Securing Endpoints and Servers

CYBERARK

Secure Every Human Identity with Endpoint Identity Security

SOLUTION BRIEF

Neglecting identity security controls on the endpoint can lead to a weakened security stance, expanded attack surfaces and the risk of non-compliance.

IDENTITY-BASED ATTACKS ON THE ENDPOINT

Organizations are constantly battling new cyber threats, and one of the ever-growing attack vectors is at the endpoint. The CyberArk 2024 Identity Security Threat Landscape Report illustrates the impact cyberattacks have on organizations.

Attackers target the identities on the endpoint, accessing privileged accounts and credentials. This allows them to bypass traditional security controls and access critical systems and data throughout the organization without being detected.

93%

of enterprises have experienced two or more identity-related breaches.

65%

of office workers bypass cybersecurity to boost productivity.

89%

of organizations were targeted by ransomware and 75% affected by ransomware paid the ransom without recovering the data.

Challenge

As organizations struggle with cyber threats, identity security at endpoints and servers is often overlooked.

Lack of Strong, Preventive and Continuous Identity Assurance

Organizations today have limited visibility into identity aspects of end-user computing and server security. Without identity assurance, organizations cannot effectively enforce least privilege or manage local admin rights to proactively protect against identity-and privilege-based attacks. This makes it easier for attackers to pose as legitimate users.

Overprivileged Users and Applications

Traditional binary identity security measures create friction, due to the lack of flexibility to allow for elevated privileges when needed. This leads to privilege sprawl that attackers take advantage of, making it easier for them to push malware and gain initial access and persistence to then move laterally through the organization.

Unmanaged Endpoint Attack Surface

Despite 91% of enterprises believing that third parties are a significant risk to their environment, they continue to expose their systems, applications and data through unmanaged endpoints owned by employees, vendors, contractors, auditors and other third parties. This attack surface presents an entry point for attackers and creates a direct data exfiltration path.

Strong security at the endpoint requires the right level of privilege controls applied across all identities. Only then can organizations meet the security needs of the modern workforce.

STRENGTHEN ENDPOINT SECURITY

CyberArk Endpoint Identity Security enables organizations to manage and secure identities and privileges on the endpoint through capabilities including:

- Passwordless experience for login and elevation on the endpoint
- Strong authentication and secure sign-in to devices
- Removal of local admin rights and least privilege enforcement
- Discovery, onboarding and password rotation for privileged accounts
- Comprehensive application control
- Credential theft protection
- Just-in-time privileges enablement
- Secure browsing
- Identity Bridge to enable centralized identity governance and administration on Linux systems

CyberArk is a Leader in multiple analyst reports, including a Leader in the 2024 Gartner® Magic Quadrant™ for PAM. CyberArk also scored the highest in Windows PEDM Use Case in the 2024 Gartner® Critical Capabilities for PAM. The solution has also received FedRAMP High certification.

Solution

The CyberArk Endpoint Identity Security solution embodies the vision of securing every human identity on the endpoint with the right level of privilege controls.

Extend Identity Security and Zero Trust

Secure every human identity working both on desktops and servers against sophisticated cyber threats that target and abuse users' identities and privileges. Enforce role-based least privilege and significantly reduce the attack surface with robust identity security measures for endpoint security, such as passwordless desktop sign-in, strong continuous multi-factor user authentication and the discovery and removal of local admin rights.

Reduce the Endpoint Attack Surface

Fortify defenses against advanced cyber threats with capabilities such as comprehensive application control, credential theft prevention and secure browsing. Take a proactive, identity-centric endpoint defense strategy to prevent lateral movement with rapid risk reduction policies, application greylisting and isolation and step-up authentication.

Reduce IT Security and Operational Costs

Enhance operational efficiency and the end-user experience by enabling flexible privilege management, reducing security alerts and decreasing the need for manual IT interventions. Simplify reporting on application usage, cut down on unused software licenses and further increase operational efficiency with transparent application elevation and integration with ticketing systems, just-in-time access and an end-to-end passwordless user experience.

Demonstrate Compliance and Meet Audit Requirements

Address the critical need for improved visibility and the implementation of foundational endpoint security controls mandated by regulations and auditors. Audit and monitor activity on the endpoint to check off compliance and cyber insurance requirements.

Learn more about how to secure identities at the endpoint.

Gartner® Magic Quadrant for Privileged Access Management, by Abhyuday Data, Michael Kelley, Nayara Sangiorgio, Felix Gaehtgens, Paul Mezzera, 9 September 2024.

Gartner® Critical Capabilities for Privileged Access Management, by Paul Mezzera, Abhyuday Data, Michael Kelly, Nayara Sangiorgio, Felix Gaehtgens, 9 September 2024.

Gartner is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, Magic Quadrant is a registered trademark of Gartner, Inc. and/or its affiliates and is used herein with permission. All rights reserved.

Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

CYBERARK®