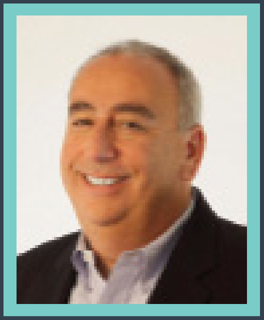
Security for Startups in a DevOps World

Table of Contents

About the Authors



Alan Shimel, Founder and Editor-In-Chief of DevOps.com

An often-cited personality in the security and technology community and a sought-after speaker at industry and government events, Alan has helped build several successful technology companies by combining a strong business background with a deep knowledge of technology.

Rajat Bhargava, Co-Founder and CEO of JumpCloud

Rajat Bhargava is co-founder and CEO of JumpCloud, the first Directory-as-a-Service. JumpCloud securely manages and connects employees identities to their systems, applications, and networks. An MIT graduate with over two decades of experience in industries including cloud, security, networking and IT, Rajat is an eight-time entrepreneur with five exits including two IPOs, three trade sales and three companies still private.

Ben Tomhave, Security Architect with New Context

Ben Tomhave is a Security Architect with New Context, a Lean Security company that automates the orchestration, governance, and protection of critical infrastructure and the industrial internet. He holds a MS in Engineering Management from The George Washington University and is a CISSP. He's previously held positions with Gartner, AOL, Wells Fargo, ICSA Labs, LockPath, and Ernst & Young. He is former co-chair of the American Bar Association Information Security Committee, a senior member of ISSA, former board member for the Society of Information Risk Analysts, and former board member for the OWASP NoVA chapter. He is a published author and experienced public speaker, including engagements with the RSA Conference, MISTI, ISSA, Secure360, RVAsec, RMISC, DevOps Connect, as well as Gartner events.

Most startups have so much promise and potential, even though they begin under conditions of extreme uncertainty.

They have to execute and work fast to build, measure, and learn what their products and services offer, without generally having significant resources. Startups don't have the same budget as large corporations do to accomplish similar tasks. The staff size is much smaller and often less specialized since there is so much to do. And because the company hasn't been around a long time, they haven't established well-worn processes that help them execute on critical tasks. Therein lies the conundrum for startups: they must secure their organization while managing everything else.

The modern era of IT, with its cloud-based services and low-cost solutions, is empowering many entrepreneurs. Amazon Web Services (AWS), for example, is a significant solution for new organizations. Startups no longer need to spend significant amounts of their capital on purchasing hardware and running that hardware in a data center that they build. Expensive applications needed to run the organization can now be purchased as SaaS, or Software-as-a-Service, applications on a monthly basis, or they can be downloaded as open source software. The cost of starting a business is far less than it has ever been.

Another factor in the accelerated development of startups is the DevOps way of software development, deployment, and operations. The convergence of new technologies being available with new ways to leverage these technologies has changed the way business is done. For startups, specifically, the changes have been seismic. A well-built DevOps program oriented around a CI/CD (continuous integration / continuous deployment) pipeline can further bolster agile execution that easily supports pivoting quickly when necessary.

Unfortunately, given the often frenetic pace of life in a startup, it's not uncommon to see corners being cut, especially with security. Yet, there's much that can and should be done - that can help enable better agility, better execution, and better quality. Startups must learn to balance effort with the ability to execute, while prioritizing what tasks will bring the most value to their business. Security is often viewed as a cost of doing business, not as added value. If startups can take the proper and critical steps to secure themselves, the benefits of doing so are significant.

Problem State

As a startup, security likely isn't your core business. In fact, it may not seem like it has much of anything to do with your business. Yet, if you're doing anything with technology (you are!), then you absolutely need to think about security concerns. You're moving quickly, you need to remain agile, so why not look for enablers and accelerators from security that will make things better?

There are a number of common practices and challenges where security can be challenging. First and foremost, it's not uncommon to think that you have to do everything on your own. It's just you and your startup against the world. But, why do everything yourself? Does that even make sense? Consider many HR, CRM, and ERP systems that target smaller businesses today. They're SaaS-based, meant to be accessible and easy to use, and at a favorable price point. Would it surprise you to know that there are security solutions that can also be described in this manner? Outsourcing can be hugely important.

Second, it's important to stop chasing the next shiny object, especially as it pertains to security. Just as sound engineering can be vital to product success in a startup, so too can sound engineering be key to evaluating security options. Look for opportunities to get extra value from security investments. For example, training programs for developers can often focus jointly on software quality and security. Cloud infrastructure investments and DevOps CI/CD builds can provide optimized frameworks into which security tools and practices are readily integrated. There are smart ways to leverage security to get wins in multiple columns. Seek those out. Don't just view security as a cost center and an obstacle to doing business.

Lastly, a word on being lean. Undoubtedly you're familiar with the concepts of lean manufacturing and, more recently, lean startups. In fact, as a startup you may be intently focused on building and selling that MVP (minimum viable product). However, don't forget about other key tenets of the lean movement, such as fostering a cooperative environment that creates generative culture of which security is an inherent, emergent property. Putting value on respectfulness, mindfulness, and cooperation means that everyone has a shared responsibility for the success of your startup, which includes ensuring the security of your systems, networks, applications, data, and people (both personnel and customers). Being lean today means creating a solid foundation upon which your business will thrive, grow, and survive.

Being lean today means creating a solid foundation upon which your business will thrive, grow, and survive.

DevSecOps Recommendations

Entire books, frameworks, standards, models, and regulations have been published on the topic of what security practices your organization should adopt. There's a glut of guidance on how feature X is important or why you should buy product type Z or else suffer dire consequences. In this section we hope to avoid boiling the ocean by providing a tangible, realistic, actionable list of recommendations that you can act on today to better support, secure, and accelerate your startup.

1. Base Infrastructure Decisions

One of your first major decisions in a startup will be where to build and host your offering. The Infrastructure-as-a-Service (IaaS) phenomenon has transformed the startup ecosystem. Companies can be started for far less money than ever before, and that's creating a new wave of innovation. But, with this technology also comes great responsibility. Securing your cloud infrastructure is more important than ever. It's important to realize that using a cloud service does not necessarily change or reduce the need for security practices. In fact, many of those same security practices and requirements persist in the cloud, but present in a different manner. As such, it's important to remember that being in the cloud does not exonerate you from your security responsibilities.

Another key decision that affects infrastructure, as well as core business processes and functions, is your approach to development and deployment. For a lean startup, agile development is generally the go-to solution, and that will often lead to a DevOps approach. Be careful, however, to ensure that you don't just stop at DevOps, and that you take the time to invest in your CI/CD pipeline so that it provides a suitable basis for automation of key tasks, like builds, testing, and deployment. Be mindful to build in flexibility and resilience from the outset so that you can adapt to changing requirements and challenges down the road.

A key takeaway here is to spend a little extra time thinking about infrastructure engineering up front so that you'll be less encumbered in later stages. It's understandable wanting to rapidly build your MVP and get it out the door, but don't harm or hinder yourself in the process. Even if you aren't able to plug-in key security practices like application security testing or vulnerability scanning, design with those practices (and more) in mind. Similarly, plan for automated builds, testing, and deployments so that patch management is a much easier problem to solve.

2. Key Security Considerations

There are a lot of things you should think about relative to security, but a lot of it can be overwhelming, distracting, or outright limiting for a startup. We think the following topics are really important to address up front because they will save you lots of pain and suffering as your venture grows and succeeds.

A. Identity and Access Management (IAM): The First Line of Defense!

Despite all the different areas of concern facing organizations today, there is one such topic that is universally important, difficult, and distressing: managing user accounts and access. We could write an entire book on this topic, but for the sake of brevity we've reduced this to a few simple takeaways, which are:

1. Minimally, setup a central system of record identity. There are several ways of accomplishing this goal. On his to make use of a federated identity provider (identity-as-a-service, or IDaaS). Another method is to work with a central Directory service or a Directory-as-a-Service provider as a means of taking your integrating your existing directory with cloud services.

2. Invest in a flexible multi-factor authentication (MFA) capability. MFA is increasingly critical to fend off many types of common attacks.

3. Don't forget all the supporting practices. All access must be authorized and reviewed on a regular basis. Some form of audit trail must be maintained for granted, as well as reauthorized, access. If you don't use a Dir-aaS that is already integrated into your cloud infrastructure, make sure you IDaaS or whatever you use can also map into cloud infrastructure environments, such as by using federated identities instead of IAM users (using AWS vernacular) and ensuring a good balance is struck between the access roles have and granting people too much access. Routinely review access and, as your company grows, put in place mechanisms to ensure that personnel have their access reviewed when changing roles. Also, once you reach a suitable size (likely as small as a dozen people), don't forget to formalize your termination process, too.

As a side note, there is much conflicting information today about passwords and password management. Much of this information is outdated and no longer applicable. When it comes to passwords, there are three things you should know:

- Length is the most important attribute. Discussions and guidance about “complexity” and “strength” are now outdated and should not be followed. The purpose being met here is to reduce the ease of guessing someone’s password. This can be easily achieved through setting a length requirement of at least 14, if not 16, characters. Along these same lines, encourage users to choose passphrases or wordsets instead of passwords.

- Besides IDaaS, invest in a commercial password vault/manager solutions. Something relatively inexpensive like Lastpass or Keeper Security can provide a viable mechanism for protecting passwords. These tools will also often allow password information to be securely shared (NOTE: password sharing is strongly discouraged, but we realize there are some cases where it must be done, such as securely archiving the AWS root credential in a place accessible to all authorized systems administrators). More expensive password vault solutions for servers, applications, and networks may also be useful as you grow.

- Ensure you have a human fail-safe for the most important systems. For example, ensure a two-key system of sorts for large financial transactions. There continue to be significant attacks on smaller organizations across multiple industries that attempt to trick personnel into making fraudulent wire transfers to criminals. Determine an appropriate threshold and then setup an out-of-band mechanism where such things are independently verified.

B. Security Architecture

The traditional approach to security architecture is too look at protection, detection, and correction balanced against the business’s priorities on confidentiality, integrity, and availability. However, in this modern IT environment where almost everything is in the cloud, we often find that availability trumps everything, followed by confidentiality as needed, and then maybe integrity. Protection solutions are prevalent and easily deployed, but a point of diminishing value can be quickly founAs a side note, there is much conflicting information today about passwords and password management. Much of this information is outdated and no longer applicable. When it comes to passwords, there are three things you should know:

1. Length is the most important attribute. Discussions and guidance about “complexity” and “strength” are now outdated and should not be followed. The purpose being met here is to reduce the ease of guessing someone’s password. This can be easily achieved through setting a length requirement of at least 14, if not 16, characters. Along these same lines, encourage users to choose passphrases or wordsets instead of passwords.

2. Besides IDaaS, invest in a commercial password vault/manager solutions. Something relatively inexpensive like Lastpass or Keeper Security can provide a viable mechanism for protecting passwords. These tools will also often allow password information to be securely shared (NOTE: password sharing is strongly discouraged, but we realize there are some cases where it must be done, such as securely archiving the AWS root credential in a place accessible to all authorized systems administrators). More expensive password vault solutions for servers, applications, and networks may also be useful as you grow.

3. Ensure you have a human fail-safe for the most important systems. For example, ensure a two-key system of sorts for large financial transactions. There continue to be significant attacks on smaller organizations across multiple industries that attempt to trick personnel into making fraudulent wire transfers to criminals. Determine an appropriate threshold and then setup an out-of-band mechanism where such things are independently verified.

4. Detection solutions, such as intrusion detection or log management, tend to be much more difficult to deploy and tune, plus they often represent a sizable investment (even for minimal value). Correction solutions tend to skew toward manual response, especially in the early, lean days of the startup. Overall, this traditional perspective may not be as useful as it once was.

An alternative approach is to think about visibility (what can I see?), control (what control can I assert?), remediation (how do I fix things?), and response (how quickly can I intervene?). Applying these four principles across endpoints (comprised of servers, user devices, and mobile/IoT devices), networks, applications, and data, we can achieve a fairly interesting view into security architecture strategy, planning, and decision-making. Where this approach becomes particularly interesting is when we start finding tools and techniques that give us benefit in multiple areas (see table 1), such as endpoint security solutions that not only give us insight into where our endpoints are and what they're doing, but also allow us to assert control over those devices, and further facilitate remediation and response (such as automated patching and collection of forensics data for investigations).

Table 1: A Matrixed Approach to Security Architecture Planning

	Visibility	Control	Remediation	Response
Endpoint - Server - User - Mobile/IoT				
Network - LAN - WAN - Extranet				
Data - In Motion - At Rest - In Use				
Applications				

C. Patch Management: Then and Now

A key area of emphasis for security architecture is planning for remediation and patch management. In a legacy world, patch-in-place is how things function. This can be frustrating, difficult, and fraught with risk. If you can't get around the traditional patch-in-place approach, then you have to plan for it. Hopefully that planning includes how to get away from patch-in-place everywhere but your user endpoints (where we simply don't have much choice today).

DevOps and the CI/CD pipeline provides us with an excellent opportunity to build for agility while also eliminating the legacy patch-in-place problem. At a minimum, we can automate the build and testing process such that you can update your host image, feed it into the pipeline, and out the other end comes your ready-to-deploy update, fully patched, happily churning away in the cloud. Deploying in an blue/ green manner can further reduce potential pain and suffering by allowing you to introduce new, patched images, test them in production, and then ramp them up while ramping the older images down, all without negatively impacting the customer.

Of course, to make this a reality, you must plan for it in advance. Ensure your product(s) account for session management in a manner that enables automated deployment in this manner. You'll find that the serverless movement makes this planning imperative all that much stronger since you still need to be able to deploy updated containers or applications, and you will undoubtedly continue to have the same concerns around uptime, availability, and reducing the potential for negative impact to customers. Note here how engineering for (relatively) easy patch management ends up improving the overall resilience of your application and environment.

D. Logging and Monitoring

You do not need to go out and buy an expensive security information and event management (SIEM) solution simply to perform adequate logging and monitoring. Capturing logs is, overall, a fairly straightforward process. How you implement may vary a bit, such as deploying a Syslog server or leveraging S3 buckets in AWS, but the principles are still the same. Enable system and application logging for certain areas (e.g., various errors, login failures, traffic spikes) and then push them to a central location. There are many good tools on the market that will serve the needs of dev and ops and security. Don't feel that you have to break the bank on buying a tool, just make sure you're pushing everything centrally and are able to do some basic dashboards and alerts.

E. Incident Management

One practice area that is often overlooked until too late is preparing for incident management. Incidents are going to happen. It's inevitable. Break-fix scenarios abound in general, and that doesn't begin to touch on various security concerns. In addition to having a reasonable logging and monitoring solution in place, you must also be ready to deal with the incidents when they come along. Define your incident response process. Ensure you have contact information for all key personnel. And, perhaps most importantly, invest in some training around formalized incident management so that you can run your response efficiently and effectively. Training programs will often spend time teaching how to setup a chain of command and reporting capability to deal with whatever crisis is facing your organization. Minutes, if not hours, of downtime can materially harm your business, and that doesn't account for a potential reputation hit, which your startup simply may not survive. How you deal with a crisis speaks volumes about how reliable you are as a business.

F. Application Security

Much can be said about application security, from teaching your developers to write better code to integrating application security testing (AST) tools into your CI/CD pipeline. All of these are good ideas and very worthwhile. Best of all, much of this can be done for reasonable costs. In fact, there are an increasing number of free and open source solutions for AST that will save you money. However, this also means you have little reason not to integrate these tools into your environment.

Additionally, as mentioned above, it is wise to make use of pre-hardened images; preferably with security tools already pre-installed. Developers should work off of these images to identify conflicts earlier in the process, and to ensure that builds will go smoothly.

A few lessons from DevOps make application security more important and more tangible to development teams:

You break it, you fix it! In keeping with the culture of DevOps, resolution of security issues should be owned by the developers, not by security personnel. It's one thing to allow a security subject-matter expert (SME) to follow-up and ensure timely remediation, but culturally it's important that developers realize they own the responsibility.

Fail fast, learn faster! Shortening feedback cycles is a critical element of DevOps, and this includes security. AST should occur as early in the process as possible and feedback should be delivered directly to developers so as to more readily own and resolve any issues.

Mistakes are ok, but avoidance is also good! Mistakes are going to happen. DevOps teaches us that we must allow for innovation and testing to occur. However, that doesn't mean we shouldn't first spend a little time thinking things through. A little forethought, especially around protection of data, can save a lot of pain later on.

Securing the Business

Beyond technical practices there are a handful of practices that are universally important and applicable, especially for startups operating under the DevOps model. This section focuses on some of these non-technical practice areas.

Awareness

Many people associate security awareness programs with anti-phishing testing, new hire training, and poster programs. While there isn't anything inherently wrong with using these practices, they often have limited tangible value because they aren't incorporated into standard business culture and practices, and they often lack reasonable measurements and objectives for modifying human behavior. Startups should absolutely invest in awareness programs, but they should be specifically tuned to and focused on changing behaviors, tied to measurements to determine positive impact. Awareness programs may look at improving decisions overall or they may focus on promulgating specific practices or uses of tools (such as in support of a password manager deployment or improving cross-team collaboration and cooperation). Use your awareness program to help grow the culture you want within your organization.

Training

Training programs are distinctly separate from awareness programs. There may be some overlap, but understand that training is about the delivery of specific information through a variety of formats. As noted in the previous section, training programs should have a specific, measurable objective being addressed. That objective may be to improve code quality, reduce security incidents, or teach how to get the most value from new or existing tools. Don't forget to evaluate a variety of training delivery methods, and measure people's attitudes and perceptions about training programs (not just efficacy, but also attitudes about it). Lastly, ensure that you're not punishing people (such as by not accommodating deadlines) for attending the training you've required them to take.

Physical Security

Awareness of an employee's surroundings is critical. While a startup's office may be small or may be a shared space, knowing who should be in the office is important. If a stranger is in the office, ask them if they are in the office to meet someone. Hackers will often try the old technique of masquerading as an employee or a visitor. Most offices are likely have some sort of physical access control either through a key, a fob, or card access system. But after the staff goes home for the night, there are a number of other people that may have access to the facility. The landlord, their workers, the cleaning crew, and countless others could access your office. Having a digital solution in place with regular logging of who enters and exits is a great first step in controlling access. It is also wise to have a few video cameras in your facility. Having cameras in place can be a simple way to ensure that your equipment and materials are safe. There are a number of cloud services that can assist in monitoring the office.

Most offices have a small server or telecom closet that may house a router, firewall, and perhaps even a server or two. Common practice is to ensure that these things are in a locked area and that access is limited to only a few members of the staff. While it isn't always possible to remove every piece of equipment from the premises, control over who has physical (and logical) access to that infrastructure is paramount.

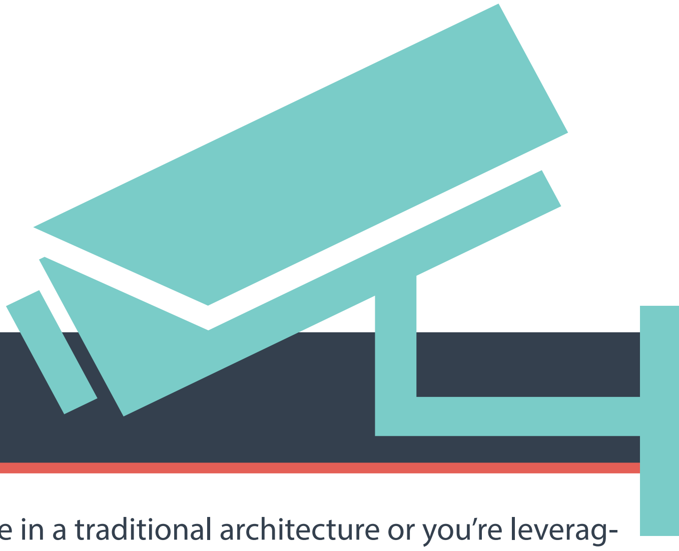
Lastly, investing in a little extra internet security for your office can pay dividends. Consider purchasing a "next generation" firewall that not only blocks inbound connections, but also provides more advanced filtering and intrusion detection capabilities. Ensure that your WiFi has been properly configured with both an authenticated office SSID connection and a separate guest SSID. The authenticated office access should integrate with your central IAM solution so that employees aren't required to save yet another password and access to the network is only by employees. If your startup has a significant number of remote employees, it then may be necessary to look at additional endpoint security solutions that can provide some of these protection mechanisms uniformly rather than simply relying on a network-based appliance.

Measuring for Success

As a lean startup, everything you do should be for a purpose. That purpose should be reasonably well defined and understood, and you should have a means of determining whether or not that purpose has been achieved and is, in fact, adding value as hoped. The same is true for security. For all the discussion here about security practices for startups in a DevOps world, the bottom line is that there is tremendous opportunity to achieve gains in efficiency and effectiveness while also improving security practices. Instilling a core value around measurement within your organizational culture will help set the bar high for further decisions and investments.

Cooperation and Generative Culture

Another key cultural value that will greatly benefit your startup is establishing, fostering, and growing a sense of cooperation that transcends roles and responsibilities. The only way security initiatives will persist and be successful within your company is if you make it everyone's duty to ensure endpoints, networks, applications, data, and people are reasonably secure. Orienting around this shared value of cooperation will lead to what is termed a generative culture; meaning that these values will not only exist today when you're lean and hungry, but they will promulgate with your organization as you grow from 10 to 100 to 1000 people and beyond.



In Closing

Basic security hygiene is incredibly important, regardless of if you're in a traditional architecture or you're leveraging cloud infrastructure. Seek solutions that will give you wins in multiple boxes and that will provide measurable value both today and in the future. Startups can afford to be light on process, policy, and documentation, but don't forget them completely. It's especially important to ensure a reasonable level of formal process and control around access management. Leverage off of tools like federated identity (IDaaS) in order to ease the burden of user and access management.

Note that we did not talk explicitly about risk management or security policies. As a lean startup, pretty much everything you do revolves around carrying a healthy amount of risk while you attempt to innovate and succeed. Policies have a place, and in some cases are required, but overall will have limited utility for startups. In fact, excess documentation, process, and policy can often be a hindrance to innovation, agility, and DevOps initiatives. As such, it is often best to focus on accelerator practices and tools that will help you get multiple wins.

Startups run lean, and their security practices should follow suit. Focus on building a healthy culture that includes security from the outset as a common shared value and responsibility. Provide training and tools that benefit your company overall, optimize effectiveness, and simplify your operating environment. Simplification, such as demonstrated by Dir-aaS and IDaaS solutions, combined with automation will often provide considerable security benefit overall. Strive for making security an emergent property of your successful business.