Whitepaper

Managing your IT service providers

WALLIX
Infrastructure and Security Solutions

Contents

I OPERATIONAL DIFFICULTIES ARISING FROM THE USE OF IT SERVICE PROVIDERS

Companies today must open up their IT systems to an ever-increasing number of external service providers. Primarily to reduce IT costs by leveraging competencies that are not core to the business of the IT department. Secondly to ensure quicker deployment of new solutions and for IS maintenance. Different types of external providers might include, for example:

· business software vendors supporting their own applications
· facilities managers responsible for some or all of the infrastructure and applications
· outsourced technical support, e.g. specialized Oracle support and tuning
· specialized consultants in specific application domains, e.g. CRM or ERP experts

All external service provision has two major short-term drawbacks. Loss of control and, through increased staff turnover, reduced productivity due to access-authorization set-up for new users and the need for these users to (re)learn specific skills. The long-term difficulty is in controlling the costs of outsourcing. IT facilities managers must deal with increased security risks, additional regulatory compliance and more user-access management.

1.1 Security risks

Service providers are indispensable to the smooth running of an IT system, but they are not company employees and therefore represent a potentially sizable risk (threat) for the company (data leakage, destruction of sensitive data, etc.). Without sophisticated audit systems, it can be impossible to identify the cause and individual(s) responsible for security breaches.

Recent studies confirm the risks inherent in the privileged access enjoyed by IT administrators, and that these risks are as high for company employees as for external service providers.

The survey* found that:

- 35% of IT administrators admit they regularly use their administration rights to inappropriately access confidential or sensitive information
- 74% of IT administrators admit they easily circumvent current security measures for protecting confidential and sensitive information
- Sensitive information to which administrators have access includes:

- Customer databases
- Human resources databases
- Merger and takeover plans
- Marketing information
- Redundancy plans

In the event of dismissal, IT administrators said they would take the following information with them:

Type of information	2008	2009
Customer Database	35%	47%
Email Server Admin Account	13%	47%
M & A Plans	7%	47%
Copy of R & D Plans	13%	46%
CEO's Password	11%	46%
Financial Reports	11%	46%
Privileged Password List	31%	42%

** Source: Trust, Security & Passwords Survey Research Brief – survey conducted in 2009 by Cyber-Ark Software, on 400 IT professionals*

It should be noted that the current global financial situation seriously increases the risk of data theft. Using external service providers - for administrating some or all of your IS systems - magnifies these risks due to:

- Very high staff turnover among many service providers. The more administrators that leave, the greater the possibility of the threats listed above.

- It is extremely difficulty for a client company to ascertain the integrity of a service provider's personnel. This risk increases when working in low-wage economies, as the trade value of the company's data increases accordingly.

A company's own IT personnel must be able to log in remotely (whether on-call or simply working at a remote location) with similar user access and connection security issues to those of external service providers.

1.2 Compliance with regulatory requirements

Access to sensitive systems and applications is subject to very strict audit rules. Access must be protected by passwords, which also are subject to similarly strict rules. Accounts must be created by authorized personnel and must be deleted as soon as the user's role changes.

Companies must be able to provide proof that these rules are enforced; this can be very costly in terms of process implementation. Critically, these processes are associated with the identity of the user and their role in the company. But how do you manage a user who has no identity within the company and whose role is defined by a facilities management contract?

External service providers access highly-sensitive privileged accounts. The integration and monitoring of their activities is a complex challenge requiring the implementation of specific roles and processes.

1.3 Implementation and maintenance costs

Implementing a facilities management contract is a long, often arduous process requiring the cooperation of many departments. For example, access to the IT system core necessitates the participation of systems managers, network managers, security managers, and so on.

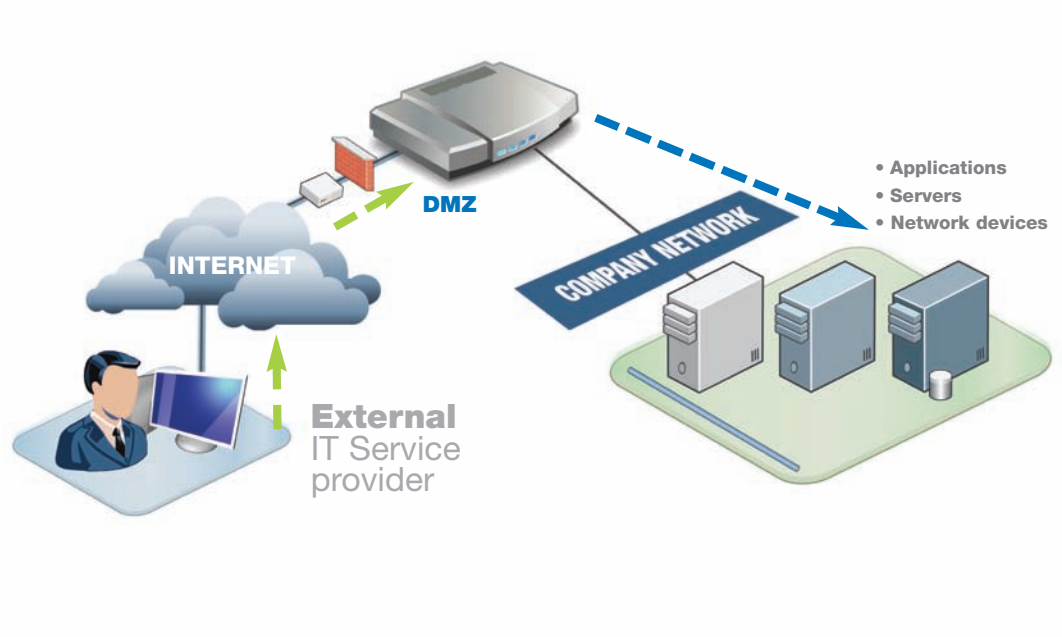
Terminating access at the end of the facilities management contract is usually more complicated to implement, often with the pressures of contract cut-off dates and possible overrun cost penalties. What is more, with nobody relying on its implementation, there is a heightened risk of access remaining open, perhaps indefinitely. IT managers must run regular audits to check that access has indeed been closed, once external service providers have logged out for the final time.

1.4 The issue of shared accounts

Common to the specific issues of compliance, security and maintenance costs, is the problem of shared accounts. For many companies they have become a necessity. Creating individual accounts for people conducting maintenance operations is something of a headache, but the more operators there are using one shared account, the more difficult it is to maintain a password policy, and the more difficult it is to audit access. Companies wishing to outsource their IT maintenance are faced with a difficult choice: create privileged accounts dedicated to their service providers, or compromise the security and compliance of their systems.

2 WHAT ARE THE EXISTING SOLUTIONS?

Various solutions already exist with the objective of providing secure access for external service providers. These include IPSEC or SSL VPN, jump servers and SSH jump servers, leased lines and in-house developments. These solutions are usually installed in a DMZ and placed between the external service provider and the target device. However, these solutions have various disadvantages:



2.1 Limited user-rights management

These solutions generally provide access control at the IP address level, without progressing to the level of the target account. It is therefore not possible, for example, to authorize connection with one or more specific accounts, but only to authorize access to a device and *all its accounts*.

2.2 Multiple solutions require complex administration

For each type of device there is, in general, a distinct solution. For example, UNIX or Linux servers will be accessible via an SSH jump server, Windows servers will be accessed via a Windows TSE server and on-call operatives will log on via an SSL VPN solution.

Each of these solutions is administered in a specific way, with the consequence of high daily administration costs, and an increased risk of granting overly privileged access rights in order to avoid having to modify them later.

2.3 Reporting unsuited to regulatory requirement

As these solutions must provide access for external service providers to critical systems, they should also provide reporting features that enable access compliance to be checked against the appropriate standards. (These include ISO 27001, PCI DSS, SOX, Basel II and HIPPA.)
The majority of these solutions do not supply reporting tools that meet these requirements.

2.4 Disclosure of passwords

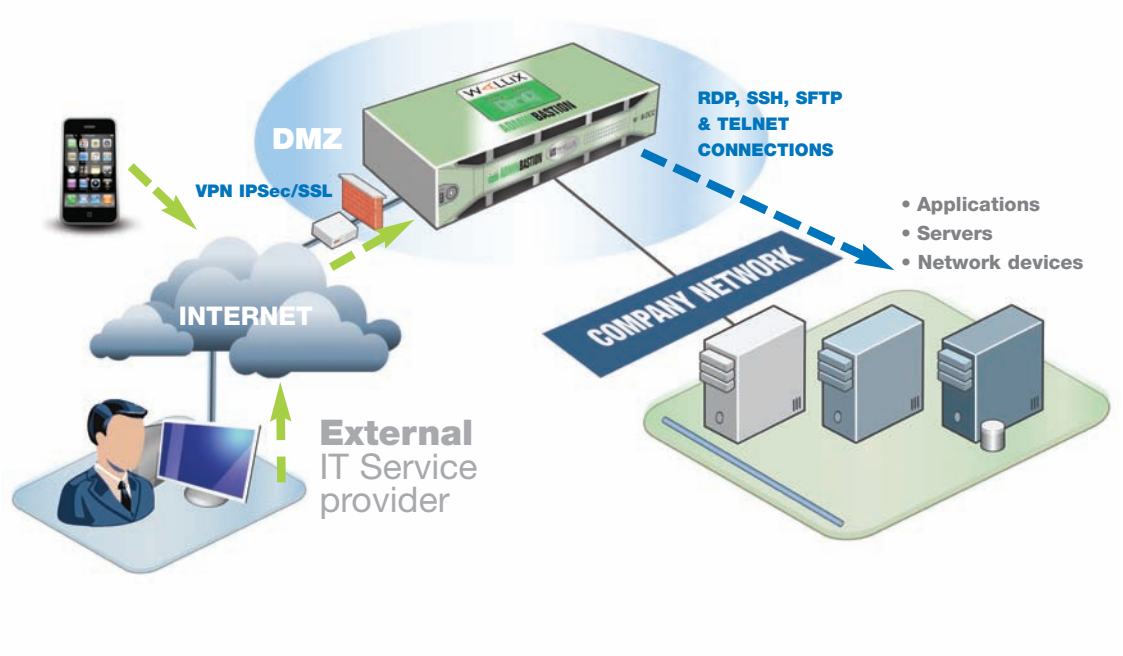
Current solutions require service providers to know the account password used on the target device, meaning that for generic system accounts (e.g. an *administrator* account on a Windows server or a *root* account on a UNIX/Linux server), the password of this account has to be given to the service provider. As passwords for generic system accounts are only rarely modified, this privilege could constitute a major security risk.

2.5 Insufficient traceability

These solutions generally maintain a connection log, but without recording precisely what was done, by whom, during the connection. The client company manager cannot see, for example, if an external provider has tried to access an unauthorized server.

3. THE WALLIX ADMINBASTION (WAB) - THE PLATFORM TO MANAGE EXTERNAL SERVICE PROVIDERS

Wallix has developed the WAB specifically for enterprises needing to implement an administration platform that solves the specific issues encountered with external service providers. It perfectly complements existing SSL or IPSEC VPN solutions and can be used to replace RDP or SSH jump servers.



The WAB offers the following benefits:

3.1 Detailed access-rights management

The WAB defines access rights at target account level not at device level. Therefore, depending on their profile, an external service provider is able to log in to a predefined set of target accounts. It also means that, on the same Windows server, external provider X could be authorized to use the *administrator* account, while service provider Y will only be authorized to use an account with far fewer privileges.

The WAB's user-rights management uses RBAC (Role-Based Access Control).

In addition to access rights, the WAB uniquely enables commands rights to be defined with SSH connections. It is possible, for individual service provider users, depending on the target account, to authorize or to block:

· access to the Shell
· execution of remote commands
· uploading or downloading of files via SCP

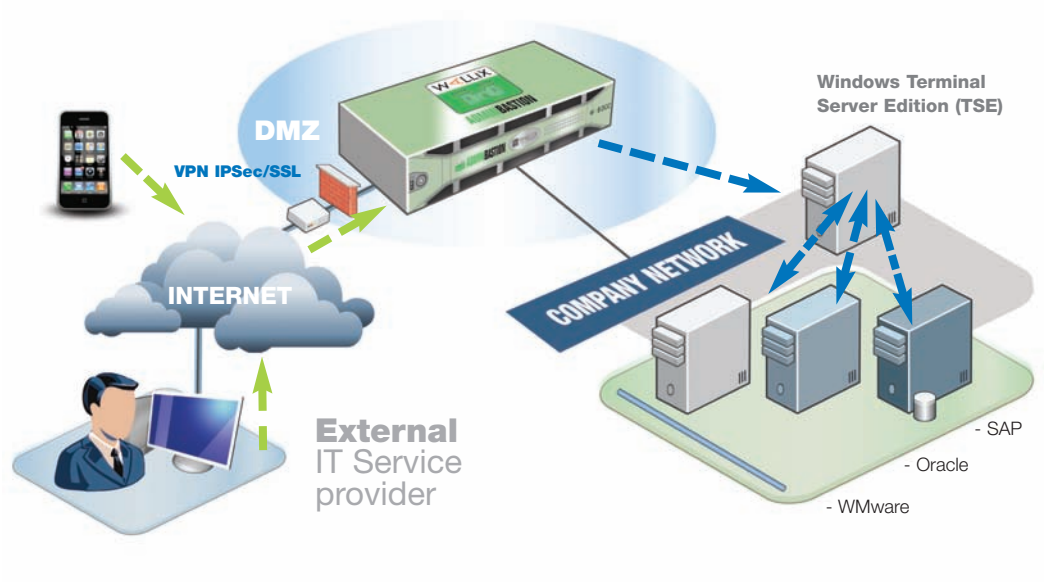
For example, this makes it possible to give the service provider, in charge of server supervision, only the right to send remote commands to specific servers (e.g., reboot command) without the possibility to connect to the Shell or to transfer files.

3.2 Multiple device compatibility

The WAB does not require the installation of an agent on the target devices. Via native support for RDP, SSH, TELNET, SFTP and RLOGIN protocols, it enables the management and recording of connections with the main types of target device, including:

· Windows servers
· UNIX servers (AIX, Solaris, HP-UX)
· Linux servers
· Network devices

In addition, the WAB is able to record connections using other protocols – in particular, specific protocols - via the use of an intermediate RDP server (e.g., Windows Terminal ServerEdition) employed as a jump server upon which the customer software is installed, for the applications that need to be registered (e.g. Oracle, SAP, Notes, VMware).



3.3 Integrated, compliance-ready reports

Via the WAB administration interface it is possible, at any time, to view the connections log *by user* or by *target account*, and also to see *who is logged in to what*. Again in real time, the WAB reports on the access authorizations for and of each user, and the access rights for each target account. For example, the WAB can automatically supply a list of the users authorized to use a specific account on a specific device (e.g., all those who have access to the *root* account of a Linux server).

3.4 Nondisclosure of target-account passwords

The WAB has a centralized authentication module which stores the passwords for target accounts. This means you can enable a service provider to log into a privileged account without sending them the corresponding password.

When an external provider needs access to several target accounts, they need know only the password for their WAB account. This mitigates the risk of password leakage common to other solutions. When necessary, this functionality can be deactivated on an account by account basis. In this situation the service provider would need first to provide authentication on the WAB, and then on the target device.

In the case of shared accounts, whether for the *root* account or any other privileged account, the WAB handles every aspect of security, controlling users' access to these accounts without them ever having to know the passwords. Regularly changing passwords is a simple admin task. Each service provider has a unique WAB identity, under which their session is logged and recorded. The WAB allows system administrators to maintain the flexibility of shared accounts without compromising audit or security regulations.

3.5 Total traceability of user operations

The WAB enables the contents of sessions to be recorded, both in Flash© video format for RDP/TSE sessions (Windows servers) and in text or video format for SSH, TELNET and rlogin sessions (Linux & UNIX servers, network devices).

These session recordings can be viewed in real time, or later, to see exactly what has been done by any service provider on any target device. A benefit of the text file records of SSH sessions is the ability to search via keywords.

Note: session records can be stored in the WAB or exported to an external storage device.

3.6 Seamless integration with legacy user-management systems

The WAB fits effortlessly into existing user-management systems. If the service provider data is contained within in an enterprise directory (LDAP, Active Directory, etc.), users can be authenticated via this directory. The WAB also allows for local authentication (the service provider password is then managed by the WAB). The WAB allows the use of RADIUS as an external authentication protocol, supporting solutions such as RSA SecurID and SafeWord.

Finally, the WAB can be managed by third-party applications, such as IAM and Helpdesk, via a built-in API.

3.7 Reduced installation and administration costs

The WAB can be delivered as a physical device and/or a virtual appliance. It is based on agent-less technology, therefore, no agents are required on the target devices or user workstations, leading to a significant reduction in deployment times. Initial configuration of the WAB, and its ongoing administration, take place via a simple web interface (https), currently available in English and French. It is also possible to administer the WAB via a Command Line Interface (CLI).

To eliminate the need to train users on new applications, the WAB enables administrators to continue using their familiar server administration tools, such as the SSH clients Putty and WinSCP and Remote Desktop (RDP) clients.

Note: to logon to target devices via the WAB, service providers can also use a PC (Windows, Mac, Linux) and, when on the move, their smartphone (iPhone, Android, BlackBerry, Windows Mobile).

3.8 Generation of alerts

The WAB ships with an *alerts generation module*. It allows an alert to be sent by e-mail to a specific person (e.g., the WAB administrator), and automatically recorded in the WAB log file, in the event of an attempted login to a target account predefined as critical. Upon receiving this alert, the WAB administrator can *allow* or *kill* the session directly, via a screen which displays a list of current open sessions.

4. RISK MITIGATION

Almost 50% of the IT administrators surveyed in 2009* stated they would use their privileges to steal critical company data. This is a significant threat, not only to IT security but also to the organization's public reputation. The WAB protects enterprises and their data against this and other risks by ensuring:

- Nondisclosure of passwords for target devices
- Granularity of access rights and their management
- Comprehensive traceability of administration sessions (session recording)
- Alerts in the event of access to critical servers

5. STANDARDS COMPLIANCE

Increasingly, leading companies see the business advantage in publicly maintaining the highest compliance standards. The WAB's inbuilt reporting tools and session recording (traceability), supports companies to maintain specific standards including ISO 27001, PCI DSS, SOX, Basel II and HIPPA. The WAB solution simplifies the process of implementing recommendations made, for example, by company auditors, so enhancing the company's profile.

6. CONCLUSION

With the Wallix AdminBastion, companies finally have a solution which enables sophisticated management of external IT service providers without undergoing root-and-branch technical and organizational restructuring.

The Wallix AdminBastion will deliver audit information, session recording and access control, increase the productivity of your service providers and provide real-time control of their systems use. In addition, since the Wallix AdminBastion uses rights management *per role*, its implementation formalizes administrator access rights and rationalizes access control policies.
When your enterprise IT System must be used by external service providers, the WAB solution secures it, monitors it and guarantees that its integrity is never compromised.

About Wallix

Wallix solutions empower organizations to guarantee the integrity of their IT systems, ensure traceability and implement a robust compliance and certification approach. (e.g. ISO 27001)

Wallix is a global leader in the market for IT security software that secures critical networks and infrastructures. Established in France in 2003, Wallix is an international organization with operations in Europe, the UK and the USA.

Wallix provides intelligent answers to security challenges posed by increasing data digitisation and by IT resource outsourcing.

We supply innovative access and control solutions to enterprises, governments and large organizations. With a user-driven strategy based on innovation and response to market demands, Wallix offers a range of scalable solutions whose features address critical corporate issues.

Because organizations expect effective and rapid responses, Wallix delivers agentless solutions that integrate easily into existing IT systems.

www.wallix.com

WALLIX FRANCE
http://www.wallix.fr
Email : sales@wallix.com
118, rue de Tocqueville - 75017 Paris
Phone: +33 (0)1 53 42 12 90
Fax: +33 (0)1 43 87 68 38

WALLIX UK
http://www.wallix.com
Email: ukinfo@wallix.com
Lincoln House - 300 High Holborn - London WC1V 7JH
Phone: +44 (0) 3333 441120
Fax: +44 (0) 3333 441160

WALLIX USA
http://www.wallix.com
Email: sales-usa@wallix.com