Security Orchestration: Herding Digital Cats

Lori MacVittie, 2013-04-03

NetCitadel's OneControl orchestration platform supports #devops for #infosec.

Generally speaking when the topic of devops comes up security isn't something we mention. If we do it's in hushed tones, eyes darting back and forth, the fear that someone might hear us overriding the certain truth that security can benefit as much from devops as any other operational paradigm but just as certain that even mentioning it in polite IT company might get us labeled as a mite crazy

Because when it comes to orchestrating security, we're really talking about herding cats. And not the fat, lazy Garfield cats of the world, I'm talking about the almost feral, fiercely independent, runs-your-house-like-their-kingdom kind of cats.

Automating something that's more art than science, for which exist so many different and highly independent systems and devices with as many different interfaces (and rarely an API) as there are types of beans (seriously, do you know how many different kinds of beans there really are??), is certainly on par with trying to herd *that* kind of cat.

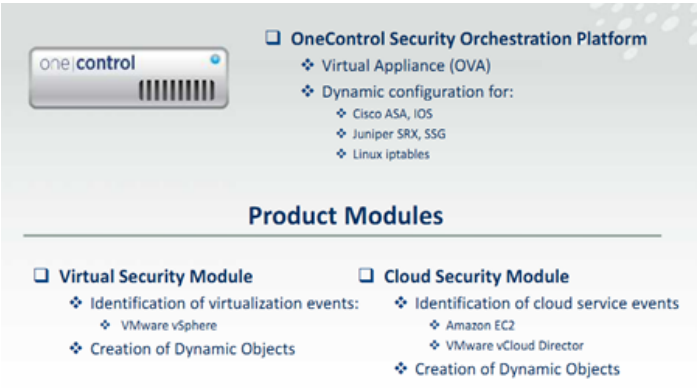
In other words, it's not something rational folk decide to do unless they're into Sisyphean tasks.

One startup is trying to change that perception. NetCitadel recently introduced its security orchestration platform, OneControl, that aims to herd the security solution cats in your data center - without all the scratching and biting that would normally occur.

Security as a Service - Sort Of

NetCitadel correctly (in my opinion) identifies a significant challenge in trying to manually manage a variety of security devices (firewalls, virtual firewalls, routers, switches) in the face of a growing number of variables including more users, more devices, more external applications, more systems.

People, it seems, are in the middle of this morass and as each side of them continues to grow and change, security operations is being outflanked.



NetCitadel's answer to this growing challenge is OneControl, a security orchestration platform that can provide dynamic security configuration (and synchronization of policy) across a variety of systems including Cisco, Juniper, Linux, Amazon EC2 and VMware vCloud Director.

In a nutshell, OneControl leverages a proprietary Security Policy Language (SPL) that allows IT to specify policy by business objects instead of IP addresses. This is increasingly necessary when considering the impact of trying to secure external resources that require access to internal resources. For example, in order to alleviate the burden imposed on IT to manage access from frequently changing IP addresses in Amazon EC2 environments, some folks simply open up their firewall to a very broad range of EC2 network addresses.

That's bad form, almost as bad as simply opening up all the ports about 1024 in the firewall.

But it's been necessary to avoid dedicating a FTE security guy to doing nothing but monitoring and changing firewall rules. NetCitadel OneControl addresses this problem by enabling updates based on requirements specified in SPL and deployed on OneControl. For example, OneControl can track changes in the EC2 environment - such as changing IP addresses - and dynamically update security devices based on policy, without requiring the entire range of network addresses be allowed to pass through the corporate edge. Not only is exposure reduced, but efficiency is increased as the burden of managing firewall updates moves from people to process and technology.

Similarly, OneControl can automate changes across staging environments, ensuring that the sometimes 100s of impacted IP addresses that must be added to or removed from specific security devices are consistently modified.

Once specified in SPL OneControl translates the policies to device-specific configurations for deployment. Approval for changes can be required. OneControl includes all the requisite devops-oriented features such as a RESTful API, versioning, RBAC, and rollback capabilities.

It's a startup and new, so it currently only supports a limited (but obviously the most usually mentioned suspects) set of security solutions but its plans are to continue expanding that support across more vendors and environments.

It's a good start with a focus on a market that sorely needs some orchestration and devops love.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com