

# Symantec<sup>™</sup> Control Compliance Suite Enforce Database Compliance and Eliminate Drift

# Table of Contents

Data Breach Risk Persists

Symantec Control Compliance Suite

Symantec CCS for Databases

British Computer Society Top Ten: Database Attack Areas

Common CCS Console Views and Details

Synopsis

#### Data Breach Risk Persists

A cursory review of recent data breaches drives home the importance of vigilant data security practices. In 2019 alone more than 4,000 data breach incidents were recorded, and the count continues to increase with every passing year. Data breaches are among the top five common types of cybercrimes in the world. Mega-breaches grab headlines, but hundreds of less familiar data hacks can also increase the risk to an organization.

Data breaches have run at a record pace. Consider these statistics from the first half of 2019:

- **3,800:** The number of publicly disclosed breaches.
- 4.1 billion: The number of records exposed.
- **+54%:** The increase in number of reported breaches versus the first six months of 2018.

Databases are one of the most critical assets of an organization's IT infrastructure and contain a treasure trove of valuable data—often highly sensitive personally identifiable information (PII). They also are an important area of emphasis for compliance programs. Non-compliance with the General Data Protection Regulation (GDPR), even in the absence of any data breach, can be very expensive. Fines for non-compliance can reach up to €20 million in case of an undertaking, and up to 4% of the total worldwide annual turnover of the preceding year, whichever is higher.

As the list of government and industry regulations grows, compliance pressure intensifies on the data stored in corporate databases. With increasing pressure to comply with these regulations, compliance is becoming a significant challenge for database administrators and security practitioners. Data professionals must be more vigilant in protecting company data, as well as monitoring and ensuring that sufficient protection is in place.

Most enterprise core database environments like Microsoft SQL Server and Oracle have the ability to be appropriately provisioned, hardened, secured, and locked down when conducting an initial installation. The challenge is understanding the important components that must be in place. It is not just the database itself; it is the server, the operating system, and the database that reside on it.

Security practitioners must ensure that the basic security practices listed on the following page are followed within an organization to secure databases from data breach and access by unauthorized individuals.

- Ensure the security configuration settings of assets comply with published security standards (Gold Standard) and industry best practices.
- Identify which network devices, servers, and databases are missing critical patch updates and have known default configuration settings and make the appropriate changes.

White Paper

## Data Breach Risk Persists (cont.)

- Ensure a continuous assessment to ensure compliance with your IT security policy and any drift to that policy is addressed on priority.
- Encrypt all sensitive, customer, and internal data with AES. Encrypt all communication links with SSLv3 or TLS.
- Ensure only authorized persons have access to the database and with appropriate access privileges.
- Segregation of duties Ensure that the person in charge of monitoring or auditing the database is not the same whose actions are being monitored.
- Monitoring privileged users Since these users have higher access privileges, special attention may be required on their actions (for database administrators, system administrators, and developers, as examples).

## Symantec Control Compliance Suite

Symantec provides solutions that allow organizations to track the implementation of the practices listed above. Symantec Control Compliance Suite (CCS) is a modular, 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. Symantec CCS rapidly discovers and inventories all networks and assets including managed and unmanaged devices—allowing for assets to be profiled and ranked for risk potential. The solution also provides role-based, customizable web-based dashboards and reports to measure risk and provide a unified view of security and compliance. With CCS, organizations can improve their security posture, prioritize remediation, and reduce risk.

Symantec CCS Standards Manager delivers asset auto-discovery across network devices, servers, and databases and assesses the security configuration of these assets. Organizations employ Symantec 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 customer security standards. These services help the customers achieve the following:

- Automatically discover network devices, servers, and databases across the physical and virtual data center.
- Leverage out-of-the-box templates to map policies, security frameworks, and standards to control statements.
- Automate the collection, aggregation, and normalization of technical security scans across a broad range of physical and virtual assets.
- Identify rogue and misconfigured assets.
- Identify which network devices, servers, and databases are missing critical patch updates and have known default configuration settings.
- Assess that the security configuration settings of assets comply with published security standards and best practices.
- Take advantage of robust asset management and exception management workflows to customize security scans in support of the organization's operational requirements and internal security frameworks.
- Use evidence data from technical, procedural, and third-party security controls assessments to deliver role-based, operational, and mandate-based reports.

#### Symantec CCS for Databases

Symantec CCS provides the most comprehensive coverage of database platforms for compliance scanning. It focuses on key security areas; regulatory compliance, pre-defined standards based on CIS Benchmarks, and a known set of configuration gotchas, including areas related to storage cost savings. The list below is a representation of controls that CCS supports, but by no means is it an exhaustive list of controls that CCS supports out of the box. In addition to the pre-built standards, one can also create custom controls or extend existing controls using the highly flexible framework provided by CCS out of the box.

- Entitlement (relevant for PCI, SOX):
  - Who has access to the grant/revoke/modify functions?
  - Who has direct access to the underlying data (versus using front-end application)?
- Security (CIS Benchmarks):
  - Is auditing/logging enabled and configured?
  - Is backup enabled and configured correctly? (Restore data after ransomware)
  - Are underlying database files adequately protected? (Oracle Configuration Files)
- Configuration:
  - Extraneous/unneeded services are disabled?
  - Are the communications limited and protected? (Database Denial of Service attacks)
- Potential storage cost savings:
  - Are database samples removed?
  - Are database files stored on the correct data volumes?

#### British Computer Society Top Ten: Database Attack Areas

The table below illustrates coverage of CCS controls across common risk areas.

	CCS	for DBs: Key Areas of Co	ontrol
Critical Areas	Regulatory	CIS Benchmarks	Configuration
1. Excessive Privileges	•	•	•
2. Unauthorized Privilege Elevation	•	•	
3. Platform Vulnerabilities			•
4. SQL Injections		•	•
5. Exploiting Unnecessary Services (and functionality)			•
6. Weak Audit		•	•
7. Denial of Service		•	•
8. Database Protocol Vulnerabilities			•
9. Weak Authentication (brute-force attacks)	•	•	•
10. Exposure of Backup Data		•	•

## Common CCS Console Views and Details

**CCS Console View of Support for Different Databases:** A snapshot of different database assets that can be scanned by CCS for compliance.

۲	Symantec. Control	Compliance Suite	<u>Help</u>
Gan Home	Technical Star	idards 🗕	
Asset	Navigation View #	Show Filters V Search standards Q	$\bigcirc$
System	Predefined     B2	Standard C	$\odot$
And Policies	D      Windows		
Jobs L	Þ 💼 MySQL Þ 💼 Oracle		
Remediation	Þ 💼 Sqi Þ- 🍋 Sybase		
Data Integration	⊳ 💼 Unix ⊳ 🚞 Windows		
Reports			
Admin			
ر Settings			

**CCS Console View of Asset Groups:** A snapshot of different versions of supported Oracle and SQL Server assets that can be scanned by CCS for compliance.

٢	Symantec. Control Compliance Suite	What's New!		<u>Help</u>
Gan Home	Assets •			
E	Asset Group Tasks   Common Tasks	<ul> <li>Asset Tasks</li> </ul>	Global Tasks 👻	Assets Q 1 asset(s)/asset group
Asset System	Asset System View	م Assets & Asset Groups	Show Filters 🗸 Search Assets Q	1 asset(s)/asset group
l	- 🏠 All Oracle 10g Databases	Drag a column header here to group by t	that column.	17
Standards And Policies	— 🏠 All Oracle 11g Databases	Name	Type 👁	
:=	- 🍘 All Oracle 12c databases	WIN-OA09V7GD BRT	SOL Server	
:=	- 🏠 All Oracle 18c Databases			
Jobs	- 👔 All Oracle 8i Databases			
Ŗ	- 🏠 All Oracle 9i Databases			
Remediation	- 🁔 All Oracle Databases			
2	- (1) All Oracle installations on UNIX machines			
Data	- (a All Oracle installations on Windows machines	-		
Integration	🔺 🚞 SOL			
L D	- 👔 All SQL Server 2000 Instances			
Reports	- 🍘 All SQL Server 2005 Instances			
0	- 👔 All SQL Server 2008 Instances			
25	- 👔 All SQL Server 2012 Instances			
Admin	- 👔 All SQL Server 2014 Instances			
£03	1 All SQL Server 2016 Instances			
Settings	1 All SQL Server 2017 Instances			
	All SQL Server 2019 Instances	-	A STOCK AND STOCK	

**CCS Console View of Pre-Defined Microsoft SQL Database Standards:** A snapshot of SQL Server CIS Benchmarks supported by CCS for compliance scanning.

Symantec. Control	Compliance S	uite What's New	Neip
Technical Stan	ndards 🧕		
Navigation View 🧧	Show Filters	Search standards Q	
4 🗁 Predefined	St	andard 💿	
Þ 🟫 Oracle	> 🔞 CIS	Benchmark for Microsoft SQL Server 2016 v1.0.0 (Deprecated)	$\odot$
Þ 💼 Sql	Control Compliance Suite     Wars Nee      inical Standards      Show Filters     Search standards      Show Filters     Search standards      Standard      Standardard      Standardard      Standardardard      Standardar		
D 💼 Unix	> 📵 CIS	Benchmark for Microsoft SQL Server 2017 v1.0.0	$\odot$
▷ · 🔂 Windows	> 📵 CIS	Benchmark for Microsoft SQL Server 2019 v1.0.0	
	CIS	Itence Suite       Wint Mee         ds       •         filters       Earch standards         ©       Standard         ©	
	> 📵 CIS	Security Configuration Benchmark for Microsoft SQL Server 2012 v1.3.0	SNer!
	> 📵 CIS	Itance Suite www.www. ds ● Filters ♥ Search standards Q	$\odot$
	Þ 🔞 Sec	urity Essentials for Microsoft SQL Server 2017 (Deprecated)	$\odot$
Technical Standards         Standards			
	Symantec. Control	Symantec. Control Compliance S Technical Standards • Stow Filters • Stow Fi	Symantee: Control Compliance Suite

**CCS Console View of Pre-Defined Microsoft Oracle Database Standards:** A snapshot of Oracle database server CIS Benchmarks supported by CCS for compliance scanning.

0	Symantec. Control (	Com	pliance	Suite Wars New	Help		
6 Home	Technical Stan	ıdar	rds 🤇				
Asset	Navigation View     #       Image: Standards     Image: Standards       Image: Image: Standards     Image: Image: Standards       Image:	w Filters	ilters V Search standards Q				
System	A 📔 Predefined			Standard 🔊			
П	Þ 💼 Oracle	Þ	(1)	CIS for Oracle Database Server 12c v1.2.0			
Standards And Policies	Symantec. Control Con Technical Stands Standar		1	CIS Oracle Database 11g R2 Benchmark v2.0.0			
:=	Þ- 🛅 Unix	Þ	1	CIS Oracle Database Server 11g Security Benchmark v1.0.1			
:=	Technical Star	Þ	1	Security Essentials for Oracle Database Server 18c			
,005	▲      ▲	Þ	1	Security Essentials for Oracle Database Server 19c			
Ŗ							
Remediation							
್ಷಿ							
Data Integration							
D							
Reports							
R							
Admin							
63							
Settings							

**Evaluation Result Details (Overall Score):** A summary of the overall risk score and compliance score along with Asset and other details against a CIS Benchmarks for SQL Server.

۵.				Evaluation Resu	It Details				- 0' ×
File Edit View Help Standard-based view Asset-based view Standard evaluated: CIS Benchmark for Micros Evaluation status: Completed Defender2001328-15	Remediation T	icketing D19 v1.0.0		<b>v</b>	Summary General Risk Score: 7. 0 10 Result summary for	l Standard -CIS Benchmark f	Compliance Score	57.69% 9 v10.0	
Enter search text here Q	r 2019 v1.0.0					57.89%		42.31%	
< m Enter search text here Q Total asset	(s)- 1			>	Check(s) Passed	Check(s) Error	Check(s) Failed	Check(s) Unk	nown
Drag a column header here to group by Asset Name	that column.	▼ # Check in Error	▼ #Unknown	▼ # Not Applicabl	e ⊽ #Passed	Compliance Score (%)	Data Collection Date	V Risk Score	6
WIN-QA09V7GDBRT	11	0	0	5	15	57.69	04-06-2020 12:25:13	7	

**Evaluation Result Details (Surface Area Score):** A drill-down into each section within the CIS benchmark for the overall risk score and compliance score along with Asset and other details.

Evaluat	ion Res	esult Details – 🗖	X
lier Edit View Help ) Standard-based view OAsset-based view Remediation Ticketing tandard evaluated: [CIS Benchmark for Microsoft SOL Server 2019 v1.0.0 valuation status: Completed 04-09-2020 12:25:15	×	Summary         Central           Bitk Score:         Compliance Score           0         10           Result summary for Section -2 Surface Area Reduction	
citer search text here Q  C C5 Benchmark for Microsoft 5QL Server 2019 v1.0.0  C C5 Benchmark for Microsoft 5QL Server 2019 v1.0.0  2 2 Surface Area Reduction  2 2 Forsure Yield Floc Distributed Queries' Server Configuration Option is set to '0'  2 2 15 Ensure Yield Floc Distributed Queries' Server Configuration Option is set to '0'  2 2 15 Ensure Yield Floc Distributed Queries' Server Configuration Option SQL Server instances  2 2 15 Ensure Yield Floc Distributed The Production SQL Server instances  2 2 15 Ensure Yield Floc Distributed text to Yee' for Production SQL Server instances  2 2 15 Ensure Yield Floc Distributed text to Yee' for Server Configuration Option is a set to '0'  2 2 15 Ensure Yield Floc Text to Yee' for Constance I databases	Ē	6922%	
- 2.16 Ensure no login exists with the name 'sa'	>	Check(s) Passed Check(s) Error Check(s) Failed Check(s) Unknown	
Enter search text here Q Total asset(s)-0 Drag a column header here to group by that column. Asset Name V #Failed V #Check in Error V #Unknown V #Not	Applica	cable ♥ # Passed ♥ Compliance Score (%) ♥ Data Collection Date ♥ Risk Score	

**Evaluation Result Details (Auditing and Logging Score):** A drill-down into each section within the CIS benchmark for an overall risk score and compliance score along with Asset and other details.

Eva	aluation Result I	Details			_ 0 ×		
le∽ Edit∾ View≂ Help∽		mmany Connect					
Standard-based view Asset-based view Remediation Ticketing	R	sk Score:		Compliance Score			
andard evaluated: CIS Benchmark for Microsoft SQL Server 2019 v1.0.0	v .	4.5		50%			
aluation status: Completed aluated on: 04-06-2020 12:25:15	R	esult summary for Secti	Ion -5 Auditing and Logging				
nter search text here Q							
SIS Benchmark for Microsoft SQL Server 2019 v1.0.0	^						
🗄 🔯 2 Surface Area Reduction							
🕀 🌄 3 Authentication and Authorization	=	\$0.00% ·					
🛞 😡 4 Password Policies							
😑 😡 5 Auditing and Logging							
– I S.3 Ensure 'Login Auditing' is set to 'failed logins'	-	Check(s) Passed	Check(s) Error	Check(s) Failed	Check(s) Unknown		
III III III III III III III III III II	>						
nter search text here Q Total asset(s)- 0							
Prag a column header here to group by that column.					i		
sset Name	# Not Applicable	▼ # Passed ▼ C	compliance Score (%) 🛛 🛛	Data Collection Date 🛛 🛪 Ris	sk Score		

**Integrated Remediation Tracking Through Third-Party Ticketing System:** An automated ticket based on the assessment results can also be created using CCS in a third-party ticketing system and tracked in the CCS console. A workflow is provided to configure the integration with a third-party ticketing system.

**CCS Console View for Configuring Automated Ticket Creation:** A view of the steps and workflow for integration with third-party ticketing systems.

Select Standards	Enable Automatic Remedia	tion Ticketing	On On
Select Assets	Select Ticket Type	Remediation Ticket Type ServiceNow closed-loop remediation	
Schedule Job			
Select Report Templates	Select Asset Types	<ul> <li>✓ Cisco Router</li> <li>✓ DB2 Databases</li> <li>✓ Devices</li> <li>✓ Edge Server MS-Exchange</li> </ul>	
Advanced Settings		<ul> <li>ESM Agent (Deprecated)</li> <li>Exchange Server</li> <li>IIS Virtual Directory</li> </ul>	
5.1 Remediation Ticketing		<ul> <li>IIS Web Site</li> <li>MS-Exchange Administrative Groups</li> <li>MySQL RDS Instance</li> </ul>	
i.2 Result Viewers		<ul> <li>Oracle Configured Databases</li> <li>Organization MS-Exchange</li> <li>SQL Database</li> </ul>	
.3 Export Report		SQL Server SYBASE Servers Unix DB2 Database Unix DB2 Database	
.4 Notification Details		UNIX Machine     UNIX MariaDB Servers     UNIX MySQL Servers	

**CCS Console View for Tracking the Ticket Status:** A view of the CCS console that is used to track the status of the automated tickets created by CCS.

sate Remediation Ticket											
vanced Search	7 Tickets View	N									
Apply 🕑 Rever	t Enter sea	arch text Q	1 native ticket(s) (L	ast Monitored - 08-06-2	020 17:21, Next Sc	heduled Monito	ring - 09-06-2020 05:	21)		(	
reated on	Drag a colu	mn header here to g	roup by that column.								
All     Before		Ticket Number	Created on	Assigned to	Modified on	Priority	Status	External Ticket Nu	ımber		
01.05.2017.00:00	- 🖉	INCA000001	08-06-2020 21:5		08-06-2020 21:5	Moderate	Open	Not Available			
After	- 1										
01.05.0017.00-00											_
Retwoon	Preview										-
between	-							🕒 Save	C Revert	C Refresh	
01-05-2017 00:00											
01-05-2017 00:00	[	Details	N doL	lame: Not Applicable (Ma	nual)						
				Enter search text here	Q						
			Che	ack Name			Asset Name				
O. Balance			Citt	Connonic			Assectionite				

## Synopsis

Symantec CCS offers the leading market solution for database security and compliance. It covers the entire lifecycle: from scanning the database for potential misconfiguration and drift from well-defined policies and CIS benchmarks to closing the loop with tracking the progress of remediation through integration with third-party systems. CCS offers comprehensive coverage of various database platforms that is continuously updated with the latest security controls from CIS and, combined with other security solutions from Symantec, ensures that critical data is protected from unauthorized access by malicious actors. Learn more.



For product information and a complete list of distributors, visit our website at: broadcom.com Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. Broadcom, the pulse logo, Connecting everything, and Symantec are among the trademarks of Broadcom. SED-DCCCS-WP100 July 15, 2020