SECURING DEVOPS IN MICROSOFT AZURE

EXECUTIVE SUMMARY

DevOps tools share highly sensitive intellectual property and confidential information. But because security isn't built into DevOps, there are inherent risks that must be addressed to protect the business. The good news is advanced security solutions such FortiGate Next Generation Firewalls (NGFWs) and FortiSandbox that share threat intelligence across an integrated security architecture can help secure DevOps applications within hybrid cloud environments like Microsoft Azure. Integrating all of the different elements of security and automating workflows and threat-intelligence sharing, Fortinet Security Fabric is a critical enabler of this process.

86% of business leaders reported DevOps as part of their future IT strategy.[1]

81% of CISOs are concerned with risks related to DevOps that allow vulnerabilities to slip in along with faster pace of development.[3]

Because of its relative immaturity, DevOps security can be an afterthought. Many DevOps engineers—who often have no formal security experience—are asked to protect these environments on top of their many other responsibilities. Further, less than half (46%) of organizations report that their security teams are integrated throughout the entire DevOps process. And three-quarters of organizations lack security for privileged DevOps accounts; if just one password or piece of data is stolen, it could have catastrophic consequences.[2]

SLOWING TIME TO MARKET, HIGHER TCO

Even with traditional security (such as a firewall) in place, problems remain. Protocols and operations in DevOps environments constantly change—breaking the connection with security, which must then be manually reconnected. These slow manual processes create additional security gaps. When a dynamic object changes, the dynamic policy change should be reflected in the security policy without delay to minimize risk exposure.

But perhaps more importantly in the demanding world of DevOps, this increased latency also reduces agility, hampers time-to-market for new applications, raises total cost of ownership (TCO), and makes it difficult to achieve scale.

DEVOPS VULNERABILITY DISCOVERED IN DOCKER

The lack of dynamic security capabilities that can keep pace with the ever-changing nature of DevOps environments leaves organizations exposed to risks from advanced malware and other sophisticated forms of attack. And cyber criminals are already taking advantage of the opportunity.

FortiGuard Labs recently discovered a perfect example of this type of DevOps vulnerability in Docker—a cloud-based collaborative tool used by application developers to work on new software applications, including in cloud environments such as Microsoft Azure, across multiple authors and physical locations.[4] Researchers at FortiGuard Labs found crypto-mining malware embedded in images that were uploaded into the tool. The results of this particular vulnerability earned criminals $90,000 in cryptojacking profits in just 30 days.[5]

In the aforementioned case, attackers exploited the lack of effective security in Docker by embedding shell scripts in some of the Docker images used by developers to build applications. The Docker workflow consists of an application developer working with a Docker client that creates a container by pulling a specified Docker image from a public registry to build their application. When a corrupted image was pulled, the script would download a Monera miner binary from a remote server. Once the malware was executed, crypto-currency mining was completely automated, happening in the background without the developer's knowledge. The result was that all the developers using the registry could be unknowingly compromised, with their organizations paying for the stolen compute cycles used in the public cloud.

A COHESIVE SECURITY INFRASTRUCTURE TO PROTECT DEVOPS

While many organizations have robust security to manage sophisticated threats on-premises, they can struggle to extend those same protections into the public cloud, where exposures like the Docker threat reside. Traditional security controls like native cloud firewalls are insufficient for blocking DevOps threats on their own because they lack continuous policy updates.

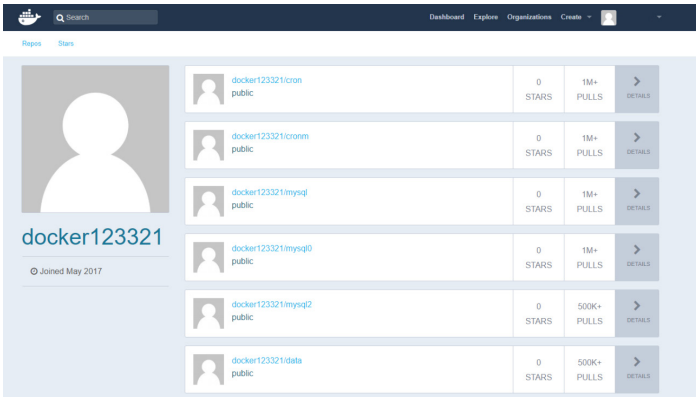

FIGURE 1: HOME PAGE ON DOCKER HUB. EACH OF THE THOUSANDS OF IMAGE PULLS EXECUTES A SCRIPT FOR CRYPTO-MINING.

To address this problem, organizations must establish a secure environment by implementing a cloud-native advanced threat protection (ATP) solution that can scale and automate defenses across hybrid environments—both on-premises and across multiple cloud deployments. The Fortinet Security Fabric architecture includes several key features for protecting dynamic DevOps environments:

1. Sandboxing. An effective security infrastructure must extend further than a successful single incident response. It must also incorporate cohesive management of threat responses across both cloud and on-premises environments as part of a holistic risk-mitigation strategy. An integrated sandboxing solution that comes in multiple form factors (on-premises, VM, and/or cloud) can take protection even further by detecting and preventing advanced threats and zero-day attacks.

FortiSandbox natively deploys in Azure cloud environments to sift traffic, discover unknown objects, isolate them, and safely analyze their behavior. If a threat is found within web application, the cloud-based FortiSandbox then generates the appropriate indicators of compromise (IoC) and shares that intelligence with other FortiSandbox deployments and other Security Fabric elements to provide real-time protection across the entire hybrid cloud infrastructure.

2. Next Generation Firewall (NGFW). Cloud-native NGFWs provide built-in functionality to target sophisticated DevOps threats. They apply real-time threat intelligence to detect and block exploits as well as new malware variants across the distributed enterprise network. To close the crypto-jacking security gap in Docker, Fortinet's FortiGate-VM NGFW for Azure references threat IoC from FortiSandbox to block the command-and-control (C2) server hosting the crypto-mining malware using IP and domain address or file hash.[6]

3. Integration and Automation. Security integration enables automation. Sharing threat intelligence in real-time across all solutions in the Security Fabric architecture—NGFW, sandbox, and more—can trigger even wider policy-based responses to contain threats and mitigate damage in an instant. Automation also reduces the manual threat response burden on IT staff.

Fortinet products for Azure includes:

- **FortiGate** next generation firewall (NGFW)
- **FortiSandbox** advanced threat protection (ATP)
- **FortiWeb** web application firewall (WAF)
- **FortiMail** secure cloud email gateway (SEG)
- **FortiAnalyzer** centralized log analytics
- **FortiManager** centralized security management

MAKING DEVSECOPS A REALITY

Cloud-enabled innovations like DevOps offer vast potential for greater business productivity, but only if these environments are kept secure. At the same time, though, the applied security policies cannot create any operational hinderances; otherwise, developers will look elsewhere and create a vicious cycle of relying on an unsecured development environment. To achieve truly secure DevOps (also known as DevSecOps), organizations need native public cloud ATP solutions—like those offered within the Fortinet Security Fabric—to protect tools like Docker from malware and other sophisticated forms of exploitation in hybrid cloud environments.

[1] "New Study Shows Cloud Adoption Boom is Fueling the Transformation of IT," SUSE, October 17, 2017.

[2] Brandon Vigliarolo, "Report: DevOps has gone mainstream, but DevOps security hasn't followed suit," Tech Republic, November 8, 2017.

[3] "2018 Security Implications of Digital Transformation Report," Fortinet, September 2018.

[4] David Maciejak, "Yet Another Crypto Mining Botnet?" Fortinet, May 03, 2018

[5] Tom Spring, "Malicious Docker Containers Earn Cryptomining Criminals $90K," Threat Post, June 13, 2018.

[6] "David Maciejak, "Yet Another Crypto Mining Botnet?" Fortinet, May 03, 2018