TWISTLOCK AND STACKERY: SEVERLESS VELOCITY WITH UNPARALLELED SECURITY
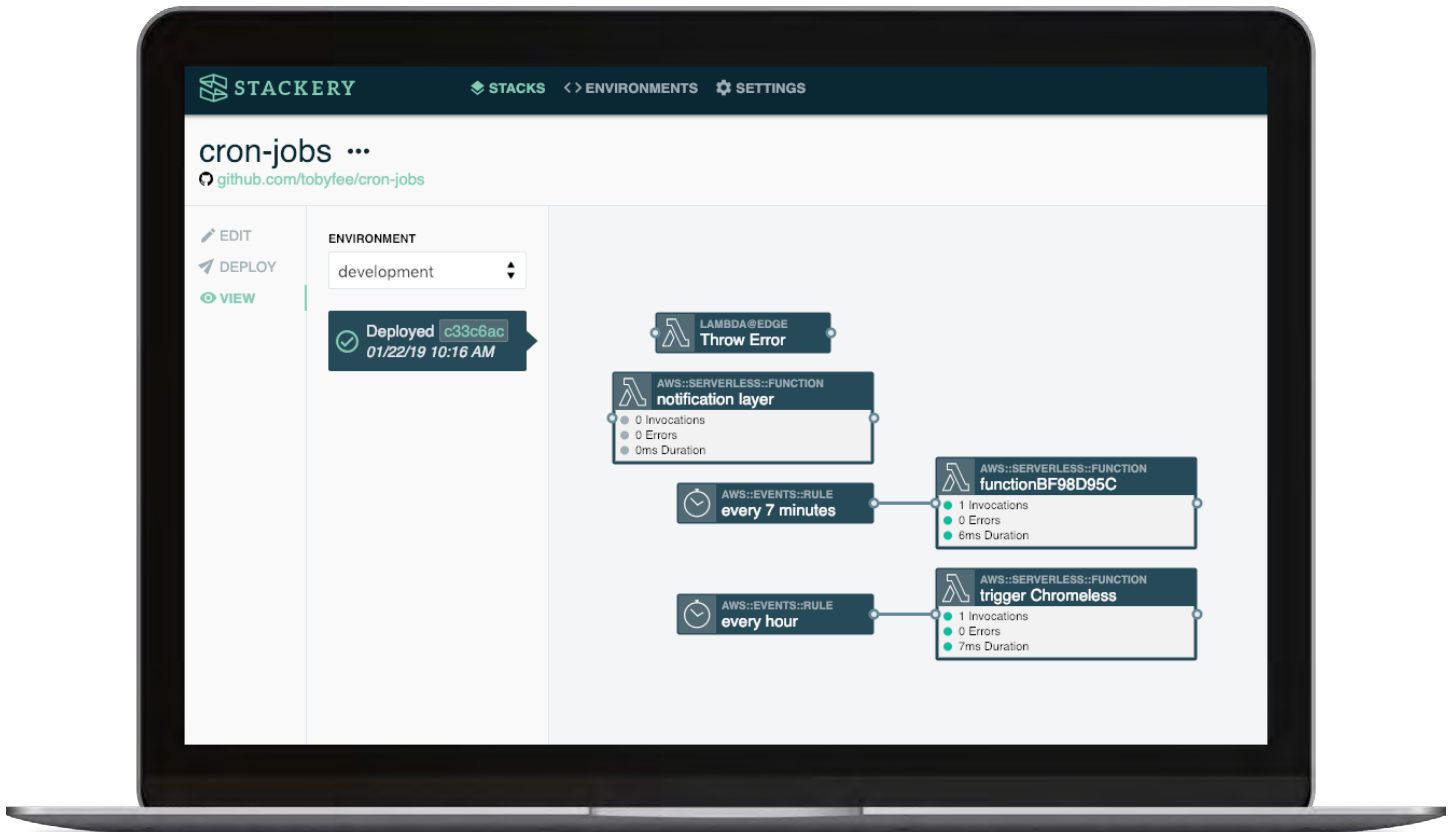
A dual-approach to rapid and reliable serverless development.

Twistlock | **STACKERY**

SERVERLESS ARCHITECTURE IS RAPIDLY BECOMING THE BEST WAY TO ROLL OUT POWERFUL NEW APPLICATIONS.

What components are communicating in your stack? Stackery makes it easy to observe your components and how they rely on each other.

Notably, serverless can be scaled up for massive demand or scaled down to minimize costs, matching your team's needs at every stage. Serverless represents a highly managed solution when compared to its predecessors: bare metal servers and later, virtual machines. As such, some security concerns are less prevalent: AWS Lambdas have no requirement to configure open ports or update their operating system base layer regularly. However, many security holes remain and serverless functions written in Node still can import malicious code, as demonstrated by the 'event-stream' repository this past November.

ENTER STACKERY:

A tool which lets you easily create code-based configuration to deploy stacks across multiple AWS accounts and regions. Stackery can improve your security and policy compliance while enabling teams to increase their serverless velocity. But how can your team use Stackery while easily detecting security policy violations and enforcing rulesets across all containers, serverless functions, and virtual machines? Twistlock has you covered.

Used in tandem, Stackery and Twistlock allow high-performance teams to produce web services that improve over traditional architectures in integral ways. Between increased velocity, observability, policy enforcement, and secrets management, Stackery and Twistlock are a non-negotiable duo if you're adopting or maintaining serverless in 2019.

SERVERLESS CAN INCREASE YOUR TEAM'S DEV VELOCITY

When you ask for a feature from a front-end developer, you'll generally get an estimate for your desired changes in days or hours– when changes rely on your backend, it might be weeks. If you're asking for complex changes to your data layer, some features are just unfeasible. Serverless promises web services built at the speed of frontend light and highly managed services spun up in a single day.

Rather than requiring a separate 'security step' Twistlock integrates with the tools your team already uses, like Travis, to get your systems up and running. From CI/CD to deployment automation, Twistlock delivers protection at every stage of the application lifecycle.

Stackery allows you to create serverless stacks in minutes with the Stackery Canvas and deploy them in two clicks via AWS CloudFormation. The bottom line? A critical process that could take hours in the AWS UI is made easy and repeatable when Stackery and Twistlock are used together.

OBSERVABILITY IS KEY TO SECURITY

At a glance, Stackery provides a map of your application's components, their dependencies, and permissions:
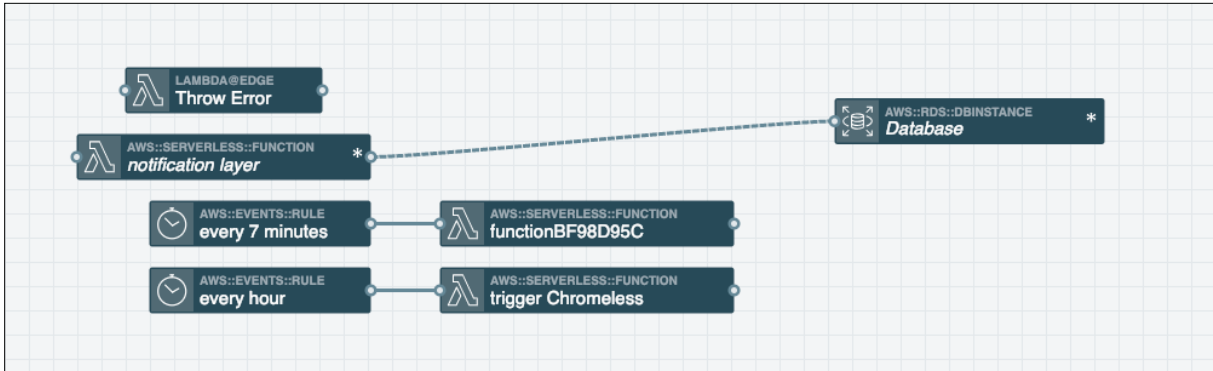
What components are communicating in your stack? Stackery makes it easy to observe your components and how they rely on each other

Many teams get burnt when trying to roll out their own alerts and notification systems. When alerts are supposed to warn you of serious failures, every post-mortem for an in-house seems to include an explanation of why this crisis didn't trigger alerts. Additionally, it can be impossible to act on all alerts when there are a multitude of them.

With Twistlock, it's easy to see a dashboard of policy violations that threaten your security. Notifications and warnings are customizable, so the process is streamlined– you only see the issues that you're concerned about. Additionally, Twistlock integrates with your existing tools so it's easy to achieve 100% coverage with the other monitoring capabilities.
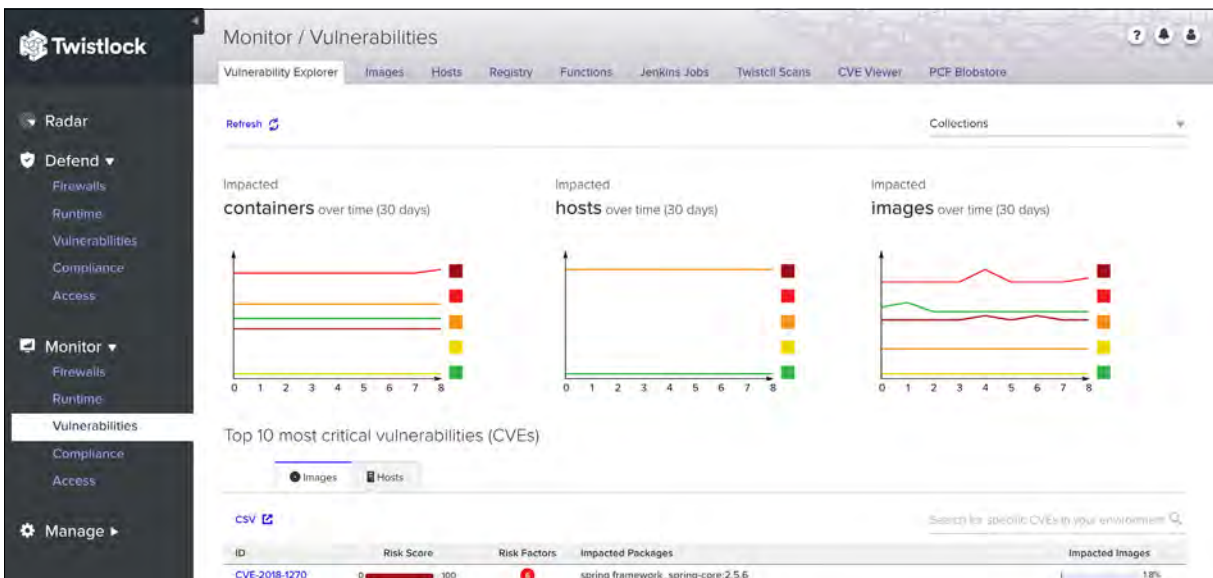
Twistlock's policies can warn you when violations occur or block bad requests.

POLICY ENFORCEMENT

If you want to deploy a stack to AWS, several tools exist but only Stackery has the dynamic configuration to let you manage stacks between different AWS accounts. It also allows you to propose new stacks or updates in CloudFormation without needing IAM permissions. This lets you involve many developers in the deployment process within that account while eliminating the need to open unnecessary vulnerabilities.
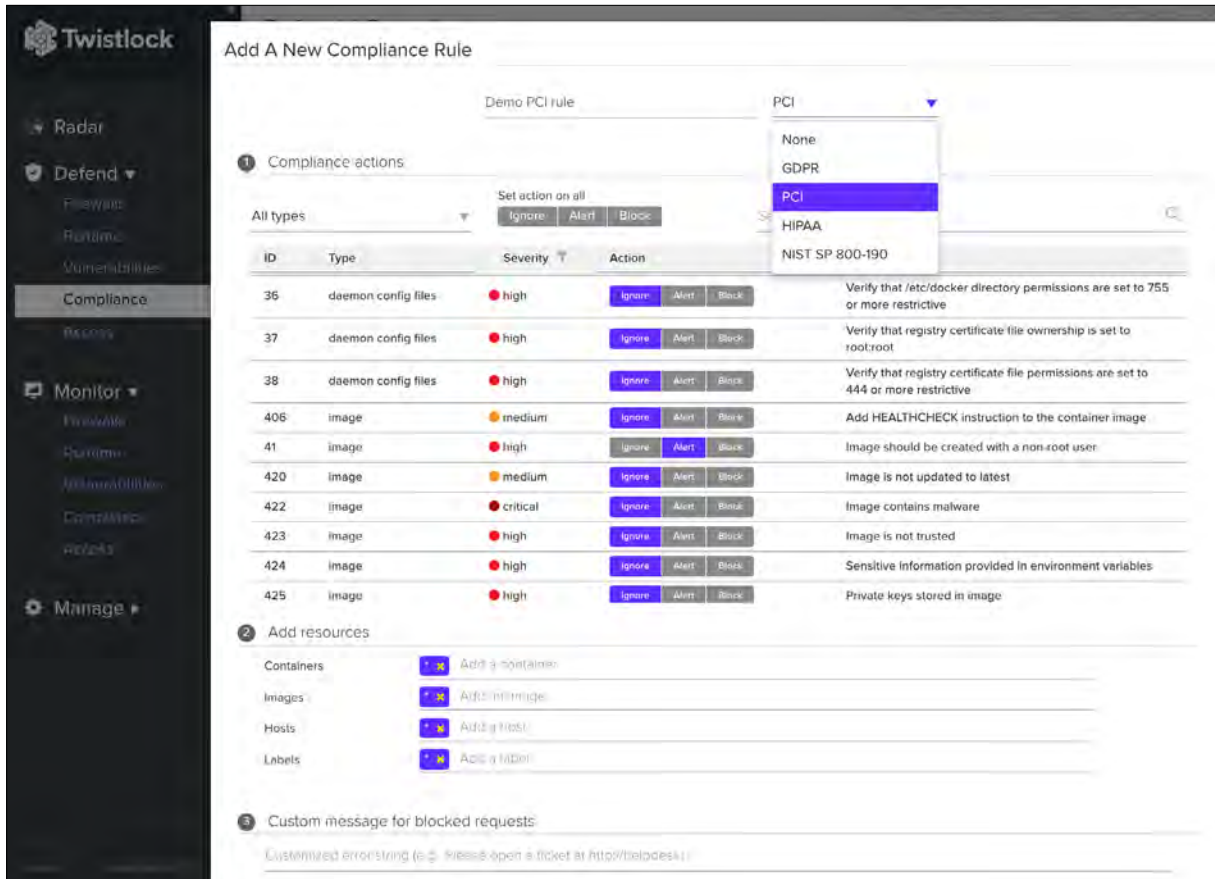
Select the images, containers, and hosts to add new Twistlock rules

Twistlock can do much more than point out policy violations and enforcement is where the tool really shines. Twistlock can seamlessly block behavior in your functions or containers which violate one or multiple policies. Don't want to allow connections to random ports? Want to prevent your DB service from responding to certain services? Opt for highly configurable enforcement with Twistlock, or even the API option if you need to make wide-ranging changes.

SECRETS PROTECTION

Twistlock goes well beyond simple process monitoring or port scanning to make sure your secrets are protected. When installed in your application, it monitors for any keys loaded into memory inappropriately.

Stackery offers clean, simple tools for environment-management and secrets storage to ensure that developers don't commit them as part of their visible codebase. In the Stackery CLI, you can create, delete, list, and set secrets. Environment secrets are stored in AWS Secrets Manager within your AWS account and can be accessed by your application using the AWS SDK.

Used together, Stackery and Twistlock are a one-two punch: a solid foundation of secret-setting and top-notch monitoring. In tandem, these tools provide your team with the best secrets protection on the market.

A UNIQUE SET OF TOOLS

Twistlock and Stackery offer a set of key features not available elsewhere. Stackery lets you visually configure complex stack templates and deploy them straight to AWS with no cumbersome configuration, and Stackery frees your engineers from either writing YAML manually or clicking through hundreds of AWS menus to configure their stack.

While other security companies are slowly starting to offer tooling for container security, only Twistlock offers a single option that can secure your bare metal servers, traditional VM's, containers and serverless functions. This means adopting serverless, the latest and fastest way to create web services, doesn't introduce new security holes into your product, the policies can stay consistent with your services written for older tools.

SERVERLESS WITH STACKERY LETS YOU MOVE FAST, TWISTLOCK HELPS YOU DO SO SAFELY

Stackery is an outstanding tool for increasing the velocity of a team using serverless. Yet, like any new and impactful development, an increase in velocity means heightened risk. Twistlock is the best tool to manage this risk while carrying out the speed and ease of using serverless with Stackery. Together, you have a dependable and complete solution to build safely with serverless–no matter your goal.