CYBERARK

DATA SHEET

DOMAIN CONTROLLER PROTECTION

Protect Windows Domain Controllers against sophisticated Kerberos-based attacks

SPECIFICATIONS

Attack Techniques Detected:

- Golden Ticket
- Pass-the-Hash
- Overpass-the-Hash
- Pass-the-Ticket
- Privilege Attribute Certificate (PAC) Manipulation

THE CHALLENGE

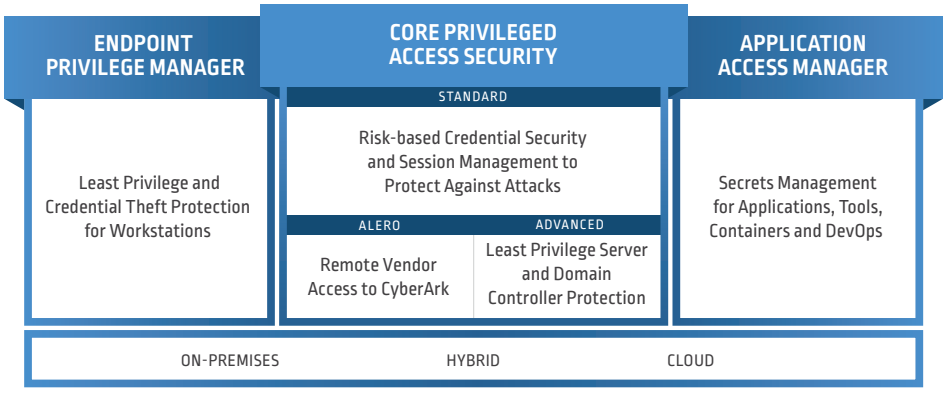
Domain Controllers are the crown jewels for attackers and if not secured properly, improper access to these assets can be devastating for an organization. Attackers can exploit vulnerabilities in Kerberos, the default authentication protocol for Microsoft Windows, to impersonate authorized users, traverse a network and gain access to confidential data and critical IT resources.

Kerberos uses renewable tickets (security tokens) to authenticate users and hosts. Bad actors can use readily available open-source tools to generate or manipulate Kerberos tickets to gain unauthorized access to various Windows accounts including privileged domain administrator accounts. Posing as a legitimate user, a savvy attacker can easily move undetected across the network, navigating from host to host to steal data, spread malware or wreak havoc in any number of ways.

THE SOLUTION

The advanced Domain Controller Protection within the CyberArk Core Privileged Access Security Solution is an ultra-lightweight agent that continuously analyzes network behavior, detects in-progress and potential Kerberos attacks, allows only approved applications to run and helps contain credential theft and secures data leakage. Deployed on a Windows Domain Controller, the CyberArk Domain Controller Protection solution defends against impersonation and unauthorized access, helping organizations bolster security and reduce the risk of irreversible network takeovers.

CYBERARK PRIVILEGED ACCESS SECURITY SOLUTION



The Domain Controller Protection solution is an integral component of the CyberArk Core Privileged Access Security Solution

In conjunction with other Privileged Access Security Solution components, the solution can restrict domain access, protect against credential theft and enforce application control on Domain Controllers, which helps to minimize the risk of a total network takeover.

The CyberArk Domain Controller Protection solution uses a combination of deep packet inspection, machine learning algorithms and advanced analytics to identify unusual user behavior and system activity in real-time, helping organizations detect, isolate and mitigate Kerberos attacks before they can do significant damage. The solution examines typical patterns of individual privileged users, privileged accounts and system activities to establish a baseline of normal behavior. By analyzing real-time activity, the Domain Controller Protection solution can detect anomalous activities such as credential theft, lateral movement and privilege escalation that are symptomatic of Kerberos attacks and other threats to Domain Controllers.

With early notification, IT operations and security teams can take appropriate action such as rotating compromised security credentials before attackers gain access to their target and accomplish their mission. The versatile CyberArk solution protects against a wide range of well-known Kerberos attack techniques, including:

- **Golden Ticket** – where an attacker gains access to the Kerberos Key Distribution Center (KDC) to generate a Golden Ticket—a master security token providing complete access to an entire domain.
- **Pass-the-Hash** – where an attacker retrieves and exploits password hashes stored in the Security Accounts Manager (SAM) or Active Directory database to impersonate a legitimate user.
- **Overpass-the-Hash** – where an attacker uses the hash of one user account to obtain a Kerberos ticket, which is used to access other accounts and network resources.
- **Pass-the-Ticket** – where an attacker extracts a Kerberos Ticket Granting Ticket (TGT) from Local Security Authority Subsystem (LSASS) memory on a host, and uses it to gain access to other network resources.
- **Privilege Attribute Certificate (PAC) Manipulation** – where an attacker modifies Kerberos ticket permission settings to gain unauthorized access to network resources.

CREDENTIAL THEFT

The Domain Controller Protection solution in conjunction with CyberArk Endpoint Privilege Manager can help organizations identify and quickly remediate credential theft on user endpoints and Domain Controllers. Relevant credential theft detections and blocks include:

- Local Security Authority Subsystem Service (LSASS), Local Security Authority (LSA), Security Account Manager (SAM), Activity Directory Database (NTDS.dit), Domain Local Cache, Crypto RSA Machine Keys and Service Accounts

BENEFITS

- **Mitigate security risks. Improve security posture.** Avoid confidential data loss and business disruptions that can result from Kerberos attacks. Safeguard security credentials and security data.
- **Improve visibility.** Detect in-progress and potential Kerberos attacks before perpetrators gain access to critical systems and do irreversible harm.
- **Reduce operations expense and complexity.** Eliminate ineffective, manually intensive attack detection and mitigation processes by employing sophisticated machine learning algorithms and advanced analytics.
- **Accelerate time-to-value.** Defend against a wide array of common Kerberos attack techniques using a single solution. Use in combination with other CyberArk Core Privileged Access Security Solution components to reduce attack surfaces, proactively manage security credentials and restrict lateral movement.

WHY CYBERARK

CyberArk is the global leader in privileged access 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 500, to protect against external attackers and malicious insiders.