CyberArk Discovery & Audit

The average enterprise has **3-4x** as many privileged accounts as employees. Scan your network with CyberArk DNA™ to:

- Locate privileged accounts on- premises and in the cloud, and on existing DevOps tools
- Identify all privileged passwords, SSH keys and password hashes
- Clearly assess privileged account security risks
- Collect reliable and comprehensive audit information

Sample Executive Summary Dashboard for easy insight into issues

The Challenge

Privileged accounts provide administrative access to IT systems, public cloud infrastructure, business applications, and sensitive data. As a result, these accounts are targeted by advanced and insider attackers in the vast majority of cyber attacks. Yet, many organizations are unaware of the volume and location of privileged accounts throughout their IT environments.

Without visibility into the scope of privileged accounts and privileged account risks, organizations can face a variety of on-going challenges, including:

- **Large attack surface.** Privileged accounts are everywhere. Every piece of hardware and software in both on-premises and cloud-based environments and DevOps tools has built-in administrative accounts. Service accounts and over-privileged user accounts only add to this challenge. Combined, the sheer volume of these accounts creates a massive attack surface.
- **Inability to measure risk.** With cyber attacks in the headlines nearly every day, executive teams and boards of directors are increasingly asking about exposure to threats. Without visibility into privileged accounts, which are compromised in the vast majority of targeted attacks, security teams cannot accurately assess cyber security risk or the resulting business risk.
- **Increased risk of compromise.** Password hashes, SSH keys, AWS Access Keys and misconfigurations throughout the IT environment can easily be exploited by attackers inside the network. Without visibility into the full scope of these risks, organizations cannot effectively mitigate these risks to reduce the likelihood of a successful cyber attack.

The Solution

CyberArk Discovery & Audit (DNA) is a powerful tool (available at no charge) that scans systems on your network to uncover accounts, credentials and misconfigurations that can create risk. Following a scan, CyberArk DNA generates a detailed report that IT auditors and decision makers can use to evaluate the status of privileged accounts in the organization and identify areas of risk. The tool is an agentless, lightweight executable designed to expose the magnitude of the privileged account security challenge in on-premises and cloud-based environments. CyberArk DNA helps organizations uncover:

- **Windows accounts and account statuses.** Identify privileged and non- privileged Windows accounts, including local administrator, domain administrator, standard user and service accounts. View the password strength, password age and last login date.
- **Unix accounts, credentials and permissions.** Centrally view the status of root and individual user accounts on Unix systems, identify SSH key pairs and trusts, and uncover misconfigured sudoers files that can increase the risk of unauthorized privileged escalation.
- **Privileged domain accounts.** Discover dormant or unprotected privileged domain service accounts that have access to critical assets or services.
- **Pass-the-Hash vulnerabilities.** Locate password hashes vulnerable to theft, and gain a visual map of Pass-the-Hash vulnerabilities and potential pathways to sensitive data and critical assets.
- **Hard-coded application credentials.** Identify systems that have embedded, hard-coded or exposed credentials in plain-text, which can be captured by malicious attackers inside the network.

- **Public cloud users, credentials and vulnerable machines.** Identify AWS Identity and Access Management (IAM) users, discover AWS Access Keys and EC2 key pairs, and learn the status of AWS credentials. Through integration with Amazon Inspector, identify machines in AWS that have an increased risk of compromise.
- **Hidden credentials in DevOps tools.** Automates discovery of hidden credentials in leading DevOps tools, including Ansible (Playbooks, Roles and Tasks) through the CyberArk integration with Ansible. This helps improve and simplify securing CI/CD pipelines.
- **Compliance status of accounts and credentials.** Enter compliance parameters prior to scanning the network so that you can easily see which privileged accounts and credentials are within policy and which require remediation.

After running a network scan, CyberArk DNA will generate both an executive summary and a technical inventory of accounts, credentials and risks. The executive summary can help management teams understand the complete scope of privileged account risks, potential audit risks and the highest risk accounts in the environment. The technical report can help teams prioritize remediation efforts and identify which specific systems, accounts or users need attention first.

Benefits

CyberArk DNA provides organizations with visibility into the true scope of privileged account risks, enabling them to quantify risk and take the first step towards mitigation.

The insights gained from CyberArk DNA enable organizations to:

- **Accurately assess privileged account risks.** Gain full visibility into high-risk accounts, credentials and users in traditional, AWS, and DevOps environments. Initial DNA scans can provide a baseline of privileged account risk, and subsequent scans can help quantify risk reduction over time.
- **Quickly uncover risks and vulnerabilities on-premises and in the cloud.** Fast, accurate reporting on privileged account information enables organizations to immediately pinpoint unknown or improperly managed accounts and act quickly to address any issues.
- **Identify high-risk systems in public cloud environments.** Uncover systems in AWS environments that have unresolved risks, and use this insight to better protect applications and data that run on these systems.
- **Create a prioritized project plan to effectively reduce risk.** Use the information learned from a DNA scan to identify high, medium and low risk accounts, and build a phased, manageable project plan to address the highest risks first.
- **Build a business case for privileged account security.** Identity valuable assets and data that are exposed to privileged account risks, and quantify the risk of failed audits due to non-compliant accounts. Measure the potential business impact of unmanaged and compromised accounts, and use this figure to request budget and resources.

Take the first step today

CyberArk DNA can help you uncover privileged accounts, build a business case for a privileged account security program and prioritize the highest risk accounts that require attention first. Once you have the plan in place, the comprehensive CyberArk Privileged Account Security Solution can help you proactively lock down privileged account credentials, secure and control access to privileged accounts, and continuously monitor user and account activity to rapidly detect threats. Visit www.cyberark.com/DNA to take the first step towards reducing risks today.

Specifications

CyberArk DNA™ runs on

- Windows 7
- Windows 8
- Windows 10

Supported Target Systems

- Both 32-bit and 64-bit versions are available for all platforms

Windows Workstations:

- Windows 2000
- Windows XP
- Windows Vista
- Windows 7
- Windows 8
- Windows 10

Windows Servers:

- Windows 2000
- Windows 2003
- Windows 2008
- Windows 2012

Unix:

- RHEL 4-7.1
- Solaris Intel and Solaris SPARC 9, 10, 11
- SUSE
- Fedora
- Oracle Linux 5
- CentOS 6
- AIX 5.3, 6.1, 7.1
- ESXi 5.0 and 5.1
- IBM Virtual I/O Server 2.2.x
- IBM Hardware Management Console 7Rx.x and 8Rx.x

Application Servers:

- Windows IIS applications
- WebSphere applications
- WebLogic applications

Public Cloud Infrastructure:

- Amazon Web Services

DevOps Tool Integrations:

- Ansible

Network Protocols

- Windows:
  - Windows File and Print Sharing
  - Windows (WMI)
- Unix:
  - SSH
  - SFTP

Sample Scanned Data

- Windows and Unix Accounts
- Domain Accounts
- Local Accounts
- AWS IAM Users
- AWS Access Keys
- EC2 Key Pairs
- Ansible Playbooks, Roles and Tasks
- Windows Services
- Windows Scheduled Tasks
- Hard-coded credentials
- Credentials on endpoints