Realtime publishers

The Essentials Series: Managing Access to Privileged Accounts

Privileged Session Controls

sponsored by

by Ed Tittel

Copyright Statement

Privileged Session Controls

The problem with providing access to key resources through privileged accounts is that clients, consultants, and vendors are essentially handed the keys to the kingdom. A common security protocol is the principle of least privilege, which dictates that consultants, developers, and vendors should be given only sufficient access to get the job done. Providing limited, task-specific access to these key resources, systems, and information is crucial to preserving the protected environment.

Providing Access: Key Resources, Systems, and Information

Areas most often supported by remote vendors include application management, desktop management, system management, platform development, and system security. Accordingly, privileged session control necessitates new and often entirely different requirements than traditionally exercised over internal employees. The enterprise landscape is comprised of multiple tiers of application and server platforms operating at various levels of infrastructure, each requiring individual security constraints and posing separate remote access challenges.

Compliance and Audit Requirements

Additional laws and federal regulations impact organizations differently. In fact, even the implementation of overlapping compliance coverage differs greatly among similar organizations. This creates an entirely new set of challenges and compromises.

For an enterprise operating in compliance with the Gramm-Leach-Bliley Act (GLBA), there's no reliable means of ascertaining whether a vendor has taken full precautionary measures to avoid violating customer privacy while rendering contractual services. Likewise, a company complying with the Health Insurance Portability and Accountability Act (HIPAA) cannot ensure that consultants haven't compromised or exposed patient data—as has happened in the recent past with security contractors retaining patient records only to have them stolen offsite. Companies can only be assured of their own compliance or negligence under such conditions, while outside sources may not be held to the same standard or governed by the same processes.

Types of Privileged Sessions

An increasing interest in outsourcing gives rise to privileged session access, which only further complicates the privileged session scenario. In an ongoing effort to maximize uptime and reduce cost of ownership, more enterprises are permitting IT equipment vendors and service providers to access network and networked systems to diagnose and resolve issues remotely. Clients, consultants, and remote vendors are also becoming increasingly involved with company IT operations where cost-cutting efforts result in outsourcing responsibility for administrating, maintaining, and repairing on-site applications and equipment.

Granting, managing, and controlling access among these expanding external groups further challenges IT administrators within the company. Remote vendors staff personnel that are beyond the scope of review by company insiders, which creates difficult issues for maintaining accountability—particularly with any shift in the remote vendor's staff or user base. Administrator accounts are universally present, but network devices and security appliances often utilize a single administrator account without support for creation of sub-accounts. UNIX systems and Windows domain controllers are fully supportive of non-administrative account creation, though few restrictions apply to lower-priority administrative roles.

Vendors

An enterprise cannot expect to dictate the rules of engagement for a remote vendor operating entirely out of their own interests in accordance with their own guidelines. This is problematic for the home team environment particularly where compliance requirements, product implementations, and security specifications clash. Furthermore, each vendor is likely governed by entirely separate site-specific security requirements and governmental regulations originating within an entirely different country.

Consultants

Hiring consultants to perform on-site or remote services is equally challenging within a protected enterprise environment. Consultants aren't bound to the same regulatory and compliance practices as the enterprise environments they work within, even if there's a contractual obligation to retain privacy and maintain certain ethical standards. Companies and consultants are bound to entirely separate codes of conduct and modes of operation even where there is significant overlap in protocol or procedure.

Remote Employees

Even when employees work remotely, especially those who must operate in privileged sessions or make use of privileged accounts, many of the same concerns that apply to outsiders also apply to them. Although employees can be held accountable to codes of conduct and expected to comply with security policy and best practices, their remote sessions need extra levels of protection, inspection, and control.

Remote Administration

Current approaches to remote administration are incomprehensive and incomplete. In a "jump box" scenario, vendors have access to a few defined machines from which they launch their sessions. Although this scenario creates a defined point of entry capable of monitoring keystrokes and providing session replay, it works only in limited situations (such as command-line activities). VPNs enforced by access control lists (ACLs) also permit limited connectivity to select systems with defined access but provide no replay and still creates administrative burden.

Enterprises need granular authorization for administrative connections permitting strong authentication at every entry point into the protected environment. Remote administration should operate under a segmentation strategy with secure connections to ensure privacy. Proxy deployment interrupts direct system-level connections to prevent creating a bridge for remote vendor malware from creeping into the protected environment.

Internal Access to Sensitive Systems

Application-to-application (A2A) or application-to-service (A2S) interactions often call upon elevated privileges to perform tasks involving sensitive data or processes. Without proper user account management, these interactions too often involve storage of credentials in configuration files or registry entries in plain text where anyone with elevated privileges can access such information. In particular, the following types of data demand more probative and careful treatment:

- *Human Resources (HR) data*: HR information is also protected under compliance requirements that dictate secure handling and processing of confidential data. This encompasses both financial data and health records but includes other sensitive information. Administrators must keep track of who goes where and what authorized parties are allowed to access and change.
- *Credit card information*: The Payment Card Industry (PCI) Data Security Standard (DSS) is a non-governmental mandate defining the requirements for handling and processing credit card data. Non-compliance with terms and conditions of PCI's DSS results in contractual penalties and revocation of the right to process credit transactions. Protecting against the prying eyes of internal employees is not enough—external clients, visiting consultants, and telecommuting vendors must also be considered.
- *Developer access to production systems*: Both internal and external developers often require access to production systems to pilot and implement new features or enhanced functionality—this is an unavoidable fact of the IT environment and product life cycles. Granting access to production systems in either case should be treated with equal amounts of discretion, even though the conditions and mechanisms for that access will vary conditionally with each case.

Privileged Session Characteristics and Requirements

Managing privileged user accounts for remote vendor access involves entirely separate concerns and conditions than with typical remote employee access. Managing and monitoring access to sensitive systems must still be centralized, policy-driven, and automated, but the underlying characteristics and governing requirements are entirely different.

Inability to Enforce Security Policy Requirements

When it comes to dealing with remote sessions, privileged or otherwise, it's often difficult if not impossible to enforce security policy requirements for firewalling, antivirus, and other anti-malware controls, platforms, applications, and so forth. Thus, when it comes to creating a cooperative environment among diverse and regionally dispersed systems and users, it's improbable to expect uniformity among operating protocols and platforms. Different organizations address system and network concerns differently, using dissimilar operating systems (OSs), network protocols, and security paradigms.

With this collaboration among consultants and vendors comes a distinct inability to enforce compatible and consistent firewall and antivirus applications. Unfortunately, this simple disparity can present a significant stepping stone for an attacker—whether automated or manual, man or man-made—to gain foothold into one or the other organizations. Where one company enforces timely updates for signature databases, firewall rules, and application updates, another may be lax or lenient; this can cause significant problems for a well-protected environment.

Inability to Enforce Remote Access Methods and Controls

Also accompanying a difference in operating platforms, protocols, and procedures is a distinct inability to enforce compliance among VPN and remote access software. Clients, consultants, and vendors utilize individually or organizationally defined products to achieve remote access with partner companies, and this includes likely non-compliance with firewall policies as well. Furthermore, dial-up connections and VPNs introduce security vulnerability and inherently lack sufficient auditing capabilities, making it virtually impossible to track external access and maintain consistent data center security.

A likely scenario is that a participating partner uses different VPN software or an incompatible communications protocol. VPN connectivity is neither consistent nor universal, which poses real problems for ground-level IT workers whose job it is to make connectivity work. Many protected environments do away with modem connections entirely for improved security, but not all organizations are inclined to make such sacrifices and continue to utilize this most insecure communications medium.

Span of Control and Access Control Issues

The span of control issues scales in size with the remote vendor and whatever complexities it brings to the table. First and foremost, remote vendor staff operates well beyond company control. On-site staff often has no idea who they're working with remotely and even a simple change in remote vendor staff creates significant accountability issues. Trust within protected environments is a fragile thing.

As an organization expands in scale and scope, the number of administrators accessing sensitive data and systems grows as well. Organizations encounter growing pains with the realization that old standby methods of account management—sealed envelopes, sticky notes, spreadsheets, and so on—are insufficient and incompatible with modern auditing requirements. Yet the need to continue granting access to protected systems remains constant, with access now reaching an external scope of outside help. This calls for more highly granular access controls, along with comprehensive controls over remote access (who gets in) and privileged session activity (who may touch which resources, and what actions they may perform).

A Solution for Remote Privileged Sessions

Numerous characteristics must be present for remote privileged sessions to be properly handled. We review the key characteristics in a workable solution for managing remote privileged sessions in the list items that follow:

- *Clientless agentless implementation*: This kind of solution enables remote vendors, consultants, and employees to utilize any tools and platforms they like for network and system access, with no strict need to enforce requirements on connecting clients. Clientless application-based solutions (often written in Java) ensure better controls and proper auditing features, while the proxy architectures minimize the chances that remote malware might spread to local host platforms inside the Internet boundary.
- *Activity logging mechanisms*: Activity logging captures all mouse and keyboard activity, permits simple replay, and supports compact session recording to maintain compliance with governmental laws and federal regulatory practices. An added benefit of keystroke recording and playback is that capturing entire sessions can span applications, platforms, and network equipment.
- *Logical separation stymies malware*: Proxying connections end-to-end between company and remote systems creates a logical separation and creates no system-level connections to company hosts. Thus, there is a firewalling effect present that gives malware no chance to migrate from a remote system to any local system. By using secure HTTP (such as HTTPS) and secure shell (SSH) protocols, remote users have no opportunities to employ NetBIOS or other insecure protocols and services.
- *Strong reliable authentication for remote sessions*: Multi-factor authentication, including tokens and smart devices, strengthens authentication and limits access exclusively to authorized parties. Opting for biometric access controls facilitates accountability particularly for remote partners, service providers, and other third parties to whom companies must extend a certain degree of trust.

- *High availability sustains service levels and fosters reliable session security*: High-availability permits uninterrupted access without frequent or significant company IT activity or intervention. Once privileged sessions are initiated, management systems must remain available to avoid negatively impacting the IT infrastructure where service levels aren't adequately maintained. It may involve dynamic DNS, load balancers, and round-robin strategies to maintain service levels.
- *Hardened intermediate appliances deter attack and unwanted access*: The use of hardened network appliances as delivery vehicles protects privileged session management from various forms of attack and compromise. Following the principle of least privilege, even where a vendor may access a device directly, proxy servers and services can ensure that vendor staff members never obtain access to a device password.
- *Specialized APIs support developer access*: Special application programming interfaces (APIs) and command-line interface (CLI) capabilities also facilitate compliant interaction for privileged sessions. Many privileged account management vendors use specialized APIs for provisioning users into an account management system that involves no development effort. In other situations, developers can access production systems under strict control and supervision that only lets them touch components and information relevant to their software, without enabling carte blanche access to its entire contents and capabilities.

Summary

Privileged sessions and the accounts they use continue to demand close scrutiny and tight control throughout the enterprise, primarily because they can bypass ordinary IT user access and management controls. Privileged sessions are only as strong as the weakest link in a long security chain. Privileged accounts should be handled with discretion, but even that is not enough to prevent authorized users from making unauthorized changes to system configurations or operational parameters. That's why account tracking, tight access controls, and activity logging are so important to delivering workable solutions that comply with security policy and regulatory requirements.