CYBERARK

SOLUTION BRIEF

MITIGATING ENDPOINT SECURITY RISKS

UNIFIED AUTHENTICATION AND LEAST PRIVILEGE MANAGEMENT

HIGHLIGHTS

Strengthen Endpoint Security

Protect against data breaches or malicious attacks from lost, stolen, or compromised access credentials. Grant the right people the right access privileges to the right endpoints at the right time.

Optimize User Experience

Provide fast, secure, frictionless, and convenient access to endpoints and network services. Allow end-users to request elevated access privileges—quickly and easily—without engaging the help desk or entering a second set of admin credentials.

Simplify Operations

Streamline security operations and free up staff by automating manually intensive, time-consuming administrative tasks.

THE CHALLENGE

Today's savvy cybercriminals are always seeking new ways to steal access credentials, escalate privileges, and move laterally across a network to wreak havoc. Lax password management practices and manual administrative processes can lead to security vulnerabilities and privilege creep, and open the door for adversaries to infiltrate networks, steal data, and disrupt business.

A wide variety of endpoints are vulnerable to attack, including physical and virtual desktops, servers and VMs, and corporate-owned devices and BYOD endpoints. Endpoint-targeted attacks like phishing and ransomware can damage a company's reputation and lead to costly lawsuits, fines, and revenue loss.

Businesses must find ways to secure access to desktops and servers, and tightly control access to privileged accounts and applications without impairing the user experience or overburdening the help desk.

THE SOLUTION

CyberArk's comprehensive endpoint security solution lets businesses secure access to endpoints and enforce the principle of least privilege without complicating IT operations or hindering user productivity. The unified endpoint authentication and privilege management solution helps organizations strengthen access security, optimize user experiences, and eliminate the manually intensive, error-prone administrative processes that can lead to overprovisioning and privilege abuse.

The integrated CyberArk solution improves security by providing Adaptive Multi-Factor and passwordless authentication when a user first logs in to an endpoint. If the user attempts to launch a privileged application or gain access to a privileged account the solution again validates the user's identity using adaptive multi-factor authentication before temporarily elevating their privileges.

Adaptive Multi-Factor and Passwordless Authentication for Endpoints

The CyberArk endpoint security solution includes Adaptive Multi-Factor Authentication (MFA) to help organizations tightly control access to desktops and servers. Adaptive MFA uses contextual information (location, time-of-day, device type, user risk, etc.) and business rules to determine which authentication factors to require when a particular user logs on to an endpoint. Adaptive MFA provides a high level of authentication assurance and protects businesses against impersonation, credential theft, phishing scams, and other endpoint-related threats.

The solution also supports a wide range of authentication mechanisms, including passwordless factors, hardware tokens, authenticator apps, and SMS-based codes, certificate-based device trust. The combination of context-based authentication and breadth of supported authentication factors strengthens security and reduces friction resulting in improved end-user satisfaction and productivity.

Least Privilege Management

Privileged endpoint accounts like Microsoft Windows or macOS administrator accounts represent one of the most significant security vulnerabilities an organization faces today. Attackers can gain unauthorized access to privileged account credentials and traverse a network, taking over workstations, servers, and other critical infrastructure. Bad actors can also exploit privileged endpoint accounts to disable threat detection programs, install malware, and launch damaging cyberattacks.

The CyberArk endpoint security solution helps reduce privileged access security risks by removing local admin rights from endpoints, and temporarily elevating end-user privileges with built-in Adaptive Multi-Factor Authentication for specific tasks—on-demand, in real-time—with minimal help desk involvement. The solution protects against ransomware by intelligently blocking or restricting suspicious or untrusted applications and defends against credential theft by safeguarding passwords and other credentials cached by Windows, web browsers and other programs.

WHY CYBERARK?

CyberArk is the global leader in Identity Security. Centered on privileged access management, CyberArk provides the most comprehensive security solutions for any identity – human or machine – across business applications, distributed workforces, hybrid cloud workloads, and throughout DevOps pipelines.

The world’s leading organizations trust CyberArk to help secure their most critical assets.

KEY FEATURES

Just-in-Time Privilege Elevation

Remove local admin rights from endpoints and dynamically escalate privileges for a predefined period of time to allow end-users to install or run applications or reconfigure endpoint settings. End-users can request elevated permissions on-demand, directly from the desktop when launching a privileged application, without having to log in as an administrator or enter another password. Requests are approved manually by authorized administrators or automatically based on policy.

Ransomware Protection

Tightly control how applications run. Allow trusted applications to run normally. Block malicious software. Force unknown applications to run in a restricted mode with no access to the corporate network.

CERTIFICATE-BASED DEVICE TRUST

The agent can manage the lifecycle of a certificate on the endpoint. This certificate can act as a conditional access factor for sensitive apps that shouldn't be accessed on non-trusted devices.

Credential Theft Protection

Automatically detect and block attempts to steal credentials cached by Windows, web browsers, password managers, Single Sign-On solutions, and other programs. Improve protection against impersonation, phishing, spear-phishing, social engineering and other scams by requiring two or more distinct mechanisms to validate a user's identity.

Risk-Aware, Adaptive Multi-Factor Authentication

Strengthen endpoint access security by requiring multiple forms of authentication. Reduce user frustration by using contextual information and machine-learning-driven, risk-based access policies to determine which authentication factors to apply to a particular user under particular conditions. Take into account a range of variables, including location, time-of-day, day-of-week, IP address, networks, or device type.

Wide Range of Authentication Factors

Choose from a variety of authentication factors, including push notifications to a mobile device, one-time password tokens, SMS messages or email notifications.

User Behavior Analytics and Reporting

Get insights into identity and authentication incidents on the endpoint via reports and dashboards. Investigate, explore, and orchestrate automated responses to identity incidents.

Variety of Endpoints

Improve the security of Windows Server, Windows Desktop, and macOS computers using a single solution with a common administrative console.

Connection we solve IT

1.800.800.0014
www.connection.com/CyberArk

CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice.