

CENTRIFY DIRECTSECURE

Secures sensitive information by dynamically isolating cross-platform systems and encrypting data in motion

How protected are you from insider threats?

Today's rapidly growing networks are becoming even more interconnected and are moving toward a hybrid of physical, virtual and cloud computing. IT organizations are facing new challenges trying to balance the need for greater accessibility with the requirement to better secure sensitive information within this dynamic computing environment.

While firewalls, secure routers and other security methods protect at the edge, unfortunately, once inside, unmanaged systems (e.g. guests and contractors) or rogue computers can cause damage in the form of introducing malware, exploiting vulnerabilities or launching denial-of-service attacks.

Equally concerning is the fact that the majority of corporate data theft is now coming from insiders who are gaining access to systems that they should not be able to access.

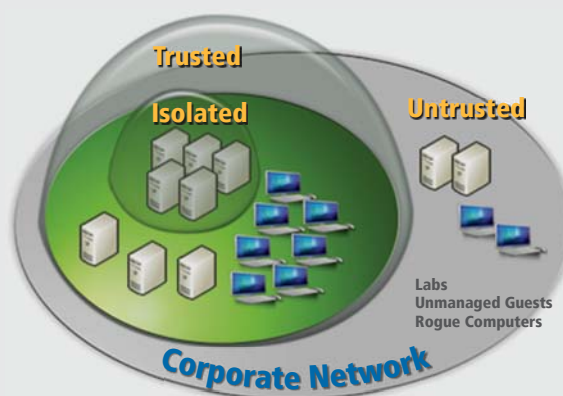
Existing solutions for securing access to sensitive information are failing

Technologies such as VLANs do exist to segment your network, but they require costly hardware or agents on each end-user system, don't work well in virtual or cloud environments, or force you to change your network topology and applications. Not only are existing solutions painful to deploy, but given the ever increasing number of successful insider attacks it is clear that existing approaches are failing.

Centrify offers a more flexible and cost-effective approach to securing your internal networks

Fortunately Centrify has the answer to securing access to sensitive information in today's dynamic computing environment: Centrify DirectSecure. Unlike other solutions that are costly to deploy and inflexible, Centrify DirectSecure is a policy-based software solution that secures sensitive information by dynamically isolating and protecting cross-platform systems and enabling optional end-to-end encryption of data in motion. By leveraging your existing Active Directory infrastructure and the native IPsec support built into today's operating systems, DirectSecure seamlessly blocks untrusted systems from communicating with trusted systems, and does so without the need to change your network or applications. Additionally, DirectSecure enables you to take advantage of the new Windows 7 DirectAccess feature to secure end-to-end communications with UNIX and Linux systems running DirectSecure.

DirectSecure leverages your existing infrastructure to add another layer to your defense-in-depth strategy



DirectSecure blocks "untrusted" systems from communicating with "trusted" systems via its unique, server-based software solution that leverages your Active Directory infrastructure and the native IPsec support in modern operating systems. DirectSecure also delivers tiered network access by further isolating groups

of systems. The result is improved adherence to regulatory compliance initiatives as well as an additional layer of policy-driven protection against network attacks for mixed Windows and UNIX/Linux environments.

With DirectSecure, unmanaged or rogue computers are not able to establish network communication with systems protected within the logically isolated network. You can then further restrict network access to specific resources and you can even selectively encrypt network traffic.

Segmenting and securing your network is done in minutes with no hardware required or changes to your environment

Step 1

Use DirectSecure to simply join a UNIX system to Active Directory to enable end-point authentication

```

root@frankfurt ~]# adjoin contoso.com -z NULL_AUTO -n frankfurt
Administrator's Active Directory password:
Using writable domain controller: denver.contoso.com
Join to domain:contoso.com, zone:Workstation Mode successful

Centrify DirectControl started.
Loading domains and trusts information
    
```

Step 2

Apply policies to enforce isolation and/or encryption

Link	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain
1	SDI - 5 Encryption Group Isolation GPO	No	No	User config...	None	2/1/2...	contoso...
2	SDI - 4 Boundary Group Isolation GPO	No	No	User config...	None	2/1/2...	contoso...
3	SDI - 3 No fallback Group Isolation G...	No	No	User config...	None	2/1/2...	contoso...
4	SDI - 2 Server Isolation Finance GPO	No	No	User config...	None	2/1/2...	contoso...
5	SDI - 1 Domain Isolation GPO	No	Yes	Enabled	None	1/30/...	contoso...
6	Default Domain Policy	No	Yes	Enabled	None	1/30/...	contoso...

BEFORE & AFTER : SERVER ISOLATION

Open TCP Ports:

- 10.1.1.1 : 53 * 88 135 139 389 445
- 10.1.1.2 : * 80 * 139 * 445
- 10.1.1.3 : * * 135 139 * 445
- 10.1.1.4 : * * 135 139 * 445

Before
User on rogue system can communicate with UNIX HR system with IP address 10.1.1.2

Open TCP Ports:

- 10.1.1.1 : 53 * 88 135 139 389 445
- 10.1.1.2 : * * * * *
- 10.1.1.3 : * * 135 139 * 445
- 10.1.1.4 : * * 135 139 * 445

After
User on rogue system is blocked from communicating with UNIX HR system

BEFORE & AFTER : DATA ENCRYPTION

Before
Using a network scanner, an insider captures the password for a system hosting credit card data

After
Data is encrypted so an insider cannot sniff passwords or any other sensitive info

Six Reasons to Choose DirectSecure

1. Deter external security threats by preventing unmanaged or rogue computers from communicating with trusted systems

Most networks are “hard on the outside and soft on the inside” from a security perspective. Firewalls, secure routers and other security methods protect at the edge, but once inside, unmanaged systems (such as those brought in by guests and contractors) or rogue computers can cause by introducing malware, exploiting vulnerabilities or launching denial of service attacks. DirectSecure addresses those threats by preventing an “untrusted” system — a system that has not been authenticated via issuance of a PKI certificate or a Kerberos ticket from Active Directory — from establishing networking communication with “trusted” systems. This means that even if an attacker has obtained a valid username and password, they can't access your trusted systems. And unlike other isolation solutions which rely on IP addresses that can be spoofed, DirectSecure cannot be spoofed because trusted systems must be authenticated. The net result is another layer to your defense-in-depth security strategy and a reduction in your infrastructure's surface area that is exposed to attacks.

2. Protect against insider threats by further restricting access to specific resources and dynamically segmenting your network

Analysts are now saying that the majority of corporate data theft is coming from insiders. DirectSecure not only protects trusted systems from untrusted systems, but can further secure your trusted systems by delivering tiered network access and tighter control over who can access specific groups of systems. For example, with DirectSecure you can dynamically segment and isolate specific groups of systems that process credit card or personal health information from other trusted systems. This software- and policy-based approach to network segmentation can help you significantly reduce the scope of an audit. For example, you can limit a PCI audit just to the systems that process credit card data, not your entire flat network.

3. Enable optional end-to-end encryption of data in motion to address compliance requirements and secure sensitive data

With DirectSecure, traffic sent between trusted systems is cryptographically protected so that the receiving system can verify that an authenticated system sent the packet and that the packet was not tampered with and/or modified in transit. With DirectSecure you can even configure groups of servers to accept specific types of traffic. In addition, some or all of the traffic between managed systems can be optionally encrypted, providing protection from malicious network users who attempt to capture and interpret network traffic. Encrypting data in motion is important to addressing audit requirements (for example, PCI requirement No. 4) or to better secure legacy applications that transport sensitive data in the clear.

4. Seamlessly implement logical secure boundaries spanning physical, virtual and cloud-based systems

The need to secure access to sensitive information has traditionally forced organizations to not take full advantage of virtualization because they don't want to consolidate their more secure systems with less secure systems on the same virtual servers. This is because in many virtualization scenarios the traffic comes from a common MAC address and it is very hard to partition traffic based on MAC addresses. A similar concern rests with cloud computing in terms of who can access your systems that you want to host in the cloud. DirectSecure addresses these concerns by letting you build logical security boundaries that span physical, virtual and cloud-based systems. These security boundaries are erected by independently authenticating and protecting each virtual machine, as opposed to attempting to partition traffic from MAC addresses.

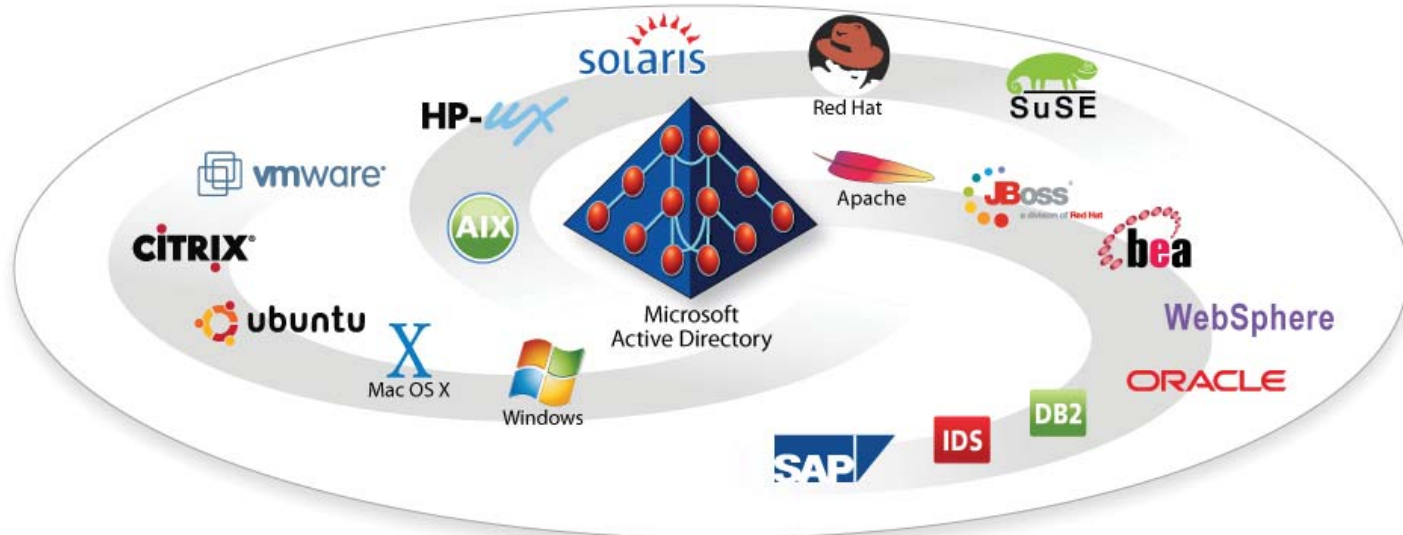
5. Automate the provisioning of certificates on UNIX and Linux systems

Managing certificates on UNIX and Linux systems is required for web servers and other types of applications, but provisioning certificates is a very manual and time-intensive process. DirectSecure automates the provisioning of certificates by delivering a UNIX client for Microsoft's certificate server that can be managed by Group Policy and is secured via Kerberos.

6. Extend your existing infrastructure in a transparent and cost-effective manner without the need for additional investments in hardware or software

DirectSecure builds upon technologies that already exist in your environment, including your existing Active Directory infrastructure and the IPsec functionality that is built into the modern UNIX, Linux and Windows operating systems that you have deployed. This means you can leverage existing skill sets to deploy and manage authentication policies that enforce the end-to-end security you want between your systems. It also means DirectSecure works without the need for additional hardware or for disruptive changes to network topology or even to applications. And because DirectSecure uses IPsec, which is a Layer 3 protocol, it operates transparently to both applications and users. Finally, because Microsoft already provides both Group Policy and IPsec as a standard part of the Windows platform through its Server and Domain Isolation solution, there is no additional cost to integrate Windows systems with UNIX and Linux systems supported by DirectSecure.

DirectSecure: An Integral Part of the Centrify Suite



DirectSecure is an integral part of the Centrify Suite of solutions for securing non-Microsoft systems and applications. Centrify DirectSecure builds on top of the Centrify DirectControl architecture, which provides the ability to join a non-Microsoft system to Active Directory, thereby facilitating the ability for a UNIX or Linux system to obtain a Kerberos ticket or, with DirectSecure installed, to obtain a PKI certificate.

DirectControl also provides the cross-platform Group Policy engine that DirectSecure leverages to apply end-point authentication policies, and can

To Learn More

DirectSecure is now available for end-point authentication leveraging public key infrastructure (PKI) and pre-shared keys (PSK). End-point authentication leveraging Kerberos and support for Microsoft DirectAccess is available under the Centrify early access program. If you're interested in evaluating DirectSecure, contact your Centrify representative.

For more details see: <http://www.centrify.com/directsecure>.

DirectSecure Supported Platforms

DirectSecure supports the following operating systems:

- Red Hat 5.x
- Solaris 10
- SUSE 10.x
- Additional platforms based on customer demand

Microsoft delivers the same capability as DirectSecure as a standard part of the Windows platform for the following operating systems:

- Windows XP, Windows Vista and Windows 7
- Windows Server 2003 and 2008

also control which users can log in to which groups of UNIX and Linux systems. Other complementary solutions in the Centrify Suite include DirectAuthorize, which provides granular role-based security, and DirectAudit, which provides user-level auditing of non-Microsoft systems.

Built on a common architecture, the seamlessly integrated Centrify Suite of solutions helps you improve IT efficiency, strengthen regulatory compliance initiatives, and centrally secure your heterogeneous computing environment.

Contact Us

The Centrify Suite centrally secures cross-platform data centers through Active Directory-based identity and access management of the industry's widest range of heterogeneous systems, hypervisors and applications. Built on an integrated architecture that leverages our patented technology, the Centrify Suite of solutions enables organizations to reduce IT expense and complexity, improve end-user productivity through single sign-on, strengthen security and enhance regulatory compliance initiatives. Key components of the Centrify Suite include integrated authentication, access control, role-based privilege management, user-level auditing and server protection solutions, consisting of Centrify DirectControl, Centrify DirectAuthorize, Centrify DirectAudit, Centrify DirectSecure, and Centrify DirectManage.

PHONE: +1 (408) 542-7500 (Worldwide)
+44 (0) 1344 317950 (EMEA)

EMAIL: info@centrify.com

WEB: www.centrify.com

Centrify and DirectControl are registered trademarks, and DirectAuthorize, DirectAudit and DirectSecure are trademarks of Centrify Corporation.

DS-016-2011-02-15