Click Here

2025 Identity Security Landscape – Download Report By combining secure SSO, Adaptive MFA, Lifecycle Management, Directory Services and User Behavior Analytics, we help you streamline operations and give users simple and secure access to resources—on-premises, cloud, hybrid—from any location, using any device. Apply world-class intelligent privilege controls across the IT estate, as well as differentiated controls to secure the unique needs of workforce users, third-party vendors, endpoints and machine identities as they access sensitive data. Streamline HR processes, ensure users have the right access to the right resources, enable compliance with industry or government regulations, and improve efficiencies across the board with orchestration and lifecycle management, permissions and entitlements, and directory and federation services. “If we can control identity, we can stop most modern attacks. That is what I call true Zero Trust and that is why we use CyberArk. This is what helps me sleep at night.” Brian Miller, CISO, HealthFirst Error - something went wrong! Implementing least privilege can be daunting, especially in today’s complex identity security landscape. CyberArk QuickStart Least Privilege Framework in Endpoint Privilege Manager (EPM) makes it easy to get started. With pre-configured policies, QuickStart helps security teams enforce least privilege and achieve immediate risk reduction with just a few clicks. This whitepaper shows how QuickStart enables you to: Quickly reduce the endpoint attack surface with layered, identity-based policies. Enforce least privilege through just-in-time elevation and role-based access controls. Discover and secure applications without disrupting users or overloading IT. Download the whitepaper to learn more. Information security professionals recognize that cyber attackers will exploit endpoint vulnerabilities and then make a beeline for privileged credentials. As a result, organizations are evaluating how they can take steps to secure privilege on the endpoint as a fundamental part of their security program. CyberArk Viewfinity has enabled organizations to reduce both the attack surface and the risk of information stolen or encrypted and held for ransom—all while achieving the right balance between productivity and security. To keep pace with the ever-evolving threat landscape, we unveiled new threat protection features this week: CyberArk Viewfinity is now available as CyberArk Endpoint Privilege Manager. By interlocking three core capabilities: privilege management, application control and new credential theft detection and blocking, CyberArk Endpoint Privilege Manager represents a combination of powerful technology, deep research and best practices to stop attackers from advancing beyond the endpoint and doing damage. Key enhancements include: New behavioral analytics to block and contain advanced threats targeting credential theft at the endpoint. The ability to detect and block credential theft attempts by malicious users and applications, including Windows credentials, remote access application credentials and those credentials stored by popular web browsers for use with, for example, corporate network and cloud applications. The ability to block hash harvesting at the endpoint to prevent Pass-the-Hash, an attack leveraging stolen credentials. The introduction of CyberArk Endpoint Privilege Manager comes on the heels of an FBI flash alert that recommends prioritizing credential protection, including implementing least privilege and restricting local accounts, to limit a threat actor’s ability to gain highly privileged account access and move throughout a network. CyberArk Endpoint Privilege Manager is available now. For additional resources on detecting and containing cyber attacks while effectively balancing security and productivity, visit . ×Sorry to interruptCSS Error CyberArk is the global leader in Identity Security. Centered on privileged access management, CyberArk provides the most comprehensive security offering for any identity – human or machine – across business applications, distributed workforces, hybrid cloud workloads, and the DevOps lifecycle. The world’s leading organizations trust CyberArk to help secure their most critical assets. For over 25 years, CyberArk has led the market in securing enterprises against cyber attacks that take cover behind insider privileges and attack critical enterprise assets. Today, only CyberArk delivers a new category of targeted security solutions that help leaders stop reacting to cyber threats and get ahead of them, preventing attack escalation before irreparable business harm is done. At a time when auditors and regulators recognize that privileged accounts are the fast track for cyber attacks and demand stronger protection, CyberArk’s security solutions master high-stakes compliance and audit requirements while arming businesses to protect what matters most. ×Sorry to interruptCSS Error CyberArk Endpoint Privilege Manager (EPM) enforces least privilege and enables organizations to block and contain attacks on endpoint computers, reducing the risk of information being stolen or encrypted and held for ransom. A combination of privilege security, application control and credential theft prevention reduces the risk of malware infection. Overview In today's world, corporate environments are more vulnerable than ever, requiring careful application control and user privilege management. EPM introduces a combined solution for application control, privilege management, and threat protection. This full set of application control and privilege management provides granular control to a secure desktop and server environment. Setting up a risk-based application control framework establishes default behavior for managing unclassified applications in your Windows environment. Privilege management Certain Windows applications and desktop functions require local administrative privileges to run and function properly on a desktop or laptop, a requirement that is reflected in the “Run as Administrator” option. This requirement is mostly handled by implementing two contradicting approaches: least-privileged user account and the “Run As” method. The least-privileged user account (LUA) approach ensures that users always log on with limited user accounts. Using this strategy, you can ensure that administrative tasks are only carried out by administrators who have administrative credentials. The LUA approach can significantly reduce the risks from malicious software and accidental incorrect configuration. However, the high amount of planning, testing, and support involved in the implementation of the LUA approach can make this approach highly expensive and challenging. On the other hand, granting full administrator rights to standard users is considered a highly risky process, because it can compromise the safety of the desktop environment and enable the operation of malicious hackers and viruses. The associated increased security risk often breaches compliance regulations put in place by the Sarbanes-Oxley Act and HIPAA. Additionally, the United States Government Configuration Baseline (USGCB) and Federal Desktop Core Configuration (FDCC) mandates stipulate that administrative rights cannot be granted to endpoint users and cannot be made available on federal desktops and laptops. The EPM Privilege Management solution addresses this issue and provides the optimal balance by elevating the privileges of standard users – that is, granting such users administrative privileges – for certain processes or applications only, rather than at the user account level. When permissions are raised, the elevation is performed directly within the security token of the process. The application or process is started by using the current user credentials, as opposed to using “Run As”, which needs an administrative account to raise privileges. The “Run As” method potentially introduces security risks and issues, for changes that are written into a current user registry. The EPM Privilege Management solution can be configured to collect events triggered by applications not covered by EPM explicit policies (unhandled applications) to a designated location, the Events Management page, as a result of any of the following: An attempt to run an unhandled application requiring administrative privileges A new occurrence of an unhandled application requiring administrative privileges Custom endpoint user requests Application Control The EPM Application Control product provides a method of ranking unhandled applications and resources, which have not yet been identified as safe (allowed) or threatening (denied). You can configure events to be collected to a designated location, called the Application Control Inbox, as a result of any of the following: EPM Application Control detects an attempt to run an unhandled application A new occurrence of an unhandled application (installation, download and so on) An attempt to access sensitive resources (Internet/Intranet sites, network shares, local files/folders, or registry keys) The applications are then evaluated and, based on the evaluation results, are blocked, restricted, or allowed to run. If certain applications should only be run under specific circumstances, Application Control offers flexible rules that enable IT Administrators to automate the handling of such applications. Instead of completely locking down the desktops of endpoint users, you can block or unblock the running execution of a specific application for the same endpoint users by simply applying different EPM policies. For example, if the brokerage division has a specific policy that prohibits any instant messaging software from running, employees within this division are assigned to the brokerage group and are usually not allowed to run this type of software. However, if two of this division’s employees take part in a conference abroad they can be assigned to a special EPM policy for traveling personnel, thereby allowing them to use instant messaging software. Using Application Control enables you to establish automated rules for identifying approved applications through trusted sources. Creating trusted sources highly simplifies and shortens the application handling process, by reducing the number of application events collected into the inbox. Using trusted sources, EPM system administrators can group together applications that would be elevated as required based on a particular set of criteria, such as applications located in a specific network share or installed by a verified software distribution system. The concept of trusted sources is enhanced by a powerful “Inherited trust” mechanism. This mechanism extends the trusted source concept to other applications installed by the original trusted source applications, even if these applications bear different properties. For example, defining Microsoft's System Center Configuration Manager (SCCM) as a trusted source means that all applications distributed by SCCM are considered as trusted, regardless of their digital signature and other properties. Also, any additional applications installed by these applications are considered “trusted” as well, and this trust continues from application to application. As the source information accompanies a file throughout its entire lifetime, the policy maintained by trusted sources is applied retroactively. For example, if an application was installed by a distribution system, after creation of a policy defining the distribution system as a “trusted source”, the application is considered “trusted”. Moreover, the “trust” is still applied to the application even if the application file is moved or copied to another location on the endpoint user's computer. After initial trusted sources have been created, you can enable collection of events for unhandled applications. Using the comprehensive EPM database, the events captured in the inbox have calculated application reputations and source history, including the full family tree with the parent and child processes, to help assist in their handling. EPM flexibility is reflected in the use of the Restrict Access option, which offers the optimal balance between refraining from interrupting users (the Monitor option) and blocking unauthorized applications automatically (the Default Deny option). In addition, EPM application control, based on its comprehensive database, provides the Application Catalog. The Application Catalog displays information on all applications installed on all endpoint user computers managed by EPM. Using the Application Catalog, you can quickly discover new applications in the system, regardless of whether the applications generated events or if they are monitored by any EPM policy. Threat protection The EPM Threat Intelligence module can integrate with your VirusTotal account to display results within the Events Management page. For details, see Detect a potential security threat. Share — copy and redistribute the material in any medium or format for any purpose, even commercially. Adapt — remix, transform, and build upon the material for any purpose, even commercially. The licensor cannot revoke these freedoms as long as you follow the license terms. Attribution — You must give appropriate credit , provide a link to the license, and indicate if changes were made . You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use. ShareAlike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original. No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits. You do not have to comply with the license for elements of the material in the public domain or where your use is permitted by an applicable exception or limitation . No warranties are given. The license may not give you all of the permissions necessary for your intended use. For example, other rights such as publicity, privacy, or moral rights may limit how you use the material. Remove local admin rights and enforce role-specific least privilege Protect from the most impactful threats including ransomware and credential theft Challenge privileged users to MFA for high-risk actions Confidently defend against attacks, including ransomware and credential theft. Drive operational efficiencies, secure the digital transformation and align security to your business goals. Create audit trail for identity and privilege on the endpoint and meet audit requirements. Harden administrative workflows, optimize administrators’ experience, and eliminate the manually intensive, error-prone administrative processes that can lead to over provisioning and privilege abuse with this integrated and unified endpoint continuous adaptive authentication and privilege management solution. Efficiently manage privileged account credentials and access rights, proactively monitor and control privileged account activity, intelligently identify suspicious activity, and quickly respond to threats. The solution protects a wide range of IT assets including loosely connected devices that are often off-network, beyond the control of corporate IT and security personnel. Remove local admin rights while improving user experience and optimizing IT operations Enforce least privilege and create scenarios for different user roles, conditions and environments with comprehensive conditional policy-based application control Defend against ransomware with an additional layer of protection centered around data, ideally complementing verdict-based threat analysis tools Skip To Main Content Capabilities Benefits Testimonials Integrations Resources With our interactive product tour, you can experience first-hand how EPM, as part of Endpoint Identity Security strategy, can help your organization secure endpoints and servers, without disrupting productivity. Sign up now to get immediate access to our EPM Interactive Product Tour! Download PDF Expand Fullscreen With over 20 years’ experience in breach remediation and through the deployment of a single agent, a combination of least privilege, privilege defense, credential theft protection, ransomware protection, and application control protection, CyberArk Endpoint Privilege Manager effectively reduces the attack surface and mitigate the risk of a severe data breach in a transparent way to end-users and without impacting productivity. We’ve detected that JavaScript is disabled in this browser. Please enable JavaScript or switch to a supported browser to continue using x.com. You can see a list of supported browsers in our Help Center. Help Center