CYBERARK®
The Identity Security Company™

merlin®

WHITEPAPER

Protect Federal Agencies by Securing DevOps, Secrets and Other Non-human Identities

Table of Contents

Introduction

Today's software development environments – including those for federal agencies – are highly complex and dynamic, with significant interactions that require seamless access controls and identity management. Developers are being asked to work and test faster and with more agility than ever before to shorten delivery cycles and quickly adapt or respond to new requirements. Meanwhile, because of recent cybersecurity challenges in the software supply chain, the federal government's requirements for secure software development are becoming more stringent. These modern demands for agility, security and reduced production time require an integrated approach, primarily through the process commonly known as DevSecOps (integrated development, security and operations), that enables agencies to satisfy their requirements rapidly and securely.

A significant part of modern development and operations (DevOps) includes the interdependent authentication needs among all the many tools, applications and devices. While identities often relate to personnel, non-human identity management considerations are increasingly required to support a large number of applications, web services, containers, external interfaces and other elements. Federal efforts to promote integrated operations, including extensive cloud-hosted and software-as-a-service (SaaS) implementations, have increased this complexity. So, while many federal efforts (including FISMA metrics) track user account security, recent research has shown that machine identities outnumber human identities by a factor of 45x[1]. This means that federal agencies need to secure both human and non-human identities, a task only possible with a centralized secret management solution. Those doing so must keep the following three critical considerations in mind:

1. Effective secrets management including eliminating hardcoded credentials and centrally managing all non-human credentials - is crucial to improving DevOps security and avoiding costly breaches that damage an agency's reputation.

WHAT ARE APPLICATION SECRETS?

Secrets are non-human credentials that are used to provide applications, automation scripts and tools, containers and micro-services, machine and other non-human identities with secure access to IT resources, cloud services, external databases, other applications and services. They facilitate authentication and authorize access to privileged resources, applications and services, similarly to how humans, like us, use usernames and password to securely access privileged resources.

Too often developers use hard coded passwords in applications or containers, sometimes even in plain text – so anyone with access to the code can potentially exploit the credential. Even encrypted hardcoded credentials are a terrible practice and should be viewed as simply a breach waiting to happen. Such secrets cannot be rotated or audited and can easily be exposed within code repositories.

Examples of non-human secrets and credentials include:

- Cloud access keys, API keys
- GitHub tokens and other application keys and credentials
- SSH keys
- Private certificates for securely communicating, transmitting and receiving data (e.g., TLS, SSL)
- Private encryption keys for systems like PGP
- System-to-system passwords

[1] CyberArk, 2022 Identity Security Threat Landscape Report, April 2022

2. Automation and integration of identity management – including the plethora of non-human identities involved in today's dynamic and dispersed environments – significantly improve the experience of developers, devops and other IT admins.
3. Implementing effective secrets management as part of a holistic identity security platform enables agencies to achieve their missions while ensuring compliance with federal security directives.

A 2023 Verizon Data Breach Investigations Report found that at least half of the breaches that they observed were directly related to lost credentials – in fact, it said, the use of stolen credentials was the most popular entry point for breaches[2]. For web-based applications, that number shot up to 86% since such breaches and incidents tend to be largely driven by attacks against credentials, with the attackers then leveraging those stolen credentials to access a variety of different resources. Password and credential hardcoding (embedding unencrypted credentials like passwords, keys and other secrets into source code and scripts) is a significant problem. Organizations often wrongly use hardcoded secrets thinking it will simplify deployment or operation, but these secrets can often be found with simple tools (or in plain sight, such as in publicly shared code repositories) and once that secret is compromised, it cannot be changed without major software patches[3]. These examples demonstrate the serious risks presented when an agency or provider fails to properly secure their secrets.

Development and operations functions are increasingly automated – while much of the focus for security identity management has been on users and administrators, the reality is that a significant portion of authentication is for securing automated services, applications and other non-human identities.

Securing non-human and human identities is equally vital. Federal enterprises are vulnerable to attacks unless all application identities are secured. Secrets management must enable the organization to defend against attacks by centrally managing and securing secrets for all application types across the enterprise. An effective privileged access management solution combined with secrets management capabilities helps enable secure operations and thwart adversaries.

> Secrets management is a key element of the President's National Cybersecurity Strategy, Objective
>
> *4.5-Support Development of a Digital Identity Ecosystem.*

[2] Verizon, 2023 Data Breach Investigations Report, 2023

[3] See more examples of improperly hard-coded secrets.

In addition to operational security, this also helps to fulfill mandatory requirements for securing federal information systems. NIST's Security and Privacy Controls for Information Systems and Organizations catalog (NIST Special Publication 800-53 Revision 5) describes numerous controls and procedures (more than 55 controls and control enhancements) for identity and access management, illustrating that every one of those non-human and human identities represents a security risk. The likelihood of a breach is increasing at an alarming rate and history has proven that cybersecurity breaches have been shown to originate with an identity management failure. When secrets management falls short, agencies pay a high price.

- In June 2023, a Federal Civilian Executive Branch (FCEB) agency identified suspicious activity in their Microsoft 365 (M365) cloud environment[4]. The agency reported the activity to Microsoft and the Cybersecurity and Infrastructure Security Agency (CISA). Microsoft determined that advanced persistent threat (APT) actors impersonated identities and exfiltrated unclassified Exchange Online Outlook data.
- This attack comes on the heels of an attack that CNN described as "Several U.S. federal government agencies have been hit in a global cyberattack by Russian cybercriminals that exploits a vulnerability in widely used software, according to a top U.S. cybersecurity agency."
- Many recent breaches show the extensive and widespread targeting of federal, state and local entities. While many exploits are financially motivated, the high percentage of state-sponsored attacks put agencies squarely in the bullseye.

IBM's 2023 Cost of a Data Breach Report points out that each public-sector incident costs an average of $2.6 million[5]. Notably, that same report highlights that, on a global average, it took 204 days to detect a breach and an additional 73 days (on average) to contain one. That is a long time for citizen and personnel data to be exposed. Governments at all levels and in every country are at risk. The stakes are high and preparedness is essential.

[4] CISA, Enhanced Monitoring to Detect APT Activity Targeting Outlook Online, July 2023

[5] IBM, 2023 Cost of Data Breach Report, July 2023.

Federal Directives and Initiatives

For many years, government networks depended upon a physical perimeter where everything within the boundary could seemingly be trusted. There are no boundaries in today's interconnected domains and our identities are the new perimeter. For this reason, the federal government is prioritizing protections, particularly the secrets management that are vital to preventing such breaches. Executive Order (EO) 14028 directs federal agencies to advance security measures that significantly reduce the risk of successful cyberattacks against federal government digital infrastructure. In particular, the Office of Management and Budget (OMB) released the federal Zero Trust (ZT) strategy in the M-22-09 Memorandum for Heads of Executive Departments and Agencies. ZT is built upon NIST Special Publication (SP) 800 207, Zero Trust Architecture, which emphasizes the goal to "prevent unauthorized access to data and services coupled with making the access control enforcement as granular as possible."

The CISA Zero Trust model points to the National Security Telecommunications Advisory Committee (NSTAC) which describes ZT as "a cybersecurity strategy premised on the idea that no user or asset is to be implicitly trusted. It assumes that a breach has already occurred or will occur. Therefore, a user should not be granted access to sensitive information by a single verification done at the enterprise perimeter. Instead, each user, device, application and transaction must be continually verified[6]." In other words, agencies must succeed at secrets management.

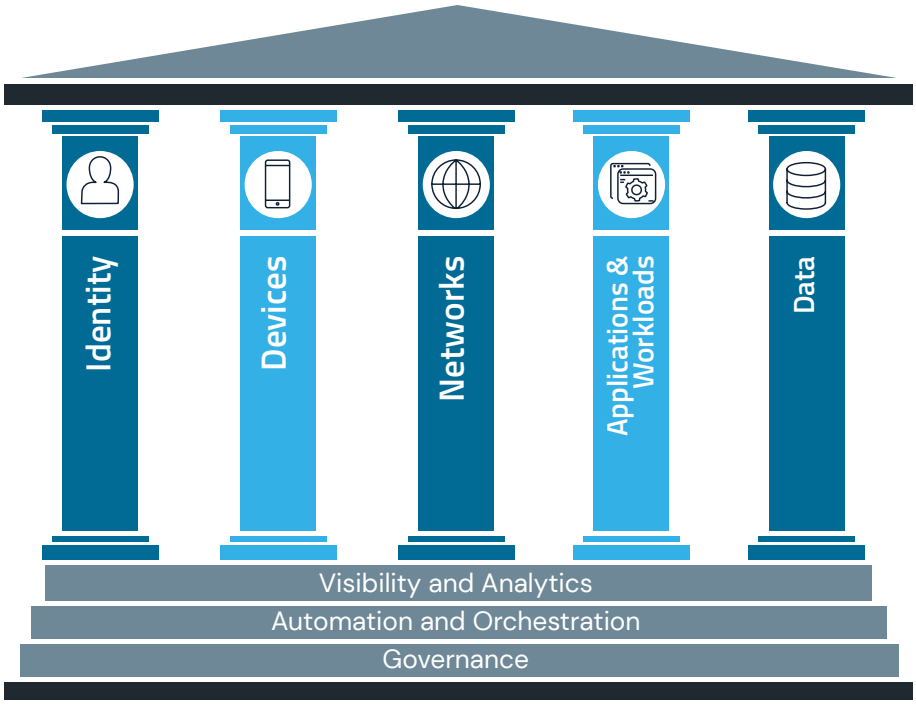

Figure 1 – Pillars from the CISA Zero Trust Maturity Model v2.0

[6]CISA, The President's National Security Telecommunications Advisory Committee. Report to the President on Zero Trust and Identity Management. February 2022.

CISA describes five complementary areas of effort (referenced as pillars): Identity, Devices, Networks, Applications and Workloads and Data, with three themes that cut across these areas (Visibility and Analytics, Automation and Orchestration and Governance). The Software Engineering Institute further points out the connection between ZT and DevSecOps as follows:

"ZT is a security strategy that uses policy to enforce explicit trust between subjects and resources. DevSecOps is a development strategy that combines tools and agility to continuously develop and operate software. Both strategies are interdependent and require balancing concerns of how services, data and infrastructure must be shared to achieve efficiency, cost-effectiveness and risk mitigation for continuous authority to operate (cATO)[7]."

While Zero Trust is a key priority today for public-sector organizations, many other security directives focus heavily on effective secrets management, including:

- FedRAMP: Both "Access Control" (including access management) and "Identification and Authentication" (including identity management) controls are part of federal requirements for all low, moderate and high cloud-based systems. Identity management, authentication methods and privilege management are vital secrets management elements of FedRAMP security plans.
- SOC 2® (System and Organization Controls for Service Organizations) was developed by the American Institute of CPAs (AICPA) and defines criteria for managing customer data based on five "trust service principles"—security, availability, processing integrity, confidentiality and privacy. While SOC2 is not always required for public-sector organizations, many find the independent validation of application security design and information access protections to be a valuable exercise. SOC 2 looks for foundational access controls such as multi-factor authentication (MFA) and intrusion detection, which work together to let users in and keep threats out.
- Controlled Unclassified Information (CUI) protection criteria are described in NIST SP 800- 171 and describe recommended requirements for protecting the confidentiality of CUI that is resident in nonfederal information systems and organizations, or when the information systems where the CUI resides are not used or operated by contractors of federal agencies or other organizations on behalf of those agencies. As with federal security controls, SP 800-171 describes the need for secrets management through access control, identity and access management requirements.

To fulfill these and many other directives, an effective and holistic secrets management solution provides comprehensive protection for the human, non-human and automated transactions occurring within the DevSecOps processes.

[7] Software Engineering Institute, "Integrating Zero Trust and DevSecOps", July 2021

Developing Secure Software

Legacy development approaches, such as waterfall, have proven inefficient; from concept and design and requirements processes to lengthy development, testing and review procedures, this outdated method takes too long for today's teams. Furthermore, historically, security was too rarely engaged throughout development, or they provided high-level requirements and were disengaged until production was complete.

Security practitioners have learned that trying to secure a completed product is complex and ineffective. For many years, the federal government has led an effort to "Build Security In" by working side-by-side with developers, integrating security requirements and capabilities from the beginning. Recently this approach has been reborn as the Secure By Design model which integrates with the DevSecOps model to design and implement security from the concept phase, including integration of secure identity and privilege management to protect confidentiality, integrity and availability. Development teams have demonstrated that DevOps is a practical approach and can integrate security (with DevSecOps) throughout the cycle.

The Increased interaction and automation lead to many of the application identity challenges described above. While a 45:1 ratio of non-human to human identities may seem like a lot, when we consider all of the various accounts and services involved, such as cloud access keys, Jenkins pipelines connecting to GitHub repositories pushing out to Kubernetes environments, it doesn't take long before the secrets start adding up. These applications must be well protected and secured – this requirement is clearly included in both EO 14028 (through the five pillars referenced in Figure 1) and other vital directives.

For DevSecOps teams to successfully navigate and balance the fast pace of development velocity and an evolving security risk landscape, they rely heavily on automated continuous integration/continuous delivery (CI/CD) pipelines and processes. These tools and processes enable engineers to more rapidly build, test, secure and implement applications and services. CI/CD and effective security controls work together to achieve the development results necessary while protecting the secrets that an adversary might exploit. An example of this successful combination is described in Defending Continuous Integration/Continuous Delivery (CI/CD) Environments, a Cybersecurity Information Sheet (CSI) jointly released by CISA and the National Security Agency[8]. The paper points out malicious actors have exploited CI/CD pipelines by using exposed secrets to gain initial access. It highlights the risk that cloud-native CI/CD tools employ numerous secrets to gain access to many sensitive resources, such as databases and codebases.

To combat these threats, the CSI calls for effective secrets management. The paper states "Secure handling of secrets, tokens and other credentials is crucial in a CI/CD pipeline." It warns that secrets (e.g., passwords and private keys) must never be embedded (hardcoded) in software and it calls for a solution that can securely store and manage for resilient CI/CD operation. A fully effective solution will provide a single source of truth that can help rotate secrets for greater flexibility and resilience, enable auditing provision and access to the secrets and support best practices such as segregation of duties.

[8] CISA/NSA, Defending Continuous Integration/Continuous Delivery (CI/CD) Environments, June 2023

Building a Resilient Ecosystem

Application of these "trust but verify" principles to the DevSecOps methodology helps to gain the benefits of increased effectiveness and continuous security. Figure 2, below, from the DoD Enterprise DevSecOps Strategy Guide illustrates the infinite loop of continuous innovation and implementation.

The simplified schematic shown in Figure 2 combines the best of the elements described, delivering a continuous and automated DevOps solution while also continually protecting internal and external resources, all at the speed of innovation.

- Security is at the center and must be considered in each aspect – how will developers, implementers and users be authenticated? How will the application be secured? Will there be secrets that must be protected during development and operations – if so, how?
- Rather than building large monolithic elements, many of these elements are built upon microservices that act as agile application interfaces, each with its own identity, protection and monitoring needs.
- The right side of the diagram speaks to the operations portion. Here again, as secure and reliable software is tested and released into production, the need for dynamic and adaptive identity management, application security, endpoint protections and ongoing assessment are vital.
- Each feedback loop in the process is based upon transparency and speed with automated processes and continuous monitoring/alerting. This approach helps ensure that software is securely designed, securely developed and security implemented, all while enabling, rather than inhibiting, a rapid and agile engineering and development life cycle.

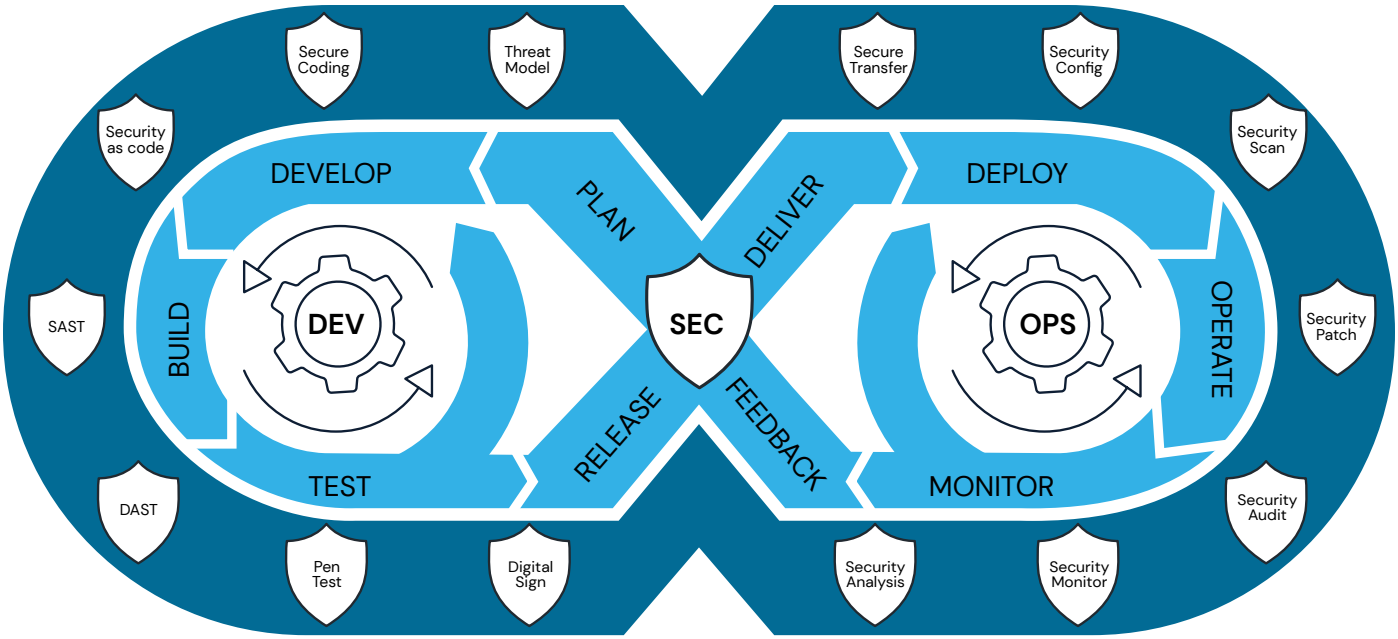

Figure 2 - DevSecOps Distinct Lifecycle Phases and Philosophies

Identity security and secrets management will be at the core of ensuring secure CI/CD pipelines and processes. Organizations will typically operate separate Dev (development) and Prod (production) environments, with multiple pipelines and robust processes in their dev environments. For example, larger development groups with potentially hundreds of developers, may adopt best practices such as setting-up and tearing-down pipelines for each build to ensure no credentials are inadvertently left around after the build is completed. Code bases will be segregated and build processes may be air-gapped.

Federal organizations are particularly accountable for ensuring the security of their cybersecurity supply chain (software developers, cloud providers and external partners). Awareness and attention have been particularly focused on the software supply chain since the December 2020 attack on many agencies through the SolarWinds product line. In that attack, adversaries exploited the lack of a secrets management solution to attack the vendor's supply chain through the CI/CD pipeline. The ability of the attacker to abuse that CI/CD pipeline and create malicious back doors on tens of thousands of victims has particularly raised the issue of cybersecurity supply chain risk management (C-SCRM) throughout most government entities. The federal government has used the incident and several since, as a wake-up call to raise the vigilance of agency risk managers, resulting in several key mandates:

- The NIST Secure Software Development Framework (SSDF), NIST SP 800-218, is a mandatory approach for ensuring that those developing software and those procuring software developed by others must attest to adequate and proper security features, including identity management. Agencies may be forced to remove software products that cannot attest to the safeguards described in this paper.
- NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, requires that agencies ensure that their external partners (and any of their providers) ensure their software's integrity. Among the many C-SCRM requirements described are access control and identity management mandates, including those supported by effective privilege and secrets management solutions.
- Per EO 14028 and the NIST Guidance, Agency Chief Information Officers (CIOs), in coordination with requiring offices and Chief Acquisition Officers (CAOs), must take steps to ensure software producers have implemented and will attest to conformity with secure software development practices (including a secured CI/CD pipeline and effective authentication practices).

Implementing an effective identity security platform will help organizations demonstrate their fulfillment of these important requirements. Failure to achieve identity security places organizations both in jeopardy of a significant breach but also increased accountability and scrutiny from CISA, OMB and other oversight authorities.

Bringing It All Together with Effective Secrets Management

For federal agencies (and for state and local government entities) CyberArk Identity Security Platform, including CyberArk Secrets Management solution, helps fulfill mandatory security requirements (such as those required by the National Cybersecurity Strategy, EO 14028 and security and privacy controls) while providing necessary security for the mission. CyberArk Secrets Management will be implemented as a core part of an overarching identity security approach, seamlessly integrated with endpoint privilege security, privileged access management, cloud security and agency identity management. CyberArk's solution provides centralized visibility and control of secrets and identities across the entire enterprise regardless of the computing environments, application types and interfaces.

Secrets and privileges for human and non-human interactions are used across a diverse and expanding application landscape, so the management solution must support a broad range of direct and out-of-the-box (OOB) integrations for both COTS (Commercial Off-the-Shelf Software) and in-house and custom developer software. CyberArk enables automated rotation of secrets based on policy to reduce the likelihood of compromised credentials and to account for operational needs like personnel changes, technical needs, or simply as a security practice.

Today's interactive and interdependent systems, applications and workloads require flexible vaulting and secrets management solutions that enable security to meet developers where they are (e.g., some development teams may prefer APIs, alternatively others may prefer to use the built-in secrets managers of the cloud service providers, such as AWS Secrets Manager or Azure Key Vault). Meeting the developers where they are with an effective solution that enables productivity with no changes to the development workflows, leads to higher adoption of secrets management tools and processes which ultimately improves the agencies overall security posture.

To ensure that security processes don't slow down the development and testing cycles, one must meet the developers where they are. CyberArk provides solutions that are easy to implement and well-integrated with the CI/CD platforms, with proven integration partnerships. This supports DevSecOps by directly meeting both security and development teams where they are with secrets management solutions that:

- Minimize impact on existing processes, for example by not requiring code changes or changes to developer workflows.
- Offer out-of-the-box seamless integrations with widely used cloud-based, SaaS solutions and DevOps tools.
- Enable key functions to be automated to improve operational efficiency and reduce the burden on security, development and operations teams.
- Operate at scale while delivering extremely high levels of performance and security.
- Centrally manage, rotate and secure human and non-human identities across the agency.

The power and promise of DevSecOps have helped to bring significant benefits to public-sector organizations as they create, maintain and operate secure and reliable software products. Digital technology touches every aspect of every one of our constituents, so we must maintain a model that is only possible at the intersection of quality, stability and security. As recent security breaches have shown, failure to provide identity security puts constituents at risk, damages the entity's reputation and may jeopardize the organization's mission.

While automation and integration are vital parts of the cycle, the DevSecOps model is still built upon collaboration among people and machines. The only viable solution must secure both human and non-human identities. Privileged access management is essential for the many identities at work throughout the enterprise, including administrators, workers, third parties, customers and others. Secrets management is equally vital for the many internal and external applications, services, databases and operations technology on which the organization depends. These solutions work together, along with endpoint protection, cloud security, automation and orchestration and other elements, to form a comprehensive identity security ecosystem.

The solution must extend to external partners and providers. Through a comprehensive approach such as CyberArk Identity Security plaform, global components of the infrastructure can work together safely to support secure, agile development and continuous integration/deployment through effective and integrated tools.

Conclusion

The consequences of not securing application credentials (such as through the CyberArk secrets management product) are clear from recent and historical breaches. The stakes for agencies are high and the mission is vital for federal stakeholders. While all cybersecurity attacks are regrettable, the large number of victims involved in or vulnerable to attacks on government infrastructure and the likelihood that a motivated and well-funded nation-state may be at the root of such an attack, mean that those who fail to invest in a proven, holistic identity security solution must answer to their citizens and constituents. The nature of the data exposed or stolen through attacks has the potential to disrupt government operations, jeopardize national security and even puts lives at stake. Fortunately, CyberArk Secrets Management as part of the CyberArk Identity Security Platform, is an effective solution that is ready to rapidly deploy, supporting effective development and security success while helping to fulfill federal mandates like Zero Trust and cyber supply chain requirements.

Next Steps

Attacks, especially by motivated and well-funded adversaries, are on the rise. There is no time for delay. Learn how CyberArk can help you with securing your secrets.

About CyberArk

CyberArk is the global leader in identity security. Centered on intelligent privilege controls, CyberArk provides the most comprehensive security offering for any identity — human or machine — across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets.

CYBERARK®
The Identity Security Company™