CENTRIFY WHITE PAPER. MAY 2014

Close the Window on Three Windows Server Threat Scenarios

Security breaches are all over the news, many of them a result of either insider threats or advanced persistent threats. Companies and government agencies are looking for solutions to mitigate the risks these threats present. This white paper details three common Windows Server threat scenarios and explains the way that they can be neutralized. By following the guidelines in this white paper, organizations can guard against inside and outside threats, protect their Windows Server infrastructure and sensitive data, and meet relevant regulatory requirements.

Contents

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organisations, products, domain names, email addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organisation, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Centrify Corporation.

Centrify may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Centrify, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Centrify, DirectControl and DirectAudit are registered trademarks and Centrify Suite, DirectAuthorize, DirectSecure and DirectManage are trademarks of Centrify Corporation in the United States and/or other countries. Microsoft, Active Directory, Windows, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Introduction

2013 was something of a banner year for security breaches, leading Symantec to dub it the year of the "Mega Breach."[1] Seemingly no organization was immune, with multinational corporations and government agencies alike experiencing massive violations of their systems, applications, and data.

What these breaches made clear is that any organization that isn't taking identity-management seriously is potentially putting their Windows Server environment at risk. Two of the most treacherous hazards of the Windows Server threat landscape—insider threats and advanced persistent threats—depend on an organization's lack of control over identity:

- → **Insider threats** come from people within an organization and occur when there's a lack of control over the identities that can access sensitive servers and information.
- → **Advanced Persistent Threats (APTs)** are attacks from the outside that can use unsecured identities as an attack surface to gain access to protected systems, applications, and data.

Make no mistake, though: whether a security breach comes from the inside or the outside, they both carry the same potential to wreak havoc with data, infrastructure, and reputations.

And in today's highly regulated environment, these breaches are more than just embarrassing. The Federal Information Security Management Act, the Payment Card Industry Data Security Standard, the Sarbanes-Oxley Act, and the Health Insurance Portability and Accountability Act are just some of the laws and mandates regulating the way businesses, government agencies, and other groups must secure access to systems and applications, audit privileged activity, and provide proof that access controls are in place and working as designed. Many organizations that passed their audits in previous years failed them in 2013 because they were not properly protecting their Windows Server environment.

This white paper details three common threat scenarios that can impact an organization's Windows Server environment – and explains how technology like Centrify Server Suite can successfully be used to neutralize these threats, allowing organizations to meet both operational and regulatory compliance goals.

[1] Symantec Corporation Internet Security Threat Report 2014: Volume 19

Threat Scenario 1: Too Many Local Admins

In today's heterogeneous IT environments, administrative identities are growing at an uncontrolled rate. Without a scalable model for managing your insiders' identities, associated privileges, and privileged activity across applications, platforms, and devices, blind spots are created that result in unanticipated risks.

Let's say a user needs to manage one or more Windows services on a group of database servers used internally by the enterprise. A typical method by IT is to grant the user local administrator group membership on the database servers.

Reality Check

At least three of the most-recognized global financial organizations failed audits in 2013 that they expected to pass, because of giving over-privileged and under-audited accounts to Windows administrators without a corresponding business need.

Perhaps the rights are time boxed; perhaps the password will be changed. Regardless, for the duration of time the user is local administrator, the user "owns" the computer and has full access to all of its resources. There is no limit to what the user can do on the database servers.

Worse still, because there's a local administrator account in effect on the Windows server, an APT now has a vector for a "land and expand" attack: for example, it could use "pass-the-hash" to leverage control over one server into control over additional servers and resources.

Solution: Provide Just Enough Privilege

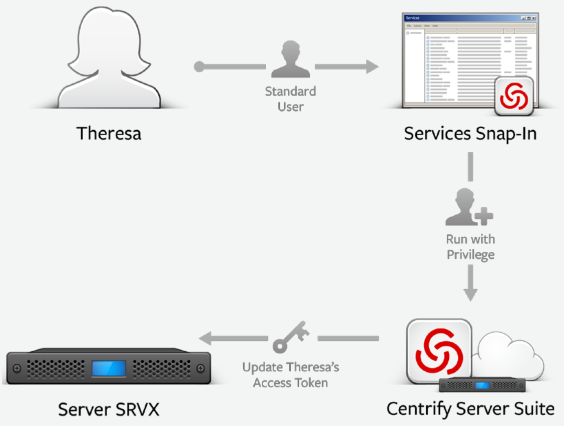
The right way to thwart this type of insider threat is by granting the user just enough privilege to accomplish their business objectives. "Just enough privilege" means the ability to manage one or more Windows services on the target database servers without granting local administrator group membership.

In taking this approach, organizations eliminate the problem of too many users having broad and unmanaged administrative powers by securing privileged access and granularly enforcing who can perform what administrative functions. Additionally, organizations gain global control and visibility over privileges and enable user-level auditing across all servers, both on-premises and in the cloud.

With a solution like Centrify Server Suite in place, organizations are able to make this type of scenario a reality and attribute actions to the correct human. This type of clear audit trail is one of the first steps towards securely managing Windows services.

Securely elevate privilege.

Theresa seamlessly elevates privilege without being Local Admin or knowing the administrative password.



Threat Scenario 2: Shared Accounts without Accountability

If there were a dictionary that contained the phrase "enables insider threats", it would surely have shared accounts at the top of the definition.

IT organizations are required to create user accounts in Active Directory and share both the account name and its password with multiple users. These shared accounts are necessary in a variety of situations. Unfortunately, shared user accounts are hard to manage and difficult-to-impossible to secure using traditional privileged account management (PAM) technologies. Users can freely share passwords for shared accounts with very little risk of accountability when IT uses only native Windows controls because native tools audit the shared account without attribution to the actual user.

Reality Check

"Where I think we were negligent... is that we allowed [Edward Snowden] some form of anonymity as he did [what he did]. Someone wasn't watching all of that. So the lesson learned for us is that you've got to remove anonymity from the network."[2]

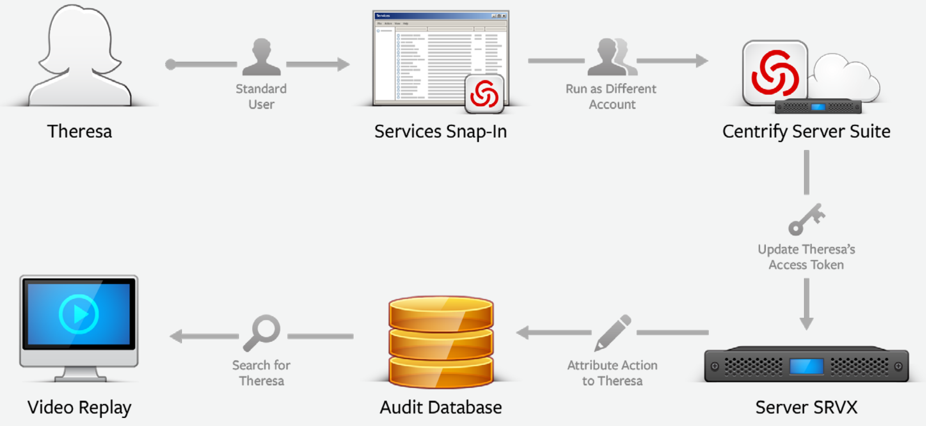
Solution: Trace Actions Back to the Actual User

Clearly, shared accounts need special handling. The right way to share accounts is to share their privileges, but not their passwords. An ideal solution should allow a user to act with the privileges of the shared account. It should not require the user to even know the password. Additionally, the user should always be audited through their single Active Directory account, so that actions attribute back to the actual human who's using the privileges of the shared account.

Centrify Server Suite allows end users to use shared accounts in Active Directory without requiring them to know the shared account name or password. The Centrify Agent adds the identity and/or privileges of the shared account to the user's security token when the user launches a privileged application, as in the following figure featuring our user Theresa:

Eliminate anonymous activity.

Theresa logs in as herself and all her privileged activity is associated with Theresa's Active Directory account (vs. a shared account).



The end result is the ability to create and deploy shared user accounts safely and with guaranteed accountability that actions are associated with the correct end user. Because it's not enough to implement access controls: one has to also be able to audit all activity associated with those access controls.

[2] Lonny Anderson, NSA Director of Technology

Threat Scenario 3: No Protection for PCI Data from Domain Admins

One of the realities of Windows domain administration is that virtually every organization of any size can run afoul of the principle of separation of duties (also called segregation of duties).

This principle manifests in multiple ways: it could mean that an employee who can create an invoice in a billing system should never have the ability to audit the creation of said invoice. Or, in what is probably the single most common violation of this principle in Windows domain administration today, it could mean that a very high percentage of an organization's domain admins – who have zero business justification for access to sensitive and regulated data – do, in fact, have access to that sensitive and regulated data.

Reality Check

2013 culminated with a security breach at a very large, well known retailer that compromised the credit card and debit card information for as many as 70 million individuals. Investigations into the security breach revealed that thieves gained access to the retailer's computer systems through network credentials they had stolen from a heating and refrigeration vendor. This vendor clearly had no business justification for access to the PCI servers – and if their credentials provided "least access" privilege, the damage would've been minimized.

Solution: Enforce Segregation of Duties

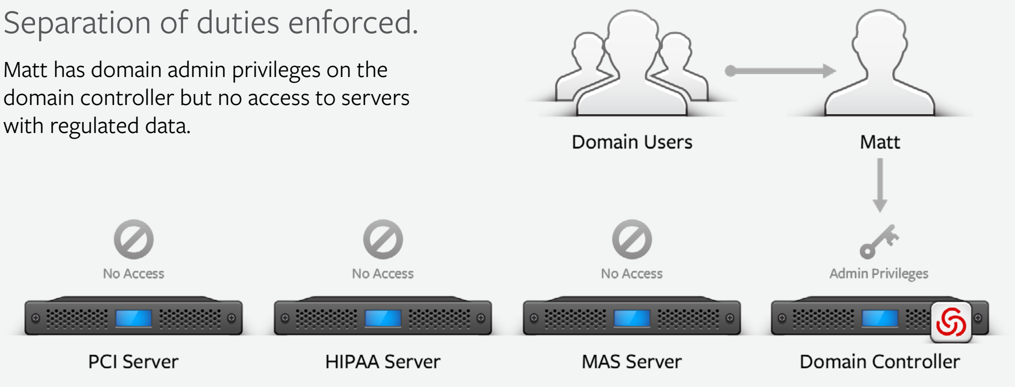
The right solution should enable you to make a user a Domain Admin based on the computer they're logged into rather than making them a local administrator on every computer in the domain. In other words, they aren't granted special privileges on any other computers.

This action protects PCI data because the Domain Admin won't have administrative credentials for the PCI servers. As an additional benefit, it reduces the attack surface for APTs because users won't be logging in with Domain Admin or Local Admin accounts.

The way that Centrify Server Suite enforces this segregation of duties can be seen in the following illustration using a domain administrator named Matt:

Separation of duties enforced.

Matt has domain admin privileges on the domain controller but no access to servers with regulated data.



Using this type of setup protects PCI data from internal employees who have no business justification for access to the PCI servers, while enabling the domain administration team to manage the Active Directory deployment using their standard tools. As a result, organizations can protect regulated data from domain administrators while enforcing the separation of duties required by regulations and auditors.

Conclusion

In today's IT security environment, malicious insiders and outsiders are ultimately after the "keys to the kingdom". Access to privileged accounts gives hackers everything they need to steal or siphon off sensitive data from mission critical servers.

This type of malicious access stems from lack of control over identity. As the three preceding scenarios illustrate, solutions like Centrify Server Suite provide organizations with the control they need to thwart these threats. It protects their Windows Server environments by:

- Granting users just enough privilege to accomplish their business objectives, enabling secure management of Windows services
- Making shared accounts in Active Directory accountable by associating the use of a shared account with the actual user
- Protecting PCI data from domain admins by enforcing a segregation or separation of duties

By taking these steps, organizations can manage their identity-related risk posture and significantly improve their ability to cost-effectively address regulatory mandates, making compliance a repeatable and sustainable part of their business.

Download a trial version of Centrify Server Suite today to see how it can benefit your organization: http://info.centrify.com/centrifysuitetrialrequest.html.

Additional Resources

Solution Information

- Centrify Server Suite: Windows Server Protection

Solution Briefs

- Secure Management of Windows Services
- Shared Accounts with Accountability
- Protect PCI Data from Data Admins

Webinars

- Identity Related Risks: Have you met your Administrators?
- Shared Accounts: The Back Door That's Tough to Close
- Protecting Critical Corporate Data from Privileged Users on Windows Server

Contact Centrify

HEADQUARTERS	Centrify Corporation 3393 Octavius Drive, Suite 100 Santa Clara, CA 95054 USA
WEB	www.centrify.com/contact
EMAIL	sales@centrify.com

US	+1 (669) 444-5200
EMEA	+44 (0) 1344 317950
ASIA PACIFIC	+61 1300 795 789
BRAZIL	+55 (11) 96644-2524
LATIN AMERICA	+1 (917) 754-1112