Making Security Agile

2017 - INVITING SECURITY INTO DEVOPS SURVEY
CEOs are caught between a rock and a hard place. On one hand, there is tremendous pressure to digitally transform their companies. As a recent Wall Street Journal article put it, “In an age of rapid disruption by the software and tech industries, a leader has to pick up the tempo and make riskier bets sooner...or else.”

Yet, moving too quickly can open a company to security risks. A recent survey underscores this, finding **vulnerable apps cause most mobile security breaches.**

The fundamental problem is that faster app development is the enemy of better cybersecurity. How can enterprises increase both at the same time? Especially when DevOps – whose mission it is to speed development agility – and security operate independent of each other.
For many enterprises, the answer is to invite security into the DevOps fold. To better understand this trend, DigiCert recently commissioned a survey of 300 U.S. enterprises in an effort to explore whether organizations are breaking down the silos and inviting security to join the DevOps movement. We began by asking enterprises to name their most important enterprise goals. Reflecting the pressures outlined above they chose increasing information security, increasing IT agility and increasing development agility.

How important are each of the following to your organization? (Somewhat/Extremely Important)

- Increasing Information Security: 90%
- Increasing IT Agility: 88%
- Increasing Development Agility: 87%

The challenge, of course, is that these goals normally conflict with one another. Going faster often means introducing security risks while maximizing security often means slowing things down. To increase agility and security would require changing how security works within the organization.
It turns out that enterprises have a strong interest in integrating security into DevOps; 88 percent rated doing so as somewhat/extremely important. The top two reasons they cited as driving this interest were to speed application development as well as security.

“The faster that we implement something, the more likely it is to have vulnerability issues,” says James, an IT manager for a large central U.S. manufacturing firm, who participated in our study. “That’s why for us security is so important; it saves us time and money in the long run.”

Survey respondents noted the top three dangers of operating security outside of DevOps were increased costs, longer delivery cycles and increased security risk.

“The last thing you want is to be in the Boston Globe due to a major security breach,” says Marsha, an IT Director for a large Boston-based government department.

With such strong interest, we were interested in how far along enterprises were in terms of integrating security into DevOps.
Security DevOps Tipping Point

Roughly half (49 percent) of the enterprises we spoke to have already integrated security into DevOps, with an equal amount actively working on completing that integration. Less than two percent have no interest in doing so.

“The security team was adamant from the get-go that DevOps included security,” says Paul, an IT manager for a large healthcare provider in the southwest. “They wanted to make sure that every angle of attack, every potential vector, every potential risk could be thought of ahead of time to minimize the potential for patient data to be exposed publicly.”

It isn’t easy to make this transition. The top three challenges cited were that it takes too long, security teams resist the change and that it requires strong relationship skills to perform the integration.

“It has been difficult integrating security and development,” says Daniel, a senior project manager for a large New York-based printer manufacturer. “The security folks are just different animals, but then, so are the developers. You have to deal with egos and fights over methodologies.”

Who’s Integrating Security into DevOps?

49% Working on completing integration
49% Have already completed integration

“The security team was adamant from the get-go that DevOps included security.”

“They wanted to make sure that every angle of attack, every potential vector, every potential risk could be thought of ahead of time to minimize the potential for patient data to be exposed publicly.”

-Paul, IT manager
Security and DevOps Challenges

It is interesting to note the challenges reported by those who have already completed the transition are slightly different than the challenges anticipated by those in the process of making the transition. Before making the transition, enterprises predict the top challenges will be:

- The organization structure prohibits integration
- They lack a champion for the transition
- The security team doesn’t really work well in a team environment
Yet, once an enterprise has completed the transition their perception of the challenges changes dramatically:

- **Takes too much time**
- **Security team resists the change**
- **The relationship skills to integrate the two teams**

Note the top challenge cited after the fact was that the transition took too long. Those who haven’t completed the challenge estimate the integration will take less than a year (seven to 11 months). Those who have completed the transition say it took an average of 1 to 2 years – roughly twice as long.

Clearly, it is a lot of work. Is it worth the effort?
Integration Pays Off

Respondents overwhelmingly report that the effort to integrate security into DevOps is worth the effort. In fact, those who have completed the transition report they are doing well in a variety of key areas:

- **Increased information security**
- **Achieving application deadlines**
- **Lowered application risk**

22% more likely to say they are doing well at information security

21% more likely to say they are doing well at meeting application delivery deadlines

21% more likely to say they are doing well at lowering application risk

Most notably, performance was better across the entire spectrum of metrics we measured.

“We’ve found that agility was actually a byproduct of putting security upfront,” says Duane, a senior project manager at a large metals manufacturer in the northeast. “If you really want to be agile, you don’t want to do things twice.”
Recommendations

What can enterprises do to balance agility with security? How can they integrate security into DevOps to achieve faster, more predictable and lower-cost app development?

Appoint a Social Leader
Identify a champion to drive cultural change including defining IT, security, DevOps roles and integrating teams.

Bring Security to the Table
Place a security lead on all DevOps initiatives and involve them from the beginning. Limit access, sign and encrypt everything within network using automated PKI.

Invest in Automation
Automate baseline security practices within DevOps workflow, including: certificate management, patching, vulnerability scanning and static code analysis.

Integrate and Standardize
Implement controls on certificate management processes and integrate with server configuration and orchestration platforms to enable automated security behind the scenes.
Agility or security? It is a false choice, as enterprise needs both to survive and prosper. Go too slow, and you lose out to the competition. Neglect security and you open the enterprise to unacceptable risk. Enterprises need both agility and security, and inviting security into DevOps is a step in that direction.

Learn more about what enterprises can do to achieve more predictable and faster app development while also integrating security. Visit www.digicert.com/mpki/