objectives should be prioritized alongside other business goals, in reality implementations often fall short.

Chalk it up to a number of traditional security tools and controls that are at odds with agile and DevOps methodologies. These include:

- **Penetration testing**. On average, it takes several weeks to test, produce and assess the report, and then implement necessary security changes in development and production. That cadence is clearly at odds with the pace of deployments in a DevOps model.

- **Web Application Firewall (WAF)**. Initial implementation cycles can take weeks, while security policy modifications can take even longer—often requiring manual changes. Four out of five organizations report at least a medium degree of manual work to try and optimize their WAF.

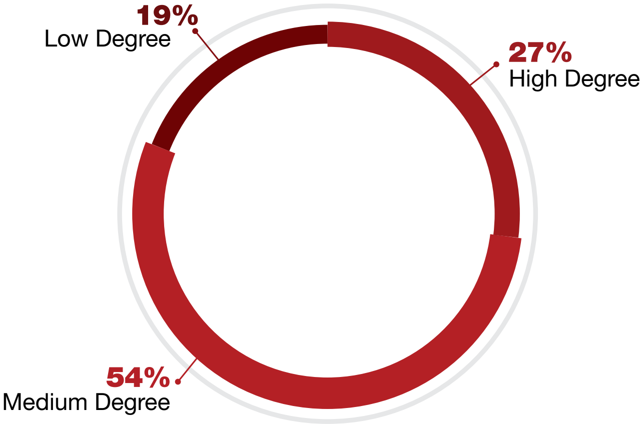

Figure 1: What level of manual tuning does your application security solution require?

- **Code analysis methodologies**. A medium-sized enterprise application can take days just to scan. The results of such a scan may reveal issues that require additional time to remediate.

Radware's security industry survey underscores the prevalence of these traditional tools, with 75% of respondents using WAF. One-fourth said they only use one method to secure their applications (most often on-premise WAF or penetration testing) and 66% reported relying on multiple tools and controls.

[1] https://puppet.com/company/press-room/releases/puppet-2016-state-devops-report-addresses-most-pressing-issues-devops
[2] Assembling the DevOps Jigsaw survey by Freeform Dynamic

Hallmarks of High Security Performance

When integration and delivery are continuous, security needs to be as well. Yet traditional security solutions are not designed to keep up with the speed and complexity driven by DevOps methodologies. The key is an adaptive security service that allows the IT organization to addresses two fundamental challenges:

- **Keeping pace with evolving threats**. An adaptive security service can detect and mitigate newly evolved threats by using a “positive” security model. In other words, the service should heuristically identify legitimate traffic—and treat all other traffic as suspect. This approach is in stark contrast to traditional “negative” models, which focus on blocking traffic that matches known attack signatures. Given the pace at which signatures emerge and change, the “negative” model is more likely to miss the latest threats. Another key capability: the ability to block attackers and spammers based on their real identity. This requires use of IP-agnostic device fingerprinting versus tracking of IP addresses, which are continually obfuscated by attackers.

- **Keeping pace with evolving assets**. An adaptive security service should automatically detect new application domains, analyze potential vulnerabilities, and automatically assign optimal protection policies. This should be followed by automatic identification of any changes in these applications as they are continuously integrated by developers. Automation should also support testing for newly introduced vulnerabilities, as well patching application protections in real time to mitigate them.

Look for a continuous security delivery service that integrates detection tools, such as Dynamic Application Security Testing (DAST), with mitigation/blocking controls, such as WAFs. This combination provides immediate resolution of newly introduced vulnerabilities via automated real-time patching, as described above. Automated independent security controls with self-adjusting rules and policies can assist in conducting scans that focus on the application zones that have been changed. That saves time and accelerates detection of vulnerabilities.

Given the rate and pace of change in both external threats and internal applications, now is the time for a new paradigm for security services. Insist on a service that has been designed for agile development environments and that adapts the protections of evolving Web applications, thereby delivering effective protection at every stage of the development lifecycle.

Download the 2016-2017 Global Application & Network Security Report to learn more.

www.radware.com/ert-report-2016

Learn More at DDoS Warriors

To know more about today’s attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware’s Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.