CalCom

CalCom Hardening Solution (CHS) for Microsoft System Center

CalCom

CalCom Hardening Solution (CHS) for Microsoft System Center is a server-hardening solution that addresses the needs of IT operations and security teams. The CHS software-based solution implements a proactive, automated hardening approach that ensures that servers are constantly hardened, secured and compliant. The CHS three-step process automates server hardening procedures in a cost-effective fashion, eliminating server down time and configuration drifts.

Key Challenges Solved

Server hardening is critical for protecting against internal cyber threats and ensuring compliance with IT regulations. Server hardening tasks are costly, repetitive, and complicated to manage – for two main reasons:

- **Downtime and testing requirements.** When using manual hardening methods or familiar hardening tools, the hardening process may affect OS or application functionality and cause server downtime. In order to prevent downtime, IT teams spend long hours testing policies in lab environments before deploying them on servers in production environments. Since these lab environments can never fully simulate the production site, a significant number of objects invariably remain unhardened and vulnerable.

- **Configuration drift.** The authorization of multiple privileged users in an enterprise environment makes it difficult to ensure that servers remain hardened. Unauthorized changes by privileged users can expose vulnerabilities, requiring IT teams to repeat the hardening process on a regular basis.

CHS provides hardening for enterprise infrastructures. Whether your organization's infrastructure is deployed in a private, public, or hybrid cloud, CHS hardens policies for a variety of Windows computers.

Features and Benefits:	
Cost-effective hardening process	The CHS pre-enforcement learning mode eliminates the cost of creating lab environments for simulating the impact of security policies on servers. With CHS, the impact is analyzed directly on production environments.
Zero server down time and outage during the hardening process	CHS predicts the impact of a policy on production servers. Visualizing the impact, CHS's smart risk management determines which values will/will not result in server outage when hardened.
One-click rollback procedure	Roll back to any previous policy that was enforced through CHS with a single click.
Simple, single-source hardening management	Simplify administration of enterprise hardening management tasks. All hardening is performed from a single management server. CHS hardens cross-domain environments, DMZs, and workgroups.
Continuous hardening and compliance	CHS enforces server security policies in real time, ensuring continuous policy compliance.
Out-of-the-box security policies	Ensure continuous server compliance with leading hardening standards and customized policies.
Preventive hardening approach	Prevent unauthorized policy changes and data access
Enable broader hardening policies	The pre-hardening learning phase enables IT teams to enforce extensive security policies that eliminate more vulnerabilities and reduce exposure to attacks.
Internal hardening of critical applications	Hardening of the internal configuration of critical applications provides an additional protection layer above and beyond OS hardening.
Audit reviews are no problem	Pass audits with no special preparation. CHS's log of server policy changes provides a complete history of server configuration changes and object access by users.
Leverage your existing SCOM investment	CHS is supplied as a SCOM Management Pack. It uses SCOM agents to perform all learning, enforcement, and rollback activities. Using the existing SCOM infrastructure simplifies the hardening system's implementation, management and configuration.
Compliance reports and dashboards	Gain continuous visibility of server compliance status.

How It Works

CHS implements a three-step workflow for managing and enforcing security policies.
The workflow enhances the server's security while maintaining service availability. The real-time, continuous process ensures that both the operating system and application layers are properly hardened. CHS is managed from the SCOM Operations Console and the CHS Policy Center Console.

The CHS three-step workflow:

Learning Mode:

Save time spent on pre-hardening policy testing and eliminate object crashes using the CHS learning mode. In learning mode, CHS performs automated impact analysis on the actual production servers. Instead of using lab environments, CHS is able to indicate what will be the policy impact on servers in production.
A "gap analysis report" visualizes the future impact of hardening an object on the server's functionality.
The learning mode phase eliminates the need for pre-enforcement policy trial and error. The learning mode phase ensures zero downtime when hardening servers, and reduces the expense of human resources required for hardening tasks.

The CHS learning mode capability:

- Indicates why an object can't be hardened, marks the object, and stores it as an exception.
- Lets you learn on one server and apply the policy to a group of identical servers
- Aids in management of conflicts with Group Policy Objects (GPOs)
- Compares different policies for a single server, allowing you to choose the strictest possible hardening policy that won't affect operations

CHS performs automated impact analysis on actual production systems. This means zero server outage and zero investment of your engineer's time in testing.

01 Discovers the objects' current status – showing their "actual values"

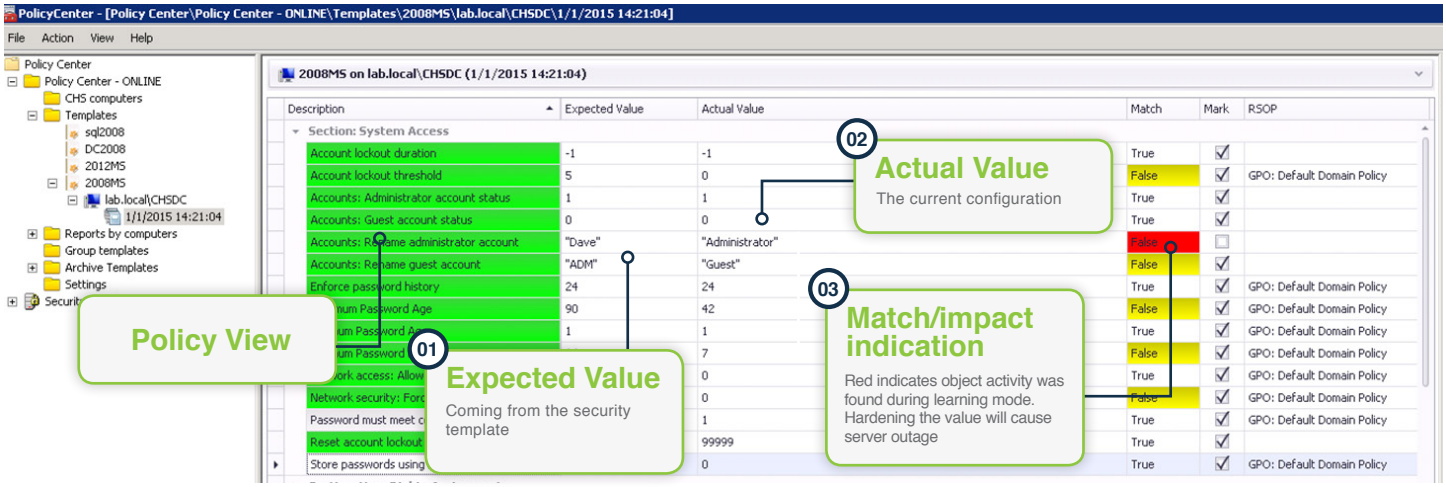
02 Displays the desired policy value

03 Indicates the impact of hardening:

- True: The expected and actual values are identical
- False (yellow): The value will be changed when enforcing the policy – with no impact on server operation
- **False (red): The object is used by the production system and the actual value is valid – therefore, hardening the desired value will cause damage to servers in production**

04 Creates a "ready to go" policy in accordance with the gap analysis report

The screenshot below illustrates the outcome of the learning mode:



Enforcement Mode:

Once the learning mode analysis is complete, CHS enforcement mode implements real-time deployment of the approved security policy. CHS deploys the baseline policy for each server – individually or for a group of identical servers – using templates for the OS and applications. Change management is available in order to quickly perform a policy rollback if needed.

The CHS enforce mode capability:

- Hardens security policies for the OS and applications
- Uses organizational policies for hardening of dynamic processes
- Performs verification, and reports on any changes and errors that occur during the hardening process
- Cross-platform change management: One-click rollback to previous policies. The rollback action can be reviewed in system-generated reports
- Easy policy modification from one centralized dashboard

Monitoring and prevention

CHS provides continuous hardening, monitoring and prevention. The monitoring mode prevents user errors and malicious activity. It provides access control rules that permit only authorized users to change hardening policies. CHS prevents object policy changes, and issues configurable warnings and alerts, in real-time.

The CHS monitoring mode capability:

- Provides real-time prevention of unauthorized changes to hardened servers
- Issues real-time policy violation alerts
- Generates policy violation reports
- Controls access to data and system objects – including files, directories and shares.

CHS automates hardening of Windows operating systems and applications using baseline policies that are created in compliance with leading standards, and that can customized to the needs of the organization.

Windows Operating System Hardening:

Windows Server 2003 (32/64 bit)
Windows Server 2008 (32/64 bit)
Windows Server 2008 R2 (64bit)

Windows Server 2012 (64bit)
Windows Server 2012 R2 (64bit)
Windows Hyper-V

Enforcing a baseline by server roles:

The CHS hardening management platform enables you to drill down to individual servers, so a special policy can easily be created – instead of creating a new GPO every time you want to change a policy. Since special policies are required for different server roles running on different Windows systems, CHS is supplied with deployment-ready policies for a variety of hardening scenarios.

Policies for server roles include:

- Domain controller
- Hyper-V
- Member server
- Print server
- File server
- Application server
- Web server
- Mail server
- Database server
- Terminal server
- DNS/DHCP/Wins server
- Remote access/VPN server

Operating System Hardening Objects:

- Users and groups
- Desktops
- File system: files and directories
- Shares
- Processes
- Registry
- Services
- System
- Devices
- Organizational units
- Group policy objects
- Delegation and security control
- Network settings, ports and protocols (TCP settings, SNMP)
- Terminal Services/RDP/ICA
- Service packs, patches and hot fixes

Organizational hardening policy examples:

- Limit the ability to add, modify, and delete scheduled jobs
- Harden and manage unauthorized application installations on the server (using black/white lists)
- DCOM and COM+ applications
- Metabase and web configuration hardening
- Limit the ability to modify an SSL certificate
- Remove user accounts (authenticated users, everyone) with assigned permissions on a file/directory or network resource
- Harden dedicated devices such as ATMs, security cameras, and public kiosks

Application Hardening

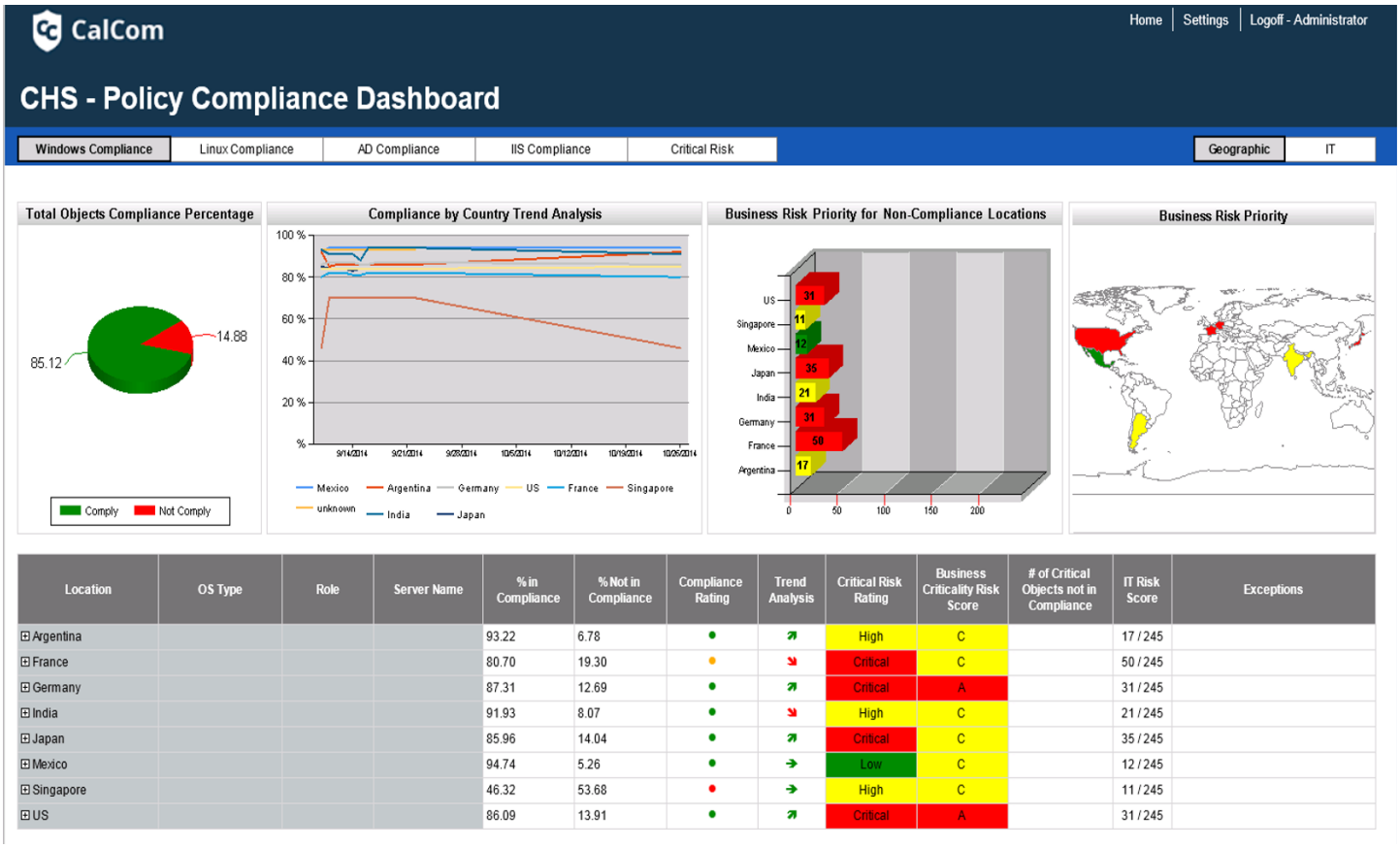
CHS provides internal hardening capabilities for critical applications such as SQL, Active Directory and IIS and more.

CHS Compliance View:

CHS's server compliance reports you visualize your server's compliance status. Based on a simple SCOM Management Pack, CHS provides a continuous compliance view of the OS and applications in the distributed network. Available as a standalone SCOM add-on, or as an integral part of the CHS server hardening suite, it provides cross-platform dashboards and reports that constantly update you regarding changes made to policies or infrastructure.

Whether you have one or several compliance initiatives to respond to, you can use CHS's pre-defined policies, or implement customized policies. With CHS, you can avoid surprises and enhance management and auditor confidence with system-generated reports that provide evidence of compliance testing and results, remediation, and exception management. The CHS compliance dashboard visualizes critical hardening data, providing:

- Unhardened exception values
- The location of vulnerable servers on a geographical or IT basis
- A risk score for the server, helping to prioritize the hardening tasks
- Drill-down to the object level



Location	OS Type	Role	Server Name	% in Compliance	% Not in Compliance	Compliance Rating	Trend Analysis	Critical Risk Rating	Business Criticality Risk Score	# of Critical Objects not in Compliance	IT Risk Score	Exceptions
⊞ Argentina				93.22	6.78	●	↗	High	C		17 / 245	
⊞ France				80.70	19.30	●	↘	Critical	C		50 / 245	
⊞ Germany				87.31	12.69	●	↗	Critical	A		31 / 245	
⊞ India				91.93	8.07	●	↘	High	C		21 / 245	
⊞ Japan				85.96	14.04	●	↗	Critical	C		35 / 245	
⊞ Mexico				94.74	5.26	●	→	Low	C		12 / 245	
⊞ Singapore				46.32	53.68	●	→	High	C		11 / 245	
⊞ US				86.09	13.91	●	↗	Critical	A		31 / 245	