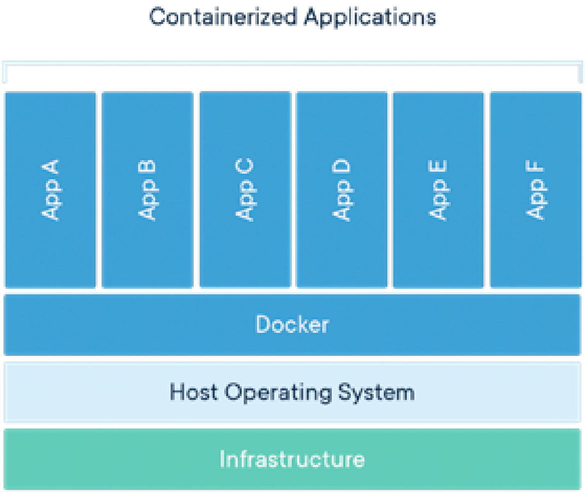
How Docker Containers Help with Identity Management Security

Avatier Corporation
4722 Cabot Drive
Pleasanton, CA 94588
www.avatier.com

TABLE OF CONTENTS

A SHORT INTRODUCTION TO DOCKER CONTAINERS

Before diving into the details of Docker security, it's first important to understand a bit more information about what containers are and how they compare to virtual machines. The following is an excerpt from the leading provider of containers, Docker.



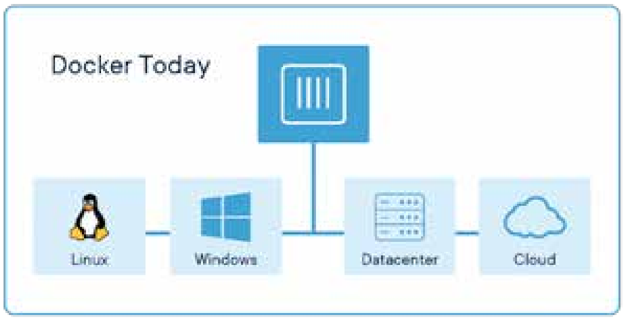
Source: Copyright Docker 2018

A container is a standard unit of software that packages up code and all its dependencies, so the application runs quickly and reliably from one computing environment to another. A Docker container image is a lightweight, standalone, executable package of software that includes everything needed to run an application: code, runtime, system tools, system libraries and settings.

Container images become containers at runtime and in the case of Docker containers - images become containers when they run on Docker Engine. Available for both Linux and Windows-based applications, containerized software will always run the same, regardless of the infrastructure. Containers isolate software from its environment and ensure that it works uniformly despite differences for instance between development and staging.

Docker Containers Are Everywhere

Docker container technology was launched in 2013 as an open source Docker Engine.



Source: Copyright Docker 2018

It leveraged existing computing concepts around containers and specifically in the Linux world, primitives known as cgroups and namespaces. Docker's technology is unique because it focuses on the requirements of developers and systems operators to separate application dependencies from infrastructure.

Success in the Linux world drove a partnership with Microsoft that brought Docker containers and its functionality to Windows Server (sometimes referred to as Docker Windows containers).

Technology available from Docker and its open source project, Moby has been leveraged by all major data center vendors and cloud providers. Many of these providers are leveraging Docker for their container-native IaaS offerings. Additionally, the leading open source serverless frameworks utilize Docker container technology.

CHAPTER 1: WILL CONTAINER ENCRYPTION KEEP YOUR ORGANIZATION SAFE

Your developers have started to use developers so you can scale up. It's a popular strategy because you can save time and effort on configuring operating systems. That's not all. Making containers and other innovative technology available in your organization means you can attract and retain technical talent easier.

Like any new technology, there are challenges to consider. For instance, your operations team may not feel confident about managing containers. That's a valid concern to address, but it won't be the focus today. Instead, the focus is on the security impact of using containers.

The Dangers of Sloppy Innovation: Containers Gone Wild?

Here's the situation: spinning up containers and hoping for the best in cybersecurity isn't going to work. There's really only one situation where that slapdash approach to technology development makes sense: during a hackathon or some experimental critical situation. That approach isn't going to work for the rest. All it takes is one gap in your security program to cause a reputation-damaging event.

When containers aren't integrated into your security program, you're leaving the door open to hackers and other problems. The first step to preventing that problem is simple: get the lay of the land before you make decisions about what cybersecurity changes are necessary.

Assessing the Impact of Containers on Your Cybersecurity Program

Let's assume you have a reasonably mature and highly effective cybersecurity program. If the program has been in place for several years, your staff may be out of practice in adapting to change. To assess your readiness to adopt containers from a security perspective, use these self-assessment questions.

1. What container technology does the organization currently use? (Aim to be comprehensive on this front)
2. Who has privileged user access regarding container setup and management? (If the answer is "every developer," then you have a high-security risk on your hands)
3. What documentation and training are available internally regarding container security? (This point is critical if your organization is rapidly expanding, as new hires need guidance to understand your needs)
4. What third parties outside the organization have access to your containers? (The main danger lies in not knowing who has access and why)
5. How was security considered during container implementation? (The best practice is to use a security-by-design approach, to include security as a fundamental first step)

Resource: Are you planning to start a container implementation? Check out 8 Docker Implementation Mistakes You Need To Avoid for tips to make sure your efforts pay off. If you make mistake 5, hackers and criminals will find it easy to break into your company.

Now that you've completed this mini-assessment, you have a decision to make. Are you satisfied with the security oversight and controls for your container implementation? If the answer is no, then you need to look at encryption and other security improvement options.

What Are Your Options for Container Encryption?

With encryption, there's no one-size-fits-all approach. You might use Docker secrets to apply encryption to sensitive data in Docker. That's a good start! What if you're using other container products? You'll need to investigate their encryption options and see how they compare. If you have multiple container products in use, you'll have different encryption options. Unfortunately, configuring your data encryption settings in your containers will only take you so far.

Now, what about the rest of your data flowing in and out of containers? You may need encryption on that data as well. Encryption is a worthwhile way to protect your data, but it isn't enough on its own.

There's a method to improve container security that you may not have considered yet. By using this strategy, your efforts to use encryption will be even more successful. If you skip this strategy, determined hackers may be able to sidestep your container data encryption easily.

The Missing Piece to Container Security: Identity and Access Management

Picture this: a manager's access credentials are hacked. Armed with these credentials, a dishonest competitor creates a user account and starts downloading data. Since the user has a "valid" ID, he or she can sidestep your other security measures. Yikes! In a matter of minutes, critical data will leak out of your organization. With a security failure like this, you can't assume that a software update from Microsoft, Apple, or another company will suddenly appear.

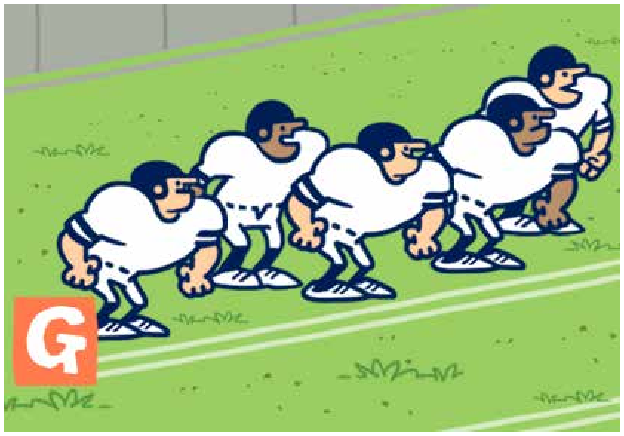
How do you prevent this disaster from happening to your company? You can never achieve 100% security protection, you can only make it harder for hackers and limit the amount of damage they can do. For instance, check whether your staff suffers from password reuse disease. That's another security problem not solved by implementing encryption.

By improving your identity and access management program, you'll help your employees manage their user accounts more successfully. Instead of asking managers to remember to inspect user IDs regularly, you'll use an identity management solution. Further, you need a solution that works across your enterprise, including containers.

Naturally, we recommend Identity Anywhere to protect your containers. Designed to run in the cloud or on-premise, Identity Anywhere is a comprehensive identity management solution. It's designed to work with Docker container technology, one of the most popular options on the market. In cybersecurity, it's important to act fast to respond to new vulnerabilities. With Identity Anywhere, you can take a continuous delivery approach to identity management. No more waiting days to fix a hole in your identity management system, you can make updates much faster.

As you improve container security, remember to capture the business benefits of this technology. For example, you can reduce your recruitment expenses by using containers to win the war for technical talent. Competitors are constantly recruiting good developers and engineers. By giving them containers and other leading technical tools to use, your technical stars will have the chance to grow and succeed by staying with your company.

CHAPTER 2: REDUCING YOUR ATTACK SURFACE



Containers are here to stay because they are much more efficient than virtual machines. Unfortunately, identity and access management have lagged behind containers until recently. Identity-as-a-Container (IdaaC) brings identity management into the container era.

Containers: Better Than Traditional Virtual Machines

Why are so many organizations adopting containerization to manage their systems? It comes down to efficiency, productivity, and security. Traditional virtual machine arrangements using Microsoft or VMWare take up significant resources. With virtual machines, demands on CPU, memory and other hardware resources can quickly skyrocket. Our research suggests that containers have 20x the density of traditional virtual machines. That means you could cut down your data center cost substantially.

Saving money is the most popular reason companies adopt containers. There is more to the story. Think about your technology as a vast wall that you must staff with defenders. Leave one part of the wall unmonitored, even for just a day, and hackers are likely to find a way to break in. With containers, you reduce your attack surface. That means your existing cybersecurity staff will not be overwhelmed with monitoring and responding to threats. Further, your security team will have fewer operating systems to test so they will have the capacity to carry out testing and assurance in greater depth.

Resource: For additional insight on attack surface, read How Do I Identify My Application Attack Surface? on SecurityWeek.com. The critical first step in understanding your attack surface is to create a comprehensive list of all your application. Missing that step is like buying a house without walking through each room with an inspector.

Simplified Application Maintenance with Containers

Question: How many applications does your organization have to monitor, maintain and support today?

Before you answer, think broadly. You might have a long list of legacy applications that run on UNIX. On the other hand, you might depend on cloud applications. Then you have niche applications built for the needs of a specific department. At a large company, there are probably hundreds of applications in regular use. If a minor application fails, it could take down critical applications.

Containers make application maintenance easier to manage. How? The answer lies in using container orchestration. By using a series of scripts, you can quickly set up multiple containers. When you first start experimenting with containers, it makes sense to set up each container one at a time. As you scale up, orchestration makes it easy to set up multiple containers. Even better, you can transfer this task to DevOps instead of IT. Taking away that point of friction adds up to faster delivery.

Tip: To build your application list, start with the most heavily used applications. Once you have that list, ask your managers and developers about the inputs and dependencies those applications rely on. Before long, you will have a good list of important applications.

Why Traditional Approaches to Identity Management Come Up Short

Your organization’s attack surface is continually changing. Decommission an old server, and there is one less area to be attacked. Start ten new containers? That is an additional attack surface. Suffering an attack is only part of the problem. If you are a public company or operate in a regulated industry like banking, internal audit will want to see you control identity and access management. Fail an internal audit on access controls, and your performance review may take a hit. Don’t wait for that happen — find a robust identity management solution before an auditor points out a problem.

Does the traditional on-premise approach to identity management still make sense when you use containers? Don’t get us wrong. Traditional IAM solutions are robust, and they can be customized to do almost anything. The major drawback? Keeping these older applications up to date is difficult. Hiring a dedicated team for access management is often required to make this approach work. If you are running security at the Pentagon, that investment may make sense. For everyone else? Let’s keep looking for a better solution.

If you follow technology, you can probably guess the next option we will consider: cloud identity management or identity-as-a-service. After all, the cloud is always better than traditional on-premise software, right? While that is true in many cases where economies of scale apply, it is not straightforward in identity management. By encouraging rapid expansion, this approach tends to encourage multi-tenant solutions. It is inefficient and creates new security risks. Don’t worry — there is a way to achieve cloud style security without the cloud’s problems.

Leveraging Identity as a Container

The best approach to comprehensive identity management? Use the identity as a container (IDaaC) approach. It is the best way to solve the issue of identity management because you combine elements of on-premise management with the flexibility of cloud approach. Identity Everywhere adds value to your organization in a few ways.

- Leverage Docker Containers. Is your team already familiar with Docker? Great. Identity Everywhere is built on Docker, so there is no need to learn a new container technology.

- Reach your continuous delivery goals. Identity Everywhere reduces downtime so your team can deliver upgrades more quickly.

- Simple Patch Management. Miss one patch to an operating system and your entire infrastructure could suffer. It has happened before — missed patches contributed to the Equifax data breach in 2017. Using Identity Everywhere and containers, you will have fewer operating systems to manage and fewer patches

- Multiple Access Governance Services in One Package. Do you need password management? It's in Identity Everywhere. Likewise, you can add single sign-on and access governance.

- Simple Pricing. Choose the service you want (e.g., access governance, password management) and the number of users, and you have an easy-to-understand price. Say goodbye to complicated pages with black box pricing.

- Educational Institutions. Do you run identity management at a college, university or other educational institution? Avatier is proud to offer special pricing to help educators accomplish more with their limited budgets.

Still on the fence about using containers? Read our article 7 Productivity Benefits of Using Containers for an introduction.

CHAPTER 3: THE HIDDEN DANGERS IN THIRD PARTY CONTAINER SECURITY AND HOW TO SOLVE THEM

You just signed an outsourcing agreement with a top vendor. They're going to take care of all your Docker containers. Fantastic! You can move on to other issues.

Listen up; if that's how you think about managing your company's technology, you're in for a wakeup call. Outsourcing is a good way to access expertise from others at a fair price; however, that doesn't eliminate your responsibility for oversight, risk management, and strategy.

Why Do You Need Outsourcing Management in the First Place?

Outsourcing is a fashionable way to improve performance in business. Whether that outsourcing takes the form of offshoring or a local arrangement, the concept is similar. You're taking a function that would typically be performed in-house and asking a third party to get it done. What can go wrong if you have no process in place to manage outsourcing?

Let's say you have a third-party firm manage your cybersecurity emergency response needs. When your email systems are hacked, you call them at midnight, and they swing into action. Hours tick by, and you're wondering when the situation will be resolved. You need updates for senior management and for your customers. Part of the problem is that you have no defined service level agreement or reporting requirements that explain how the outsourcing relationship will work. As a result, the provider simply uses its standard approach, which is to stay quiet until it's solved the problem completely.

What Mistake Can Happen with Outsourced Containers?

All the risks and rewards of outsourcing in other areas directly translate to managing containers. Without oversight, reporting, and other management, your containers are more likely to be mismanaged. To prevent that from happening, you need to know what can go wrong.

1. You receive poor or no reporting about your container technology

Without up-to-date information, you can't measure what's happening with your container arrangements. This means you're going to get a nasty surprise when you receive your monthly invoice, and that's not the only potential cost you face. What if your CTO or CIO asks about container performance in advance of a major launch? If you struggle to answer those questions, you're not going to look good to your leadership.

Tip: Not all your providers who use containers will disclose that fact. After all, container technology supports productivity rather than an end user application. It's up to you to ask your technology vendors whether they use containers to serve your account, and ask how they manage security risk.

2. Your provider doesn't play ball with your cybersecurity program

Some technology providers take great pride in their security programs. What's the problem with that? Well, too much professional pride translates into poor customer service. Specifically, the company may refuse to adjust its procedures and processes to meet the needs of your company. Solving this lack of flexibility is difficult. Ultimately, you may have no choice except to switch to another provider.

Speaking of "not playing ball," you might be making a specific contractual oversight.

3. You have no audit rights for the provider

When you suffer a cybersecurity hacking incident, you need to understand your entire technology stack. You interview staff. Your experts review system logs. Of course, you also need to talk to technology providers. When you request to send your IT auditors to visit the company, suddenly you find out that confidentiality clauses in your agreement prevent such an inspection from happening. The result? Your security review has holes, and you can't be sure you've identified all your risks.

Insisting on audit right in a contract is sometimes a difficult proposition. If you're operating in a highly regulated industry such as banking, it's worth the effort to push for it.

4. You haven't tested the third-party container technology for risk and resilience

You may have originally pursued container technology as a way to scale up your company faster. What if your company's product is featured on Slashdot, TV, or another high-profile source? You need the capacity to scale up your entire infrastructure rapidly. You may even need to set up additional containers to handle the load.

Instead of guessing whether your technology can handle that load, there's a better way.

With all that can go wrong with outsourced technology, what can you do to mitigate these risks?

Your Options to Better Manage Outsourced Container Risk
If you're tempted to close this article and cancel your container technology contracts, stop right there. There are ways to manage this technology risk and realize significant benefits.

Use the monitoring and reporting provisions
Have you read your agreements with third-party container management providers? If not, set aside half an hour today to complete that review. In particular, look for any provisions regarding reports and key performance indicators. Make sure you're receiving a copy of these reports and that they're clearly defined.

Educate staff on container security risks
As container use expands, take the opportunity to improve your coverage of containers. This new "container security" module is best targeted to developers and DevOps; it doesn't need to be completed by all employees. For all employees, make sure you provide password management training.

Appoint a manager for container technology risk
Appointing a single person – typically an IT security manager – with responsibility for container tech risk is a smart move. If responsibility is spread too thin, you'll struggle to ensure full coverage.

Improve identity and access management governance
If the wrong people obtain access to your containers through stolen or misappropriated credentials, your data and applications are at high risk. Fortunately, there's an affordable and systematic way to improve this part of your IT governance program.

The New Way to Solve Container Technology Security Risk
By improving access controls, you keep your containers safe from the start. Even better, you'll also keep your IT auditors happy because they'll see clear evidence that access is being managed in your containers. How do you realize this improvement? Simple: implement Identity Anywhere, a flexible identity management solution that's built with container management in mind.

CHAPTER 4: USING DOCKER CONTAINERS TO REDUCE YOUR CYBERSECURITY RISK

Avatier has the first security and identity management product built on Docker Containers. We're committed to helping Docker Container users manage and reduce their cybersecurity risk.

What does this mean for you as an IT manager, developer or security professional?

We have a few answers to that question, depending on your role: IT manager, developers, or cybersecurity specialists. Let's explore the implications for technology managers first.

What Does This Mean for IT Managers?

When one of your IT key performance indicators slips out of the green zone, you know you're going to have a bad day. You may have to meet with the CTO or CIO or have an uncomfortable conversation with a customer. That's just the surface level problem, as something worse also happens. You have less time to spend on strategy, developing new project ideas, and innovation.

How do you avoid the fate of a reactive IT manager who constantly has to explain away poor performance? You need to use robust systems that work together with minimal problems. For example, if all your developers and operations staff are using Docker Containers, your IT management systems need to be aligned with that choice. To help you simplify your identity management processes, use Avatier Identity Anywhere. It's built to work with Docker Containers, with no need for your team to tinker with customization.

Making Life Easier for Developers

As a developer, your time is valuable. According to US News, software developers earned a median salary of $100,000 in 2016. That means every hour you spend on workarounds or using outdated systems costs your company money. When your company commits to using Docker Containers, this change needs to resonate with the rest of the organization.

What does this look like at the ground level? You no longer have to send an email to a manager or operations team every time you need an access change. You also don't have to worry about documenting your access management requests. Instead, use Identity Anywhere to contain all those access requests.

Resource: What if you don't have Docker Containers implemented in your company? Face the fact that you're falling behind the competition. Fortunately, we have you covered. Check out our article: Before You Implement Containers, Read These 5 Questions.

HELPING CYBERSECURITY PROFESSIONALS GET OUT OF THE WEEDS

In cybersecurity, you're surrounded by threats. Software weaknesses, IT complexity, and low-cost hacking tools mean it's easy to launch attacks. At the same time, cybersecurity pros only have so much time in their day. Sure, you might have to burn the midnight oil when you're responding to an attack. However, if you let that work-around-the-clock mindset continue, your security is going to suffer. You need to leverage tools to take care of the small problems so you can focus on significant issues. For example, you could improve your company's cybersecurity training program for new employees.

How does Identity Anywhere make a difference? It's simple. Instead of manually reviewing identity management requests, you can adopt a self-serve model. All requests are handled, logged, and verified according to your security policy (and logs are kept for your auditors to review).

What Else Does Identity Anywhere Bring to the Table?

If this is the first time you've heard of Identity Anywhere, you might have a few questions. Full compatibility with Docker Containers is helpful. Here are six ways that Identity Anywhere makes your life easier.

Save money on cloud services: Creating a business case for security software is tough. What if there was a way to demonstrate cost savings? It's more than possible with Avatier! How? You can track cloud app usage through our product and see what your real usage is. For example, you may find out that only 20% of your users are using your customer relationship management cloud app. In that case, you could reduce your cloud license usage right away.

Cut down your password complexity: "Not another password policy! I can barely remember my passwords as it is!" That's what your employees think whenever you impose complicated password rules on them. You can take away password complexity without sacrificing security. How? Use a single sign-on solution.

Reduce hacks with Multi-Factor Authentication (MFA): A single password is no longer enough to protect your company's precious data. You need the ability to verify users by phone and other means. We have built-in support for MFA, so your users can verify their access easily.

Fulfill demanding compliance requirements: Do you need to meet demanding requirements in healthcare, government, or banking? Some products are just not up for the challenge. Avatier's client list – the Government of Alaska, Central National Bank, and more – shows that you're in good hands when it comes to meeting exacting compliance standards. Learn more about how we can help you with SOX compliance.

Flexible hosting: Unlike other Software As A Service products, Identity Anywhere is available in hosted and non-hosted. The non-hosted option is a good choice for organizations that require in-house control and oversight over software. This flexibility is a good option for organizations that are anxious about software in the cloud.

Simple pricing: If you've ever bought an enterprise software product, you know that price tends to be complicated. There are discount codes, credits, and so forth. Identity Anywhere is simple. You pay per user so you can easily forecast your expenses. You can scale up and down as your headcount changes over time.

What's Next for Your Container Technology Program?

Using Identity Anywhere is an excellent way to improve identity management in a container environment. What are the other benefits to using containers? Productivity improvement through time savings is a critical benefit. Instead of constantly tinkering with settings, you can use one container. That means you'll have more time to work on innovative technology products. Second, you'll be able to attract and retain better technical talent because you have newer technology such as containers in place.

AVATIER™ | Identity **Anywhere**™

Avatier Corporation
4722 Cabot Drive
Pleasanton, CA 94588
www.avatier.com

For more information on **Avatier Solutions** and how we can reduce your cybersecurity risk, visit us at **www.avatier.com** or call us at (800) 609-8610.

Published 2/5/2019 v1.1