CYBERARK

FICHA TÉCNICA

CORE PRIVILEGED ACCOUNT SECURITY

Protege, monitorea y controla eficazmente las cuentas privilegiadas a nivel local, en la nube y en las infraestructuras híbridas

Especificaciones

Algoritmos de cifrado:

- AES-256, RSA-2048
- Integración con el módulo de seguridad de hardware (hardware security module, HSM)
- Criptografía validada por la Norma Federal de Procesamiento de la Información (Federal Information Processing Standard, FIPS) 140-2

Alta disponibilidad:

- Soporte en clústeres
- Múltiples sitios de recuperación ante desastres
- Integración con el sistema de respaldo empresarial

Gestión de acceso y flujo de trabajo:

- Protocolo ligero de acceso a directorios (Lightweight Directory Access Protocol, LDAP)
- Gestión de identidad y acceso
- Sistemas de control de billetes y flujo de trabajo

Portal multilingüe:

- Inglés, francés, alemán, español, ruso, japonés, chino (simplificado y tradicional), portugués de Brasil, coreano

Métodos de autenticación:

- Usuario y contraseña, LDAP, autenticación de Windows, RSA SecurID, Web SSO, RADIUS, PKI, SAML, tarjetas inteligentes

Monitoreo:

- Integración de SIEM, capturas de SNMP, notificaciones por correo electrónico

Continúa en la siguiente página...

El desafío

Las cuentas privilegiadas representan la mayor vulnerabilidad, en términos de seguridad, que enfrentan hoy en día las organizaciones. Estas cuentas poderosas existen en cada rincón del hardware y software de una red. Si se emplean correctamente, las cuentas privilegiadas se utilizan para realizar mantenimiento a los sistemas, facilitar los procesos automatizados, proteger la información sensible y asegurar la continuidad de los negocios. No obstante, si caen en las manos equivocadas, estas cuentas pueden utilizarse para robar datos confidenciales y provocar un daño irreparable para la empresa.

En prácticamente todos los ataques cibernéticos se vulnera la seguridad de las cuentas privilegiadas. Los delincuentes pueden utilizar las cuentas privilegiadas para deshabilitar los sistemas de seguridad, tomar el control de la infraestructura fundamental de Tecnología de la Información (TI) y obtener acceso a datos comerciales e información personal de carácter confidencial.

Las organizaciones enfrentan numerosos desafíos para proteger, controlar y monitorear las cuentas privilegiadas; entre ellos, se incluyen los siguientes:

- **Manejo de credenciales de las cuentas.** Muchas organizaciones de TI dependen de procesos administrativos manuales intensivos propensos a derivar en errores para rotar y actualizar las credenciales de las cuentas privilegiadas: un enfoque ineficiente, riesgoso y costoso.
- **Seguimiento de la actividad de las cuentas privilegiadas.** Muchas empresas no pueden monitorear y controlar de manera centralizada las sesiones de las cuentas privilegiadas, lo que las expone a amenazas de seguridad y violaciones de cumplimiento.
- **Monitoreo y análisis de amenazas.** Muchas organizaciones carecen de herramientas de análisis integral de amenazas y no pueden identificar proactivamente las actividades sospechosas y remediar los incidentes de seguridad.
- **Control de acceso de superusuarios.** Las organizaciones suelen tener dificultades para controlar y auditar eficazmente el acceso de superusuarios a sistemas empresariales críticos, lo que genera riesgos de cumplimiento y complejidades operativas.
- **Protección de controladores de dominio de Windows.** Los atacantes pueden aprovechar las vulnerabilidades de seguridad del protocolo de autenticación de Kerberos para hacerse pasar por usuarios autorizados y obtener acceso a recursos y datos confidenciales críticos de TI.

La solución

La Solución CyberArk Core Privileged Account Security es la solución más completa de la industria para proteger, controlar y monitorear las cuentas privilegiadas a nivel local, en la nube y en las infraestructuras híbridas. Diseñada desde cero para fines de seguridad, la solución de CyberArk ayuda a las organizaciones a manejar eficazmente las credenciales de las cuentas privilegiadas y los derechos de acceso, monitorear y controlar proactivamente la actividad de las cuentas privilegiadas, identificar de manera inteligente la actividad sospechosa y responder rápido a las amenazas.

- **Acceso seguro y controlado de manera centralizada a las credenciales privilegiadas en función de las políticas de seguridad definidas a nivel administrativo.** La rotación automatizada de las contraseñas y las claves SSH de las cuentas privilegiadas elimina las tareas administrativas manuales intensivas, extensas y propensas a derivar en errores, y protege las credenciales que se utilizan a nivel local, en las infraestructuras híbridas y en la nube.

Especificaciones

Modelo de dispositivos administrados compatibles:

- Sistemas operativos, virtualización y contenedores: Windows, *NIX, IBM iSeries, Z/OS, OVMS, ESX/ESXi, XenServers, HP Tandem*, MAC OSX*, Docker
- Aplicaciones de Windows: Cuentas de servicio, que incluyen cuentas de servicio de servidor SQL en clúster, tareas programadas, agrupaciones de aplicaciones de IIS, COM+, acceso anónimo en IIS, servicio de clúster
- Bases de datos: Oracle, MSSQL, DB2, Informix, Sybase, MySQL y cualquier base de datos que cumpla con el estándar ODBC
- Aplicaciones de seguridad: CheckPoint, Cisco, IBM, RSA Authentication Manager, Juniper, Blue Coat*, TippingPoint*, SourceFire*, Fortinet*, WatchGuard*, Industrial Defender*, Acme Packet*, Critical Path*, Symantec*, Palo Alto*
- Dispositivos de red: Cisco, Juniper*, Nortel*, HP*, 3com*, F5*, Nokia*, Alcatel*, Quintum*, Brocade*, Voltaire*, RuggedCom*, Avaya*, BlueCoat*, Radware*, Yamaha* McAfee NSM*
- Aplicaciones: CyberArk, SAP, WebSphere, WebLogic, JBOSS, Tomcat, Cisco, Oracle ERP*, Peoplesoft*, TIBCO*
- Directorios: Microsoft, Oracle Sun, Novell, proveedores de UNIX, CA
- Control remoto y monitoreo: IBM, HP iLO, Sun, Dell DRAC, Digi*, Cyclades*, Fijitsu* y ESX
- Archivos de configuración (sin formato, INI, XML)
- Entornos de la nube pública: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP)

*Es posible que este complemento requiera adaptaciones o pruebas de aceptación en el lugar. Si desea obtener más información, consulte al ingeniero de Ventas de CyberArk.

- **Aislamiento y protección de las sesiones de usuarios privilegiados, y protección de los sistemas objetivo contra los malware en los endpoints.** Las funciones de monitoreo y registro les permiten a los equipos de seguridad ver las sesiones privilegiadas en tiempo real, suspender automáticamente y finalizar de manera remota las sesiones sospechosas, y mantener una traza de auditoría integral apta para realizar búsquedas de la actividad del usuario privilegiado.
- **Detección, generación de alerta y capacidad de respuesta frente a la actividad anómala privilegiada.** La solución recopila datos de múltiples fuentes y aplica una combinación compleja de algoritmos estadísticos y deterministas para identificar la actividad maliciosa en las cuentas privilegiadas.
- **Control del acceso con menos privilegios para *NIX y Windows.** La solución permite que los usuarios privilegiados ejecuten comandos administrativos autorizados desde sus sesiones nativas de Unix o Linux y, a la vez, elimina los privilegios de raíz que no se necesitan. También permite que las organizaciones bloqueen y contengan los ataques en los servidores de Windows, a fin de reducir el riesgo de que se robe o cifre información y que se pida un rescate por ella.
- **Protección de los controladores de dominio de Windows.** La solución ejecuta un control de la aplicación y con menos privilegios en los controladores de demonio y permite detectar el ataque en progreso. Protege contra la imitación y el acceso no autorizado, y ayuda a proteger contra diversas técnicas de ataque de Kerberos frecuentes; entre ellas, la manipulación de Golden Tickets, Overpass-the-Hash y del certificado de atributos de privilegios (Privilege Attribute Certificate, PAC).

Beneficios

- **Reducción de los riesgos de seguridad.** Fortalece la seguridad de las cuentas privilegiadas. Protege el acceso a las contraseñas y las clave SSH de las cuentas privilegiadas. Protege al sistema contra los malware y los ataques. Detecta y responde eficazmente a la actividad sospechosa y las acciones maliciosas. Protege contra el acceso no autorizado a las cuentas privilegiadas, y contra su imitación, fraude y robo.
- **Reducción de las operaciones costosas y complejas.** Elimina los procesos administrativos manuales intensos, extensos y propensos a derivar en errores. Simplifica las operaciones y mejora la eficiencia de los equipos de seguridad de TI. Libera al valioso personal de TI para que se centre en las tareas estratégicas, a fin de brindar soporte para las actividades comerciales centrales.
- **Mejora del cumplimiento reglamentario.** Establece controles de acceso a las cuentas privilegiadas basados en las políticas para asegurar el cumplimiento con las reglamentaciones del gobierno y la industria. Muestra con facilidad las políticas y los procesos a los auditores. Genera trazas de auditoría e historiales de acceso detallados para poner de manifiesto el cumplimiento.
- **Se acelera el tiempo que transcurre hasta la obtención de valor.** Protege y amplía las inversiones anteriores. Aprovecha las integraciones listas para usar con una amplia variedad de operaciones y sistemas de seguridad de TI, entre ellos, sistemas de autenticación, soluciones de control de billetes, plataformas de administración y acceso de identidad y soluciones del Sistema de gestión de eventos e información de seguridad (security information and event management, SIEM).
- **Mejora de la visibilidad.** Conoce las cuentas privilegiadas que existen y quién tiene acceso a ellas. Establece políticas de seguridad de cuentas privilegiadas bien informadas. Monitorea la actividad histórica y en tiempo real de las cuentas privilegiadas.