PRODUCT BRIEF

Control Compliance Suite

AT A GLANCE

Control Compliance Suite automates compliance assessments to identity security gaps and potential vulnerabilities.

KEY BENEFITS

- Automatically discover and identify security gaps across your hybrid IT infrastructure
- Measure and track compliance with internal security policies and external mandates
- Prioritize out-of-compliance remediate controls based on criticality and risk
- Address over 100 regulations, frameworks, mandates and best practices

KEY FEATURES

- Automated discovery of assets across network devices, servers, and databases
- Identification of rogue and misconfigured assets and detect security configuration drifts
- Provides policy content and templates to map assets to controls, standards, and regulations

Overview

Security is paramount for every organization. Organizations are under tremendous pressure to secure their customer, financial, and other proprietary data against a burgeoning pantheon of threats. For those that suffer a breach, the repercussions can be costly: fines, increased public scrutiny, decreased customer loyalty, and reduced revenues. But it can be challenging to ensure your organization is efficiently and effectively keeping cyber criminals at bay. Because security gaps due to misconfigurations and unpatched systems have been a critical success factor in many data breaches, organizations are focusing on automating the assessment and remediation of their IT infrastructure to ensure that systems address these gaps and comply with internal policies, best practices, and regulatory mandates.

Symantec® Control Compliance Suite (CCS) addresses this challenge through two modules that can be deployed independently or as a combined solution:

- **Standards Manager** delivers asset auto discovery across network devices, servers and databases, and it assesses the security configuration of these assets. Organizations employ CCS Standards Manager to discover and identify rogue and misconfigured assets, detect configuration drifts, and evaluate if systems are secured, configured and patched according to industry best practices security controls (CIS Benchmarks) or customer security standards.
- **Policy Manager** automates policy definition and policy lifecycle management. Key capabilities include out-of-the-box policy content for multiple mandates and out-of-the-box templates for mapping assets to controls, standards, and regulatory mandates. Customers use Policy Manager to identify common controls across multiple mandates, update the content and technical standards updates on a regular basis, and manage the lifecycle of security policies, standards and controls.

CCS is a highly scalable solution to help identify security gaps and vulnerabilities and automate compliance assessments for over 100 regulations, mandates, and best practice frameworks including GDPR, HIPAA, NIST, PCI and SWIFT.

Secure Configuration Assessment

CCS delivers a comprehensive solution to help identify security gaps and automate compliance assessments through the following features and capabilities:

- **Asset Discovery:** CCS performs a network-based asset inventory to rapidly discover all networks and assets, including managed and unmanaged devices, and it allows for network leak detection. High-speed unauthenticated agent-less network scans help to discover the assets quickly without impacting the network performance.
- **Policy Mapping:** CCS automates policy definition and policy lifecycle management. Leveraging out-of-the-box policy content and templates, administrators can easily map assets to controls, standards and regulatory mandates. This solution can also help identify common controls across multiple mandates, update the content and technical standards updates on a regular basis, and manage the lifecycle of security policies, standards and controls.

CCS leverages these capabilities to support automated assessment of the system security configuration, permissions, patches, and vulnerabilities.

Automated Compliance

CCS uses security content to evaluate compliance of endpoints. Developed by Symantec, this security content comprises technical standards. These standards are based on over 100 regulations, mandates, and best practice frameworks. During assessment, systems are evaluated against these standards to identify if they are secured, configured, and patched accordingly. In this way, rogue and misconfigured assets and configuration drifts are easily detected. Additionally, CCS provides role-based, customizable web-based dashboards and reports that enable the organization to measure risk and track the performance of its security and compliance programs.

Automate Remediation

CCS can also improve your security posture by prioritizing remediation to reduce risk. The solution can help automate the controls remediation, including a closed loop remediation of failing controls by integrating with third-party ticketing systems.

Summary

CCS automates key IT risk and compliance management tasks. The solution ensures the coverage of external mandates through written policy creation, dissemination, acceptance logs, and exception management. It allows customers to link the written policy to specific technical standards to demonstrate compliance to both external regulatory mandates and internal policies. Customers can access these policies using a highly scalable agent-less or agent-based tool. CCS supports automated assessment of the system configuration, permissions, patches and vulnerabilities, and it scores assessment results against specified risk criteria. The solution also includes dashboards and reports to quickly identify and remediate risks.

For more information, please visit:
broadcom.com/products/advanced-threat-protection/control-compliance-suite

BROADCOM
connecting everything®

For more information, visit our website at: www.broadcom.com

CTRL-COMPS-PB101 November 21, 2023