CYBERARK®

CyberArk 特权账号安全解决方案

一个完整的解决方案，以保护、 监测、 检测、 警报和响应特权帐户活动

目 录

特权账户 — 一个真实的无处不在的威胁

恶意黑客肆虐全球，凭借计划周密、 复杂和直接针对企业最有价值核心资产的高级网络攻击。局外人突破周边，获得内部访问。一旦进入网络内部，他们即开始寻求访问企业核心，意图造成昂贵的损害，包括名誉受损、 财务损失和被盗的知识产权。

那些已经在组织内部的人员，对公众泄露敏感信息，或种植使内部损伤的种子，也出现了。在 100%的这些最近违规事件中[1]，被盗、 被滥用或误用的特权凭据是罪魁祸首。

特权帐户代表组织今天面临的最大安全漏洞。为什么企业内部和外部的攻击者要瞄准特权帐户?

- 特权帐户到处都是，在每个网络设备、 数据库、 应用程序、 服务器和社交媒体账户上–在驻地网，云和工业控制系统中
- 特权帐户有全能访问机密数据和系统
- 特权帐户有共享管理访问权限，使其用户匿名
- 特权帐户授予太广泛的访问权限，远远超出用户执行其工作职能所需的,
- 特权帐户未受监控和未经报告，因此没有安全保障

简单地说，特权帐户允许任何一个拥有他们的人控制组织资源、 禁用安全系统，以及访问大量的敏感数据。所有的预测都指向特权帐户滥用将来会恶化，除非组织现在就采取行动。最佳做法要求特权帐户应纳入企业组织的核心安全战略。特权帐户的安全问题和组织需要制定好全面的控制措施保护、 监测、 检测、 警报和响应所有的特权帐户活动。

特权账户凭证 – IT 王国的钥匙

特权的帐户凭据是 IT 王国的钥匙。需要他们解锁所有特权帐户，他们被外部攻击者和恶意的业内人士寻找，就是可以直接访问企业的心脏。因此，组织的关键系统和敏感数据就如访问这些资产所需的特权凭据一样安全。

大多数组织今天依靠密码和 SSH 密钥，对用户和系统的特权帐户进行身份验证。当不安全时，攻击者可以破坏这些宝贵的凭据以获得拥有特权的帐户，并利用它们来促进对组织的攻击。事实上，网络安全研究表明每个攻击者需要成功的一件事是对特权帐户的访问。值得注意的是，一些组织已经开始保护特权密码，攻击者已把他们攻击方法转向 SSH 密钥，组织在保护特权帐户时往往忽视他们。事实上，在 2013 年超过一半由 Ponemon 研究所调查的企业承认受到 SSH 相关的损害。

要防止有针对性的攻击，保护 IT 王国的钥匙和保持敏感数据对攻击者的隔离，组织必须采取一种特权帐户安全策略，包括对所有特权凭据，包括密码和 SSH 密钥的主动保护和监督。

1 2013 CyberSheath Report, APT Privileged Account Exploitation

向专家学习： CyberArk 特权账户安全

CyberArk 是特权帐户安全方面受信任的专家。我们对特权帐户安全比任何其他供应商有更多的经验，我们把这种专门知识为我们的客户工作，用一个明确而有效的方法来管理与特权帐户相关的风险。

为了减轻严重的违规风险，企业需要采用专门针对特权帐户风险敞口的安全解决方案。CyberArk 的特权帐户安全解决方案提供了全面的防护、 监测、 检测、 警报和报告，是强制性的要求，以阻止恶意的内部人员和高级攻击者。

您是否低估了风险级别?

在最近公布的 2013 年 CyberArk 特权帐户安全与法规遵从性调查报告，我们发现 86%的大企业不知道，或者是大大低估了，他们特权帐户安全问题的严重性。这些组织中 30%的受访者认为他们有 1-250 个 特权帐户。然而，一个拥有 5000 名员工的组织，特权帐户的数量估计要至少高出五到十倍。调查还发现超过三分之一的受访者不知道他们的组织在哪里可以找到特权帐户。
此外，随着高级威胁的风险增加，像 PCI DSS、萨班斯奥克斯利法案、NIST、NERC CIP、 HIPAA 和更多的法规，增加其对控制、 管理和监视特权帐户访问的要求。不能完全理解他们特权帐户环境的组织，面临审计失败的前景，导致剧增的罚款和刑罚，并使他们自己易受严重违规的影响。

你的特权账号用户是谁?

企业往往忽视庞大的特权帐户访问阵列。设置很少的，如果有的话，安全或审计策略来控制与他们相关的风险。对这些帐户的匿名、未经检查的访问，让企业公开滥用，如果被攻破可能会严重削弱组织。

第三方供应商。特权访问授予执行作业功能，容许承建商在匿名的名义下工作。一旦进入内部，第三方承包商在整个组织内不受限制地访问，以提升权限来访问敏感数据。

虚拟机监控程序或云服务器管理员。业务流程，如财务、 HR、 和采购，移动到云端应用，使企业资产暴露于高风险，来自于云系统管理员授予的广泛访问权限

系统管理员。在 IT 环境中的几乎每个设备，都有一个共享的特权帐户，可以提升特权和不受限制地访问其操作系统、 网络、 服务器和数据库。

应用和数据库管理员。应用程序和数据库管理员被授予广泛的访问权限以管理分配到的系统。这种访问还允许他们连接到在企业中找到的几乎任何其他数据库或应用程序.

某些业务人员。高层管理人员和 IT 人员经常有特权进入到保存敏感数据的业务应用程序。在错误的人的手里，这些凭据提供对企业的财务数据、 知识产权和其他敏感数据的访问。

社交媒体。授予特权访问权限给管理员，来管理公司内部和外部的社交网络。员工和承包商被授予访问权限写入这些社交媒体账户。误用这些凭据可导致公共接管，引起组织品牌或行政声誉的损害。.

应用程序。应用程序本身使用特权帐户来与其他应用程序、 脚本、 数据库、 web 服务和更多的实体通讯。这些帐户经常被忽略，并带来重大的风险，因为他们的凭据往往是硬编码和静态的。黑客可以利用这些攻击点提升特权访问整个组织

策略优先：校准风险管理与业务目标一致

最佳实践要求组织创建、 实施和强制执行特权帐户安全策略，以减少严重的违规风险。有效的企业安全和法规遵从性从很好地执行业务策略开始。政策优先的方法可以确保暴露于外部威胁、 内部威胁和滥用是减少的，严格的政府和行业法规得到满足。，

CyberArk 共享技术平台

从最底层开始特权帐户安全设计，CyberArk 以我们的核心产品构建了强大的底层基础架构，为驻地网、 云计算和工业控制系统（ICS）环境提供了最全面的解决方案。

在基础设施的核心是孤立的保险库服务器、 一个统一的策略引擎，一个发现引擎和安全层，为特权帐户提供可扩展性、 可靠性和无与伦比的安全性。

CyberArk 产品保护、 管理和审核用户和应用程序的凭据，提供最小访问权限、控制端点和服务器上的应用程序，确保、 监视和分析所有的特权活动–实时提醒异常行为。这个保护、 监测、 检测和响应的完整的企业级解决方案，可以防篡改、 可扩展，为复杂的分布式环境构建，从内部和高级威胁中提供最大的安全。

主策略 ™—简化、统一，以及无与伦比地制定优先政策

主策略是创新策略引擎，使客户能够在一个单一、简单，自然语言接口的界面设置、 管理和监测特权帐户安全策略。一度很复杂的业务政策转换过程和程序技术设置过程，现在易于管理，并为组织的利益相关者包括安全、 风险和审计团队所理解。主策略嵌入在核心，其能力跨越所有的 CyberArk 特权帐户安全产品，提供简化的、 统一的和无与伦比的政策管理。

主策略将书面的安全策略映射到技术设置，以自然语言管理这项政策。现在可以在短短几分钟内执行特权帐户安全控件，没有主策略时可能需要几天甚至几周时间，此过程提高了门槛。主策略可以在设置企业全球政策时确保快速执行和灵活性，同时提供可控的、 细粒度级别的例外处理，以满足操作体系、 地区、 部门或业务线的独特的业务需求。

数字保险库 ™

屡获殊荣的专利 Digital Vault™（数字保险库）是孤立和堡垒硬化服务器，以 FIPS 140-2 加密，只响应保险库协议。为确保完整性，所有 CyberArk 产品直接与保险库交互、共享数据，以使所有的产品模块和组件得以安全地进行通信，安全存储密码、 SSH 密钥、 策略设置和审核日志（防止他们被篡改）并从中受益。没有单点故障。

- **职责分离和强大的访问控制。**保险库管理员没有访问存储在保险库中凭据的权限，确保适当的职责分离。该解决方案支持多个身份验证方法，以确保安全和控制所有的特权凭据访问和活动。
- **安全层次。**内置的七层安全机制，用于身份验证、 访问控制、 加密、 防篡改存储和数据保护，没有后门或 DBA 访问通道为特权帐户提供了前所未有的安全
- **高可用性和灾难恢复。**基础设施专为高可用性而设计，具有内置的故障安全措施，以满足并超越灾难恢复要求，包括安全备份和简单恢复。

发现引擎

旨在不断发现到您的 IT 环境变化，发现引擎启动不断的最新保护，并确保所有特权帐户活动被解释和安全。随着新的服务器和工作站被添加或删除，自动发现特权帐户的更改。

企业级集成

CyberArk 特权账户安全解决方案可立即利用现有投资，从而实现众多设备、网络、服务器和应用程序，包括网站和社交媒体的开箱即用支持。

- **SIEM.** 与 SIEM 供应商全双向集成改进了威胁检测和报警功能。CyberArk 为 SIEM 解决方案供给特权凭据访问和操作事件，以及通过特权会话监视捕捉到的命令级活动。
- **混合云。**混合云环境的支持确保为云管理员，AWS，SaaS 应用程序和 Twitter、 Facebook 和 LinkedIn 等社交媒体账户，发现和保护虚拟机监控程序和客户镜像账号。
- **漏洞管理器。**与领先的安全漏洞管理供应商的充分集成，使他们能够简化"验证扫描"（也称为"深扫描"），每当他们需要登录到目标服务器来执行扫描时可以从保险库中取得特权帐户。
- **身份管理。**与领先的身份与访问管理 (IAM) 解决方案集成，基于目录详细信息、 组成员身份或身份治理策略来提供帐户到解决方案中。集成也使我们的客户能够利用以前在强大的身份验证，PKI、 Radius、 web-sso、 LDAP 等方面的投资。
- **帮助台。**与工单系统相集成，如 Remedy,HEAT, HP 服务管理器和内部解决方案。功能包括服务请求验证、 创建新的服务请求，与经理审批（双重控制）和定时可用性等审批工作流集成

可扩展、灵活、低影响的架构

CyberArk 特权帐户安全解决方案的体系结构影响最低，并保护您在当前的 IT 环境中的现有投资。所有的组件独立工作，但利用共享的资源和数据。这个灵活的方法将允许组织可以从部门级别开始一个项目，随着时间的推移扩大规模到一个复杂的、分布式的企业解决方案。

CyberArk 产品

CyberArk 特权帐户安全解决方案中的每一件产品是独立的，可以独立地管理同时仍然从公共基础结构共享资源和数据。

每个产品解决了特权帐户安全不同的要求，所有工作一起为本地网、 云计算和 ICS 环境的操作系统、 终端结点、服务器、数据库、应用程序、虚拟机监控程序、网络设备、安全设备和更多的设备系统提供一个完整、安全的解决方案。

保护你的特权帐户的步骤 ：.

- 首先设置策略
- 发现您所有的特权账号和凭证
- 保护和管理用户和应用使用的特权账号凭证
- 控制、保护和监控对服务器、数据库、Web 站点、SaaS 和任何目标应用的特权访问
- 为业务用户和 IT 管理人员提供最小特权访问
- 控制终端和服务器上的应用
- 使用实时特权账号智能检测和相应进行中的攻击

企业密码保险库™

特权密码的保护、管理和审计

企业密码保险库可以防止恶意使用特权用户密码，并为易受伤害的帐户带来秩序和保护。企业密码保险库基于您的特权帐户安全策略保护特权密码，控制谁、何时可以访问哪些密码。这个自动化的过程减少了手动跟踪和更新特权密码这种耗时和容易出错的任务，轻松满足审计和法规遵从性标准。

- 发现特权帐户和相关服务，提供这些帐户到数字保险库进行管理
- 基于策略控制对特权账号密码的访问
- 提供可自定义工作流，为密码请求，包括双重控制和帮助台工单系统集成
- 具有“单击，连接” 的能力，以免暴露最终用户的密码
- 基于您的要求计划自动密码更改
- 提供一次使用密码的控件
- 与服务台和工单系统集成
- 在持续的基础上验证凭据，不同步时自动恢复和重置密码
- 对可能受到影响的特权帐户接收来自特权威胁分析的警报，自动旋转受影响的密码

SSH 密钥管理器™

SSH 密钥安全、轮转和监控

SSH 密钥管理器可以帮助组织防止到私人 SSH 密钥的未经授权的访问，经常有特权的 Unix/Linux 用户和应用程序用这些 SSH 密钥向特权帐户进行身份验证。SSH 密钥管理器保护和轮转特权 SSH 密钥，基于您的特权帐户安全策略，控制和监控对受保护 SSH 密钥的访问。此解决方案使组织能够控制 SSH 密钥，提供对特权帐户的访问，但经常处于非托管状态。

- 安全存储和控制对数字保险库中特权 SSH 密钥的访问
- 自动轮转 SSH 密钥对，使之符合组织的策略
- 支持和强制使用强访问控制，认证和管理提权请求
- 坚持预设 SSH 密钥的签出和签入的政策
- 使管理员能够跟踪和报告用户和应用程序对 SSH 密钥的使用

特权会话管理器™

安全、控制和实时的会话监控和记录

特权会话管理器保护，控制，并监视特权用户对关键 Unix，Linux，基于 Windows 的系统、 数据库、 虚拟机、网络设备、 大型机、 网站、 SaaS 和更多系统设备的访问和活动。它提供了一个单一访问控制点，防止恶意软件跳转到目标系统中，通过连续监测记录每次击键和鼠标点击。

类似 DVR 的记录提供了全貌的会话情景，具有无需通过日志筛选对敏感事件进行搜索、查找和警报的能力。实时监测确保连续保护特权访问，以及实时的干预可以终止会话，如果任何活动被视为可疑。特权会话管理器还提供与第三方 SIEM 解决方案的充分集成，对不寻常的活动给以警报。

- 建立特权会话的单点控制
- 保护特权密码和 SSH 密钥免受高级攻击技术，例如击键记录和哈希传递攻击
- 保护和控制特权会话，防止恶意软件或零日漏洞绕过控件
- 扩展了特权会话对应用程序客户端、 web 应用程序或带自定义连接器的网站的监视
- 创建一个索引的、 防篡改的特权会话记录
- 提供命令行控制和本机 SSH 访问，同时仍提供对特权用户使用密码或 SSH 密钥的安全访问
- 为特权会话鉴定分析，导出数据到 SIEM 产品
- 提供 AD 桥功能，使组织能够集中管理通过 CyberArk 平台链接到 AD 的 Unix 用户和帐户

特权威胁分析™

分析和警报恶意的特权的帐户活动

CyberArk 特权威胁分析是一种安全情报解决方案，允许组织检测、警报、响应异常特权活动，表示正在进行攻击。解决方案从多个来源，包括 CyberArk 数字保险库、 SIEM 和网络探针/交换机收集一整套有针对性的数据。然后，解决方案应用统计和确定性算法的复杂组合，通过识别恶意特权帐户活动使组织能够在攻击周期早期检测到损害迹象。

- 实时检测和警报
- 启动自动响应检测到的事件

- 建立了典型的特权用户行为的配置文件
- 标识异常，包括恶意的特权帐户活动和可疑的 Kerberos 流量，指示正在进行的攻击
- 以自学习算法使威胁检测适应不断变化的风险环境
- 关联事件并分配威胁级别
- 开箱即用特性增强了与现有 SIEM 解决方案集成的价值
- 以用户模式和活动的信息数据提高了审计过程

应用身份管理器™

保护、 管理和审计嵌入应用程序的凭据

应用身份管理器消除了硬编码的密码和存储在本地的应用程序和脚本的 SSH 密钥。CyberArk 的应用身份管理器确保可用性和业务连续性等高端企业级需求得到满足，即使在复杂和分布式的网络环境中。本产品消除了嵌入应用程序的凭据，通常无需更改代码和对应用程序性能的零影响。

- 替换硬编码密码和本地存储的 SSH 密钥为脚本，使应用程序可以从数字存储库按需检索这些凭据
- 为实现高可用性并保持高性能，在服务器上提供安全的本地缓存
- 提供即时应用凭据替换而不会增加延迟
- 基于其物理属性如路径或应用程序签名对应用程序请求的凭据进行认证
- 生产系统提供高可用性和可靠性
- 用于管理应用程序服务器上的数据源凭据提供了一个独特的专利的解决方案

Viewfinity

终端和服务器的最小特权和应用控制

Viewfinity 使组织能够执行业务用户和 IT 管理员的最小特权政策，同时需要时无缝地提升其运行授权的应用程序或命令的特权。这有助于减少受攻击面，减少意外或故意损害终端和服务器，隔离在 Windows 服务器上的管理职责。辅助的应用程序控件帮助防止恶意应用程序渗透环境，同时允许未知应用程序运行在安全、有限制的模式。

- 使组织能够从日常业务用户删除管理员权限，而不用停止生产
- 在环境中自动创建超过 90%的应用程序提权和应用控制政策
- 通过控制基于用户角色的管理员特权，隔离在 Windows 服务器上的职责
- 基于策略无缝地提升运行授权的应用程序或命令所需的特权
- 可防止恶意应用程序进入和在整个环境传播
- 允许用户在“受限模式”中运行未知的应用程序，帮助用户保持高效
- 结合 Check Point, FireEye and Palo Alto 等网络威胁检测解决方案，对未知应用程序实现自动分析
- 确定恶意应用程序在环境中的原始来源和所有地点，以加速修复
- 支持三种部署方法，包括服务器、 SaaS 和微软 GPO

按需特权管理器™

Unix 和 Linux 最小特权和应用控制

按需特权管理器允许特权用户从其本机的 Unix/Linux 会话使用管理命令，同时消除不必要的根访问权限或管理员权利。这个安全和为企业准备的类似 sudo 的解决方案，提供了所有超级用户活动的统一和相关的日志记录，将其链接到个人的用户名，同时提供履行工作职能所需的自由。给出了细粒度的访问控制，同时不断监测所有超级用户基于角色和任务运行的管理命令。

- 以集中式的方案替换常用的 sudo 解决方案，提供细粒度权限控制和审核日志的安全存储
- 向担保、 管理和控制的超级用户权限的审计者提供证明
- 提供详细的审核，跟踪哪些个人提升特权到根权限，何时以及原因是什么
- 限制超级用户特权给只有那些必需的，以减少暴露于滥用或错误的风险
- 授权使用完全授权的根壳，让用户根据工作流程直观地工作
- 把一个根帐户和活动链接到个人的用户名
- 在每用户或每个系统的基础上启用白名单/黑名单命令

为什么选择 CyberArk 特权账号安全解决方案?

企业证明、 业界领先的专家

凭借我们屡获殊荣，专利的技术和行之有效的专业技能，CyberArk 是唯一一家能够提供充分保护的公司，从高级和内部威胁以减轻您的风险，到满足高风险的合规性要求。

CyberArk 比任何其他供应商有更多的在大规模的分布式虚拟环境中部署的案例，解决了更多特权帐户安全挑战。我们可以在本地网、 云计算和 ICS 环境中支持绝大多数的设备。CyberArk 是唯一一个纯粹的解决方案供应商，可以提供充分的凭据保护、 会话安全，最小特权和应用程序控制，以及连续的监测，以迅速察觉威胁和报告特权帐户活动。

现在就开始评估您的特权账户风险

CyberArk DNA™ （发现和审计）是一个免费的评估工具，将帮助您在整个企业中发现您的特权帐户在哪里。明确了解了所有您的用户帐户、 SSH 密钥、 服务帐户、 设备和应用程序，我们可以帮助您实现对特权帐户安全风险的大小和程度的理解。此工具将协助建立您的业务案例，或规划一个特权帐户安全项目，帮助你决定最弱处在哪里和如何优先安排项目。

虽然一些组织选择跨企业部署整个战略的解决方案，但 CyberArk 解决方案的灵活性与强大也可以使您可以从最弱的地方开始特权帐户安全项目。一些组织将通过保护特权凭据开始，然后移动到监测，这时他们的优先事项已经转移。因为基础设施已经到位，很容易添加额外的组件来增加你对特权帐户的保护。最终整个解决方案将为你的组织和你的组织的安全性提供安心保护，防止内部人和高级威胁。

关于 CyberArk

CyberArk 是唯一安全公司，专注于打击针对性的网络威胁;那些冲进内部来攻击企业心脏的家伙。CyberArk 致力于在他们停止业务之前阻止攻击，得到了世界上领先的组织的信任，来保护他们最高价值的信息资产、基础设施和应用程序。 为 CyberArk 十多年了，导致市场在确保企业应对网络攻击，采取后面内幕特权盖和攻击关键的企业资产。

在确保企业应对隐藏在内部特权后面以攻击关键企业资产的网络攻击市场方面，CyberArk 已处于领先位置十多年了。今天，只有 CyberArk 交付一种新的有针对性的安全解决方案，以帮助领导人改变只能对网络威胁作出被动反应的境地，而是赶在他们前面，在不可弥补的业务危害之前，防止攻击升级。当审计和监管者都认识到特权帐户是网络攻击的捷径和要求更强的保护时，CyberArk 的安全解决方案掌握了高风险合规和审计要求，以保护企业最重要的业务。

更多信息，请访问 www.cyberark.com。

CyberArk 和 CyberArk 的标志是 CyberArk 软件在美国和其他国家的注册的商标。© 版权所有 2016 CyberArk 软件。保留所有权利。在美国，3.16 出版。

CyberArk 认为此文档中的信息在发布日期时是准确的。此信息提供，不带任何明示、法定的或暗示的保证，如有更改，恕不另行通知。

本文档包含的信息和思想，它们都是 CyberArk 软件有限公司专有的。

未经 CyberArk 软件有限公司的事先书面许可，本出版物的任何部分不可以被转载、存储于检索系统或以任何形式或通过任何手段传输，电子、 机械、 影印、 录制、 扫描或其他方法。

Copyright© 2000-2014 by CyberArk Software Ltd. All rights reserved.