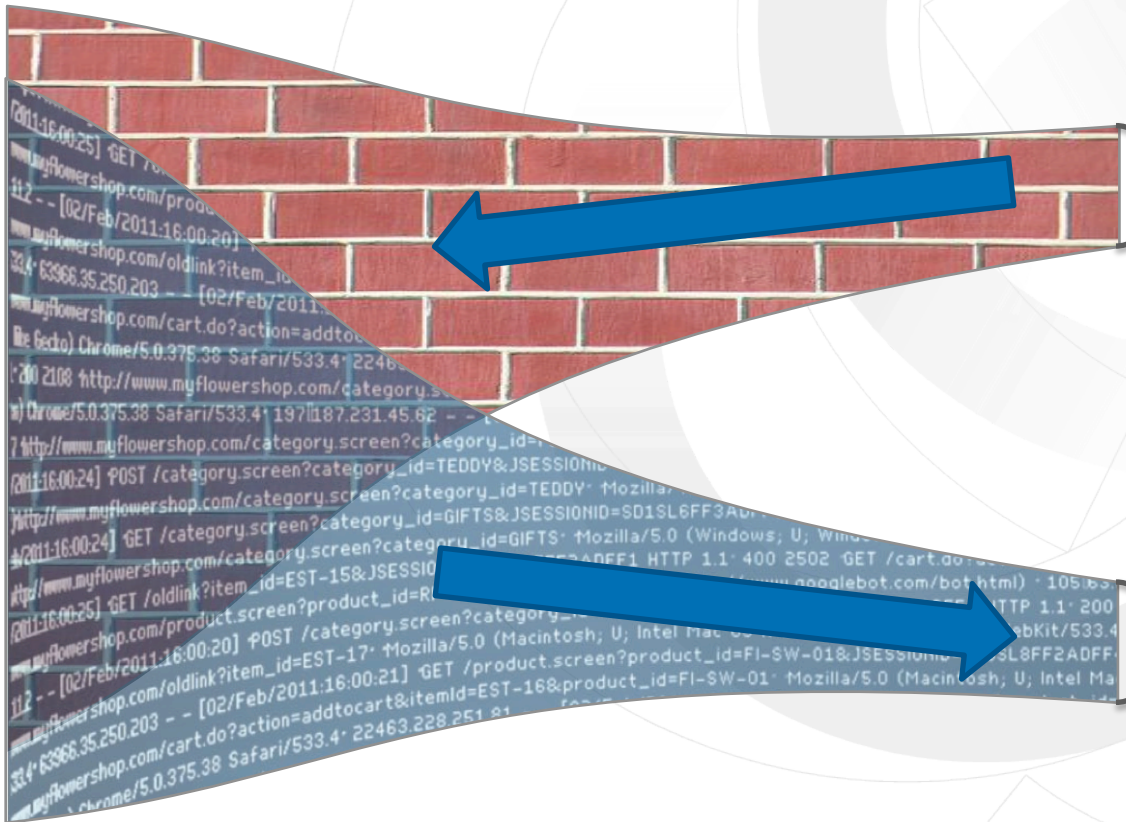
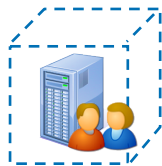


How Do Centrify and Splunk Work Together?



Control.



Visibility.

Introducing the Centrify Suite

Control, secure and audit access to cross-platform systems and applications by leveraging an infrastructure you already own — Active Directory

Corey Williams
Director of Product Management
Centrify Corporation



Evolving IT Trends Create Risk, Loss of Control

Emerging IT Trends

- Hybridization of the data center
- Evolving regulatory climate
- Adoption of virtualization and cloud computing platforms
- Consumerization of IT
- The new office

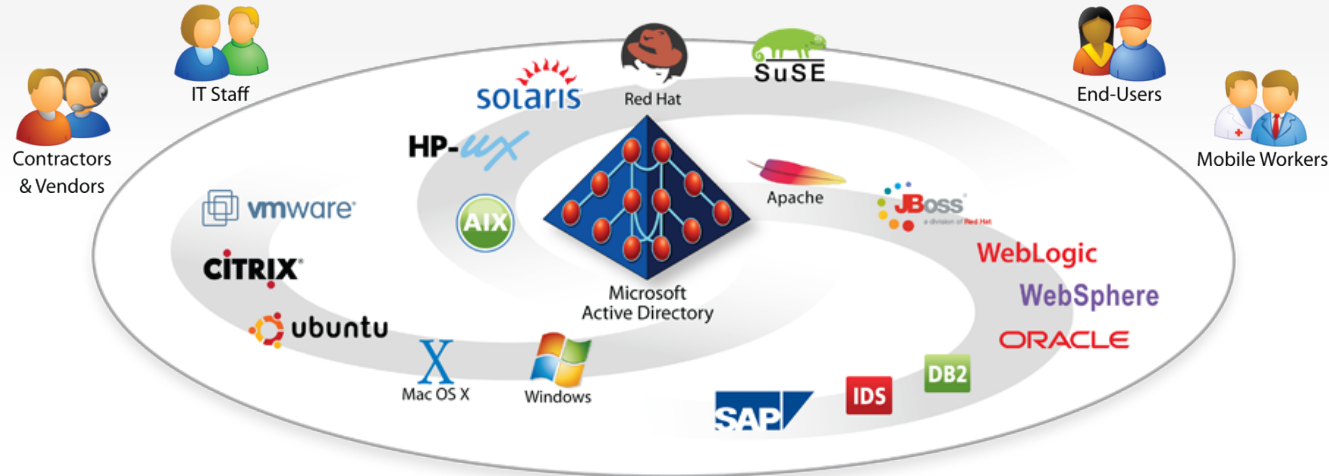
Corresponding Challenges

- Can I effectively control who has access?
- Can I manage what users can do?
- Can I verify for auditors what users did?
- Can I manage personal devices employees bring into the workplace?
- How do I effectively leverage my existing infrastructure and skillsets in this world?

The Centrify Vision

Control, Secure and Audit Access to Cross-Platform Systems and Applications

Centrify the Enterprise



Leverage infrastructure you already own – Active Directory – to:

Control

What users can access

Secure

User access and privileges

Audit

What the users did

Trusted by Over 3000 Customers Worldwide

Banking & Finance



Pharma & Chemical



Defense & Government



Retail & Internet



Technology & Telecom



Automotive & Energy



Solutions that Centrifly Delivers

Compliance and Audit

- Auditing and reporting (SOX, PCI, FISMA, HIPAA, Basel II, etc.)



SOX / JSOX

VISA

PCI DSS



FISMA



HIPAA



**Basel II.
FFIEC**



... ?

Solutions that Centrify Delivers

Compliance and Audit

- Auditing and reporting (SOX, PCI, FISMA, HIPAA, Basel II, etc.)

Security

- Risk mitigation & security of users with privileged access

Meet Strict Security & Audit Req's

- ✓ Enforce system security policies
- ✓ Enforce "least access"
- ✓ Lock down privileged accounts
- ✓ Enforce separation of duties
- ✓ Associate privileges with individuals
- ✓ Audit privileged user activities
- ✓ Protect sensitive systems
- ✓ Encrypt data-in-motion

Solutions that Centrify Delivers

Compliance and Audit

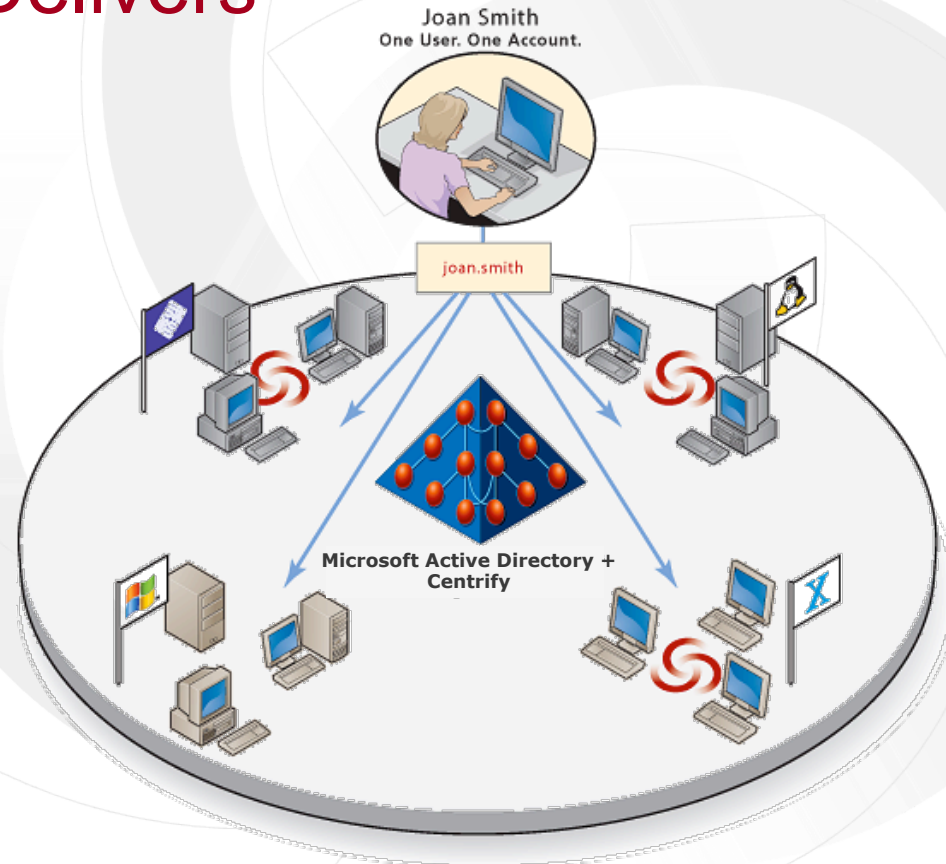
- Auditing and reporting (SOX, PCI, FISMA, HIPAA, Basel II, etc.)

Security

- Risk mitigation & security of users with privileged access

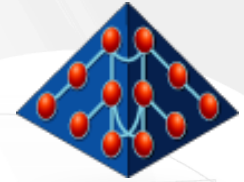
Operational Efficiency

- Leverage existing architecture
 - Leverage existing tools, skillsets and processes
 - Consolidate "islands of identity"
 - Deliver single sign-on for IT and end-users
- Enable new computing models such as virtualization, cloud and mobile



Proven Methodology for Better Governance

Centralized Identity. Automated Policy.



280+ Systems

- Red Hat
- SUSE
- Solaris
- AIX
- HP-UX
- Mac
- Etc.

Dozens of Apps

- SAP
- Apache
- WebLogic
- WebSphere
- Apache
- Jboss
- DB2
- Etc.

Privileged Access Management

- Associate privileges with individuals
- Enforce “least access” and “least privileges”
- Audit privileged user activities
- Isolate systems & encrypt data-in-motion

Identity Consolidation

- De-duplicate identity infrastructure
- Get users to login as themselves / SSO
- Single security policy engine
- Single point of administrative control

Governance



Compliance



Security



Connectivity

Centrify Products... Delivered as the Centrify Suite

EXPRESS STANDARD ENTERPRISE PLATINUM

DirectManage

Centralized Management and Administration



DirectControl

Centralized Authentication and Access Control



DirectAuthorize

Role-based Authorization and Privilege Management



DirectAudit

Detailed Auditing of User Activity



DirectSecure

Server Isolation and Protection of Data-in-Motion



Single Sign-On For Applications

With all editions you can purchase SSO modules for:

- Apache and J2EE web applications
- SAP NetWeaver & GUI
- DB2

Centrify-Enabled Open Source Tools

All editions also include free, Centrify-enabled versions of:

- OpenSSH
- PuTTY
- Kerberized FTP and Telnet
- Samba

Centrify Express – Get Started Today!



Centrify Insight Powered by Splunk

Show me accounts not used in last 90 days.

Are there any systems where Centrify is not connected to AD?

How long was a user in a role?



I want to see all failed login attempts.

Are there any newly created local accounts on my server?

Who zone-enabled this user?

Centrify Insight Powered by Splunk

splunk > Centrify Logged in as Administrator | App | Manager | Alerts | Jobs | Logout

Dashboards - Logs and Configs - Search - Support - Help | About

Centrify Insight Overview | Actions

Getting Started

Add the data sources required for this app to provide meaningful functionality:

- Splunk Search Head — Install Splunk 4.2, install this app, enable the twitter input and forward the remaining boxes here.
- Windows Domain Controller(s) — Install the Windows Universal Forwarder. Collect Security Log and Active Directory. Must be run as an Active Directory domain user.
- Centrify managed "NIX boxes" — Install Splunk 4.2, install this app, enable the appropriate inputs and forward to the Splunk Search Head.

To learn more about this app and Centrify:

- Read the Installation Guide
- Free Active Directory Tools for UNIX, Linux and Mac
- Centrify Express Community
- Splunk Answers for Centrify Insight
- Centrify Customer Support
- Centrify Support Tweets

NOTE: There are several scheduled searches we run on a regular basis in Splunk Enterprise. In Splunk Free you will need to manually run these searches once or twice a day. It is also useful to manually run these searches after changes like turning on addebug to collect centrifydc.log data.

- Reload Active Directory Lookups
- Reload Active Directory History
- Reload centrifydc.log hosts
- Reload centrifydc.log modules

Centrify Insight Dashboards

- Centrify Zone User
- Active Directory User
- Search Centrify Data

Recent Centrify Support Tweets

- | date | tweet |
|-------------------|--|
| about a month ago | adinfo adds a capability to validate AD user and password against a given domain. E.g., adinfo -A -u ADUSER |
| about a month ago | Centrify Suite 2011 now integrates more than 280 UNIX, Linux and Mac platforms with Microsoft Active Directory |
| about a month ago | Centrify Suite 2011 now available for download. For more details, visit http://bit.ly/hLcvok (Requires login to Centrify) |
| about a month ago | @pwyfliu : Did you mean SLES 11 SP1 ? If so yes' Please check out our detailed list of supported platforms here |
| about a month ago | RT@CentrifyNews: Happy 6 year birthday #Centrify #DirectControl !! http://bit.ly/bYTS66 V1.0 had support for |

splunk > Centrify Logged in as Administrator | App | Manager | Alerts | Jobs | Logout

Dashboards - Logs and Configs - Search - Support - Help | About

Centrify Zone Activity | Actions

Object Type Activity Type Zone

User Any Any

≥ 2 matching events | 102,989 scanned events

mary

Created a day ago by CENTRIFY-SEadministrator

centrify.se/Program Data/Centrify/Zones/RHEL/Users/mary

Centrify Zone	UNIX User	UID	Shell	Home
RHEL	mary	10011	/bin/bash	/home/mary

Show all 359 lines for 10 events DC — se-win2k8ent.centrify.se

thor

Updated 2011-04-05 22:06:02.523000 by CENTRIFY-SE

centrify.se/Program Data/Centrify/Zones/RHEL/Users/thor

Centrify Zone	UNIX User	UID	Shell
RHEL	thor	10009 → 10010	/bin/bash

Show all 479 lines for 13 events DC — se-win2k8ent.centrify.se

splunk > Centrify Logged in as Administrator | App | Manager | Alerts | Jobs | Logout

Dashboards - Logs and Configs - Search - Support - Help | About

Active Directory Activity | Actions

Object Type Activity Type Group Type Search Text

Any Any Any

≥ 5 matching events | 183,682 scanned events

test107group

Added member(s) to this group a day ago by CENTRIFY-SEadministrator

centrify.se/Users/test107group

AD Group	Group Scope	Group Type	Affected Members
test107group	Global	Security	centrify.se/Users/Corey Williams centrify.se/Users/Mary Williams centrify.se/Users/Matt Palmer

Show all 263 lines for 8 events DC — se-win2k8ent.centrify.se Windows Event Codes — 4728, 4737, 5136

test107group

Created a day ago by CENTRIFY-SEadministrator

centrify.se/Users/test107group

AD Group	Group Scope	Group Type
test107group	Global	Security

Show all 201 lines for 6 events DC — se-win2k8ent.centrify.se Windows Event Codes — 4727, 5136, 5137

Becky Williams

Updated a day ago by CENTRIFY-SEadministrator

centrify.se/Users/Becky Williams

AD User	Mail
Becky Williams	becky.williams@centrify.se → bwilliams@centrify.se

Show all 270 lines for 7 events DC — se-win2k8ent.centrify.se Windows Event Codes — 4738, 4781, 5136

Common Centrifly and Splunk Customers

Finance & Insurance



Technology & Telecom



Others



Defense & Government



Why Customers Choose Centrifly

Gartner. *Centrifly is the "right vendor to choose" for Active Directory integration: Centrifly's solution is "mature, technically strong, full featured, and possess(es) broad platform support."* – 2009

"We recommended that clients strongly consider Centrifly ... its products can fit well within a multivendor IAM portfolio." – 2010

Experience & Expertise

- 3000+ enterprise customers
- Largest dedicated team
- Unparalleled 24x7 support
- Record growth and profitable

The Best Solution

- Single architecture based on AD
- Comprehensive suite
- Proven success in deployments
- Non-intrusive

Industry Awards



Industry Certifications



How To Contact Us

WEB SITE

www.centrifys.com

TECHNICAL VIDEOS & MORE

www.centrifys.com/resources

SUPPORTED PLATFORMS

www.centrifys.com/platforms

REQUEST AN EVAL

www.centrifys.com/trial

CONTACT US

www.centrifys.com/contact

PHONE

Worldwide: **+1 (408) 542-7500**

Europe: **+44 (0) 1344 317950**

FOLLOW US



centrifys.com/rss



twitter.com/centrifysnews



youtube.com/centrifys



facebook.com/centrifys