CYBERARK®

REPORT

CYBERARK GLOBAL ADVANCED THREAT LANDSCAPE SURVEY 2018: FOCUS ON DEVOPS

Unaware and Unprepared: A Lack of Security Awareness and Planning Increases Risk of DevOps Secrets Exposure

Table of Contents

About the CyberArk Advanced Threat Landscape 2018 report....3
DevOps: Powering business....3
Roadblocks to the security of secrets....3
Security strategies lag vulnerabilities....4
A surprising lack of awareness....5
It takes an integrated team....6
The fusion of DevOps and security....7
Key takeaways....7
About CyberArk....7

About the CyberArk Advanced Threat Landscape 2018 report

The CyberArk Advanced Threat Landscape 2018 annual report is the 11th of its kind and will be released in three parts. This is part one, focusing on how privileged account security is incorporated into DevOps processes. The survey was conducted by Vanson Bourne in September and October 2017 among more than 1,000 IT security decision makers, DevOps and app developer professionals and line of business owners, across seven countries worldwide.

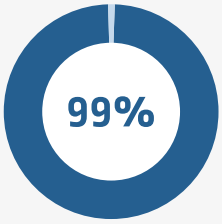
DevOps: Powering business

As DevOps moves into the mainstream, forward-thinking organizations are leveraging this software development practice to improve agility and achieve significant IT and business advantages. They recognize that DevOps can accelerate application delivery, automate routine manual IT tasks and reduce operational costs by boosting efficiencies and productivity.

What are Secrets?

Due to the dynamic nature of DevOps, 'secrets' – privileged account credentials, SSH Keys, API keys and more – are proliferating throughout the IT infrastructure at a rapid-fire pace, creating massive security risks for organizations

Secrets are Hiding in Plain Sight



Nearly all security pro and DevOps respondents failed to identify all places where privileged accounts or secrets exist

Sample size: 825

Unfortunately, meaningful business advantages rarely come without risks. As organizations adopt cloud-based environments and DevOps pipelines, more and more privileged account credentials and secrets are shared across interconnected business ecosystems. Automation tools enable machine to machine interactions without human intervention, and consequently rely on machine identities rather than human identities.

While this further helps accelerate the pace and agility of compute environments, it also increases and dynamically creates credentials, secrets and access points— expanding the attack surface with increased numbers of privileges and credentials and also enabling vulnerabilities to potentially be more rapidly exploited.

Nearly every component of the highly interconnected DevOps ecosystem utilizes secrets. But when asked to identify where secrets exist within the organization's environment, 38% of respondents did not cite cloud environments, containers, CI/CD tools, microservices and source code repositories, according to findings from the report.

Roadblocks to the security of secrets

Bolstering DevOps security is a challenge because security systems for managing privileged accounts and secrets are not integrated with DevOps processes. What's more, the need for cohesive security is increasing apace with the explosive growth of entities that must be managed. Additional challenges include:

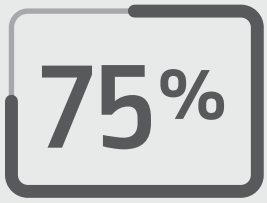
- More critical and regulated workloads are moving to the cloud, creating an additional layer of risk.
- Deployment of virtualized services, containers and microservices has become so fast that humans cannot monitor and manage them without code-based tools.
- As automated solutions execute tasks traditionally performed by employees, new security gaps are opened at system interconnections.

Together, these issues represent a formidable challenge to the security of secrets. Put simply, traditional security programs and practices have not kept pace with the proliferation of vulnerabilities powered by automated IT tasks, opening new attack vectors.

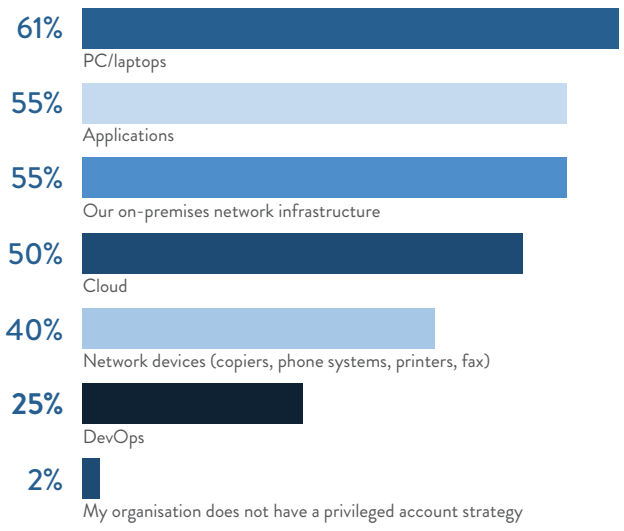
Security strategies lag vulnerabilities

As a comparatively nascent discipline, DevOps security has not reached the maturity levels of traditional enterprise IT, with a very high number (75%) of security respondents reporting their organization has not implemented a privileged account security solution for DevOps. This is potentially problematic, especially in light of 60% of DevOps respondents saying that they store privileged account or administrative passwords in a document on a company PC or laptop. These represent unmanaged, unsecured high value accounts.

For which of the below environments and devices does your organization have a privileged account security strategy in place?



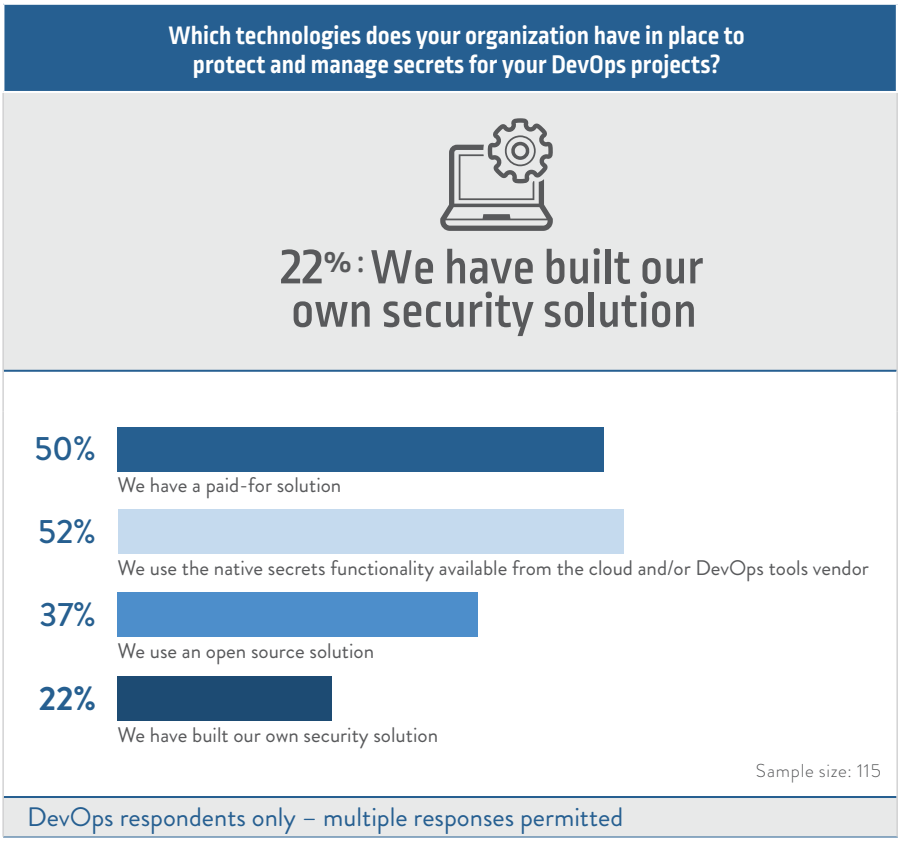
75% of security respondents reported that their organization has not implemented a privileged account security solution for DevOps



Sample size: 710

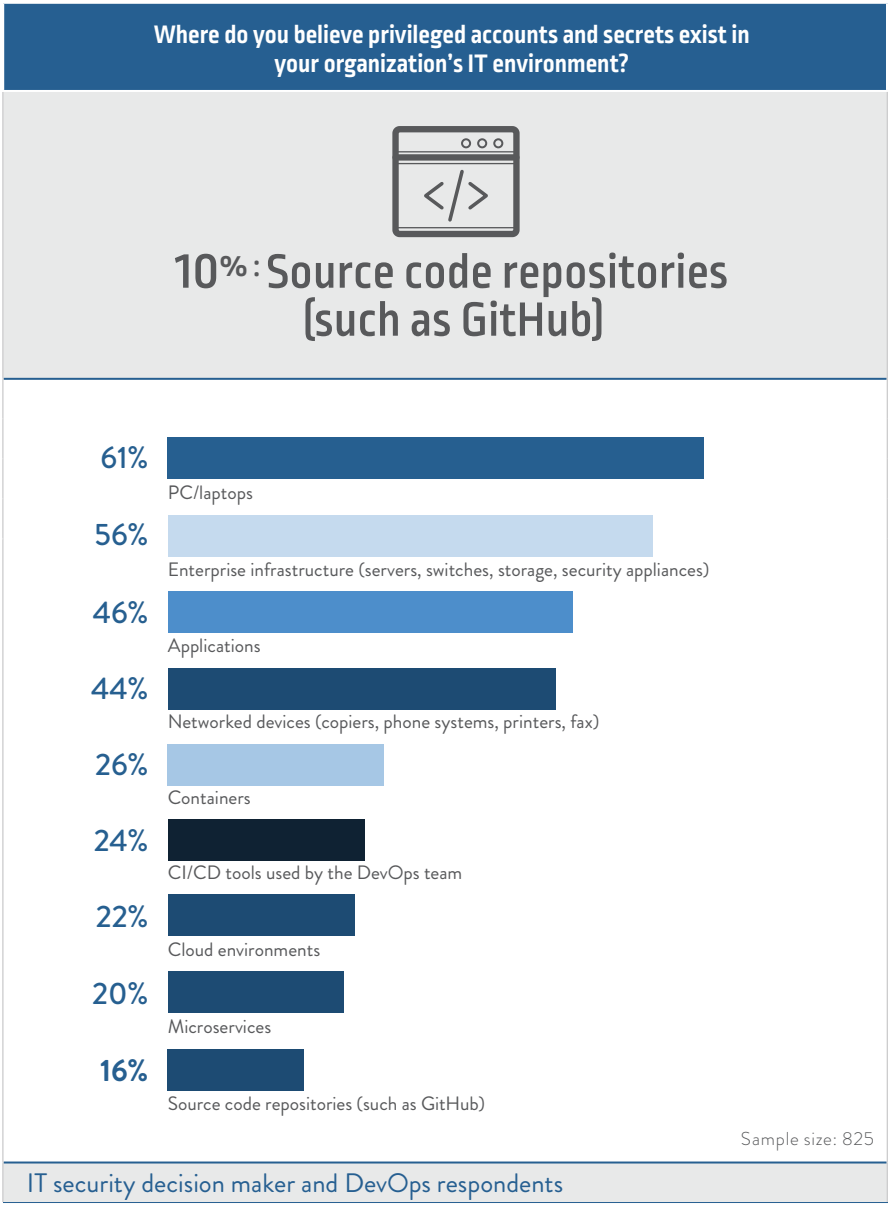
IT security decision makers only

Strategies to protect and manage secrets for DevOps projects in organizations vary widely. The majority of DevOps respondents (52%, with multiple responses permitted) say they rely on the native secrets functionality of their cloud or DevOps vendors. This is potentially a risky approach because it creates separate security silos that are difficult to manage with an overall security policy. Half (50%) say they employ a paid-for solution, which is most likely security-centric and therefore more capable of addressing needs. More than one-third (37%) use systems built from open-source software.



A surprising lack of awareness

It's not just that businesses underestimate threats. As noted above, they also do not seem to fully understand where privileged accounts and secrets exist. When asked which IT environments and devices contain privileged accounts and secrets, responses (IT decision maker and DevOps/app developer respondents) were at odds with the claim that most businesses have implemented a privileged account security solution. A massive 98% did not select at least one of the 'containers', 'microservices', 'CI/CD tools', 'cloud environments' or 'source code repositories' options. At the risk of repetition, privileged accounts and secrets are stored in all of these entities.

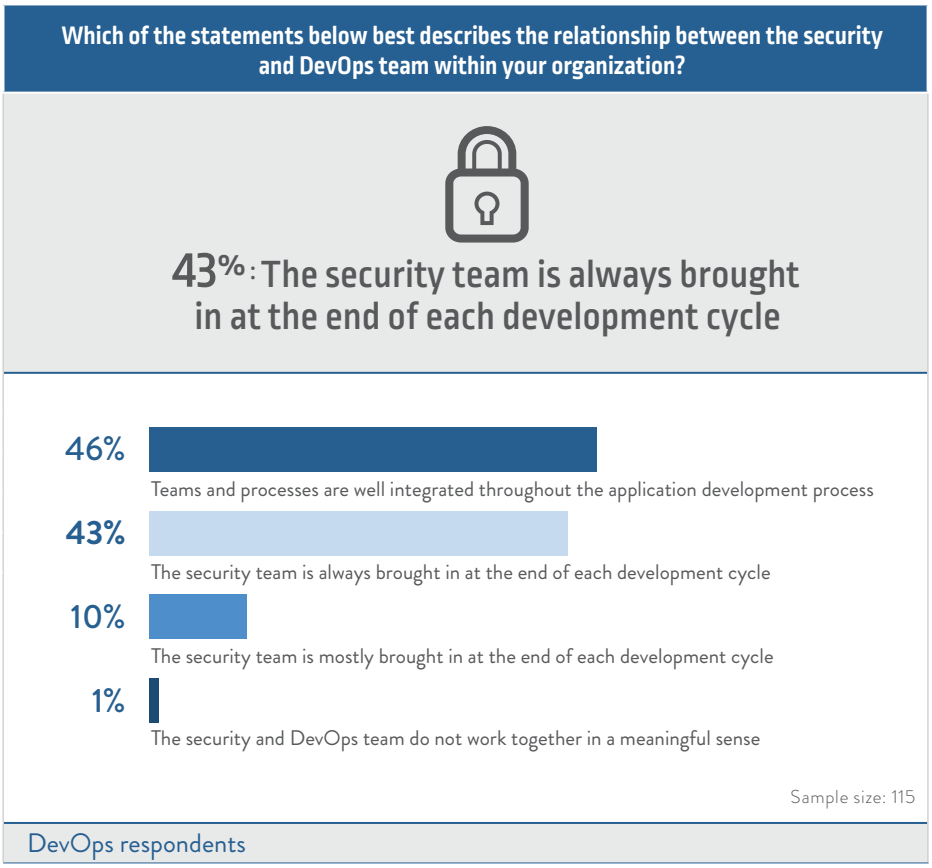


DevOps personnel may not be thinking about security because they – perhaps rightly - don't consider it their ultimate responsibility. Unfortunately, threat actors do make these connections—and explore these areas for access to privileged credentials and secrets. With only 25% of security professionals saying that their organization has a privileged account security strategy for DevOps, attackers are likely to find success in this area.

It takes an integrated team

DevOps is a new discipline, so it's not entirely surprising that respondents report a lack of integration between DevOps and security teams. In fact, fewer than half (46%) of DevOps respondents say the two teams and processes are well integrated throughout the development process. And 43% say that the security team is always brought in at the end of each development cycle. This may be adequate—but only if the length of a sprint averages a week or so. The most effective strategy will demand that security and DevOps work closely together from the very beginning and throughout development, testing and deployment.

It's worth noting that collaboration varies by industry. Closer partnerships between DevOps and security are most often found in consumer services and technology and telecommunications segments. On the other hand, it was surprising that financial services organizations report slightly below-average collaboration. And it was downright troubling to learn that only 16% of healthcare respondents believe that their security and DevOps teams are well integrated.



The fusion of DevOps and security

Fusing DevOps and security tools and processes will be a success marker in protecting privileged information and secrets. What's needed is one dedicated technology tool and a single security stack that can seamlessly connect with DevOps tools and other enterprise security solutions. This singular approach can help unite the fragmented processes and technologies that govern cybersecurity, privacy and regulatory compliance.

It's equally essential that DevOps and security teams be tightly integrated from the outset. This collaborative approach will help businesses build a scalable security platform that is constantly improved as new iterations of tools are developed, tested and released.

Taken together, this year's survey findings indicate that many organizations do not understand the need—or the mechanisms—to secure privileged account credentials and secrets. Three quarters of our survey's IT security pro respondents say their organizations have not deployed privileged security for DevOps. It's time to get started.

Key takeaways

- Vulnerabilities are very real–DevOps teams must build-in security collaboration from the start or risk having new apps blocked on risk grounds.
- Security and IT teams must realize and understand that DevOps practices, whilst powering businesses, are also expanding threat models/potential vulnerabilities.
- The risks being run are unnecessary. Tools and solutions are readily available to secure and manage secrets.
- The issues cannot be ignored as the problem will only get worse; businesses need DevOps and cloud to drive improved efficiency and cost savings.

About CyberArk

CyberArk (NASDAQ: CYBR) is the global leader in privileged account security, a critical layer of IT security to protect data, infrastructure and assets across the enterprise, in the cloud and throughout the DevOps pipeline. CyberArk delivers the industry's most complete solution to reduce risk created by privileged credentials and secrets. The company is trusted by the world's leading organizations, including more than 50 percent of the Fortune 100, to protect against external attackers and malicious insiders. A global company, CyberArk is headquartered in Petach Tikva, Israel, with U.S. headquarters located in Newton, Mass. The company also has offices throughout the Americas, EMEA, Asia Pacific and Japan. To learn more about CyberArk, visit www.cyberark.com, read the CyberArk blog or follow on Twitter via @CyberArk, LinkedIn or Facebook.