



Core Compliance

Access Certification and Compliance Management

Benefits:

- Automate the discovery, analysis and management of user access rights, using business-friendly entitlement descriptions
- Change, disable or delete inappropriate access rights, without requiring a provisioning engine
- Demonstrate compliance with enterprise policy and relevant regulations to auditors, regulators, and other interested parties
- Sensitive data and user activity integration - managers can validate access to sensitive data identified by OLP products, or manage user activity captured by SIEM and other log tools

Identity and access management has become a complex Big Data problem for IT departments. The world of users, identities and access creates a continual demand for identity and access changes throughout the organization as employees move from new hire status to transfer, promotion and termination.

So what happens when the auditors come in for access certification reviews? Are you sure your organization is in compliance? How many users have been added to the enterprise and how many have been removed since your last review? Does audit approval really reduce risk?

Core Compliance is Core Security access certification and compliance management solution for companies seeking to certify and manage employee access rights, ensuring that only the right individuals have access to the right resources and are doing the right things with them.

As the number of users and identities grow and their access needs change, the risk that the business may be compromised by users with inappropriate access rights also grows. Reducing the risk associated with unauthorized access and meeting stringent government and industry regulations is a critical security concern in many industries and this can have tangible top and bottom line implications for your business.

How It Works

Users should not be granted more access privileges than necessary to perform their job or business function. Core Compliance enables authorized business managers to review and certify user access rights using language they understand, and take immediate remedial action when they identify access rights that are inconsistent with policy or regulatory requirements.

Effective access compliance requires three elements:

- **The business context of the user's access rights:** Core Compliance addresses this by providing the ability to translate complex, cryptic or obscure IT entitlements into business-friendly terms familiar to line-of-business managers.
- **Limit access review and remediation to only authorized business users:** Core's technology ensures that business users can only review and manage access rights for personnel who are relevant to them from a compliance perspective.
- **Provide comprehensive, integrated remediation:** Core Compliance provides remediation capabilities, including email notification, help desk trouble ticket creation, or business manager enablement to directly change, disable or delete inappropriate access rights to any enterprise platform or application. Direct interaction with a provisioning platform is not needed. Alternatively, if an organization already has a functioning provisioning solution in place, Core Compliance can leverage that investment, regardless of the vendor provider. Most other access certification products only integrate with a limited set of enterprise provisioning platforms, making the remediation process expensive, cumbersome and difficult to manage.





Features and Benefits

Compliance and Attestation to effectively respond to auditor and regulator demands for data, demonstrating compliance with corporate policies or key industry and government regulations.

Automatic Notifications to notify or periodically remind business managers to confirm user access rights on a schedule or according to company policy.

Business-friendly view of entitlements to confirm or remediate user access rights.

Integrated Remediation initiates corrective actions, without the need to install a provisioning solution.

Comprehensive Data Integration identifies users with access to sensitive data (data loss prevention or DLP) or review prior activity (Security information and event management or SIEM) to ensure compliance with security guidelines, and identifies and remediates segregation of duties (SoD) violations.

Track and store transactions for audit tracking or forensics analysis.

Powerful, interactive worksheets and graphics capabilities to meet the needs of a wide variety of end-users.

“Core’s solution will allow us to manage access controls for all users across a variety of target systems and applications while supporting business operations ...helping us improve compliance, mitigate risk and deliver a streamlined experience to all users simultaneously.”

*— Patrick Kittell Vice President and Chief Security Officer
Universal American*

ABOUT CORE SECURITY

Core Security provides companies with the security insight they need to know who, how, and what is vulnerable in their organization. The company’s threat-aware, identity & access, network security, and vulnerability management solutions provide actionable insight and context needed to manage security risks across the enterprise. This shared insight gives customers a comprehensive view of their security posture to make better security remediation decisions. Better insight allows organizations to prioritize their efforts to protect critical assets, take action sooner to mitigate access risk, and react faster if a breach does occur.

Core Security is headquartered in the USA with offices and operations in South America, Europe, Middle East and Asia. To learn more, contact Core Security at (678) 304-4500 or info@coresecurity.com

blog.coresecurity.com | p: (678) 304-4500 | info@coresecurity.com | www.coresecurity.com

Copyright © 1996-2016 by Core Security Corporation. All Rights Reserved. The following are trademarks of Core Security Corporation “Core Impact”, “Core Vulnerability Insight”, “Core Password”, “Core Access”, “Core Provisioning”, “Core Compliance”, “Core Access Insight”, “Core Mobile Reset”, and “Think Like an Attacker”. The following are registered trademarks of Core Security Corporation “WebVerify”, “CloudInspect”, “Core Insight”, and “Core Security”. The names of actual companies and products mentioned herein may be the trademarks of their respective owners. The names of additional products may be trademarks or registered trademarks of their respective owners.

