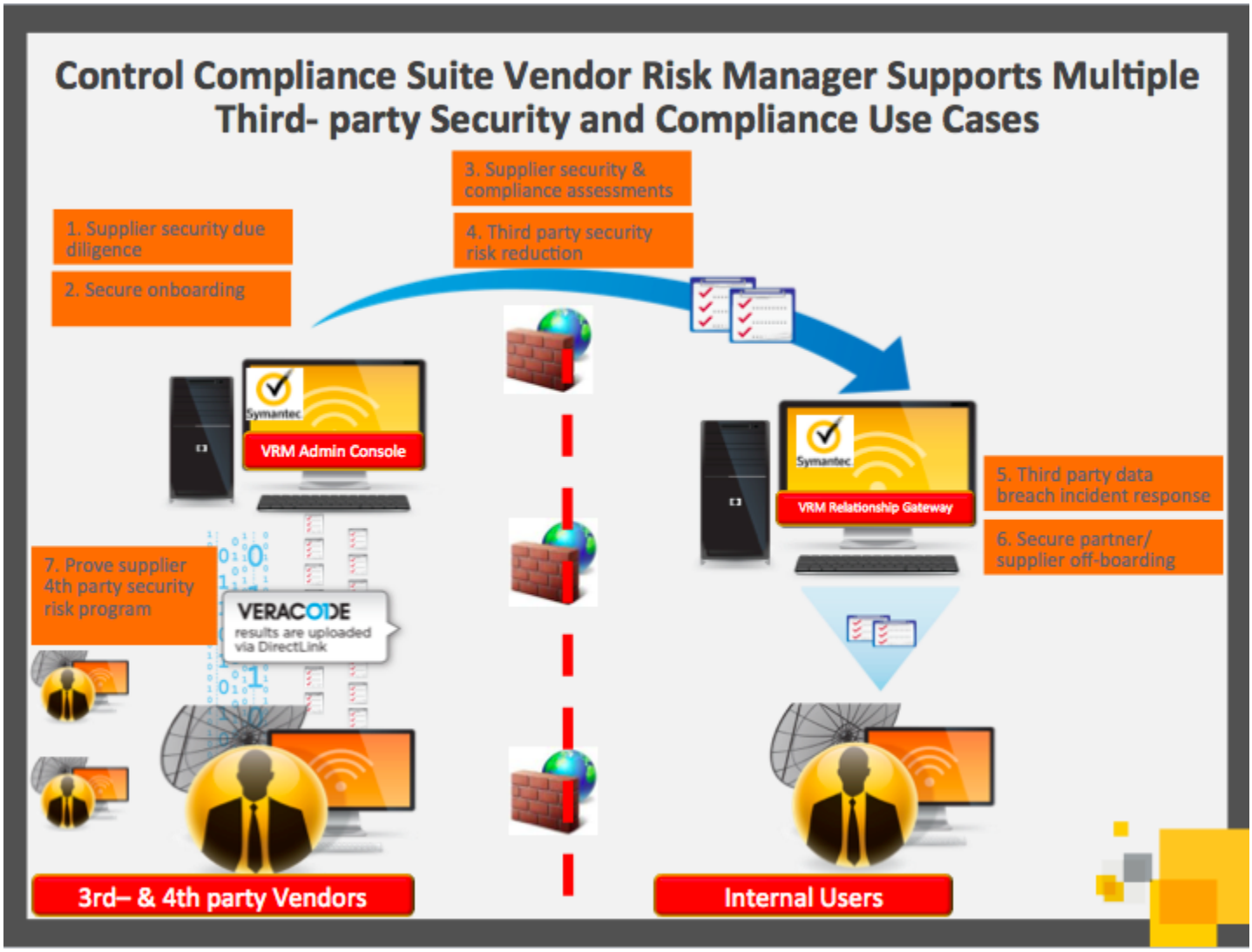
DATASHEET CONTROL COMPLIANCE SUITE VENDOR RISK MANAGER 11.1

Continuously Assess, Monitor, & Secure Your Information Supply Chain and Data Center

Data Sheet: Security Management



Is your organization able to:

- Demonstrate an effective vendor security risk management program to your auditors, regulators, and customers?
- Assess the application security posture of third-party applications and IT services that are being used by your organization, including private, hybrid, and public cloud infrastructures?
- View the dependencies and assess IT security risks across multiple vendor, software, and service provider/IT outsourcing relationships across your information supply chain?
- Provide mandate-based reporting on third-party security compliance requirements such as PCI DSS 3, HIPAA Omnibus, CFPB, and OCC Guidelines?

- Automate best practices for the secure onboarding of business partners and suppliers in your information supply chain ecosystem?
- Demonstrate to your regulators and auditors that your service providers and third party relationships are managing their own third-party vendor security risks?

Solution Overview

Enterprise data centers today have increasingly fluid perimeter security infrastructures.

- Many businesses rely on third parties to enable some of their most critical business activities. These partners and vendors often access sensitive business data such as customer and employee personally protected data (PII and PHI) and confidential intellectual property.
- These partners, in turn, may also be sharing sensitive information and critical processes with their own third parties and business partners.
- In addition, enterprises today are increasingly using public cloud and third-party collocation facilities to augment their on-premise data center resources.

Outsourcing business activities and infrastructure, and automating transactions and business processes across its partner ecosystems present opportunities for business to realize cost efficiencies and enhance their agility. However, suppliers and business partners also present new vectors of risks.

An organization may have stringent data security practices in place, but their suppliers and business partners may not exercise the same due care. Malicious entities are very much aware of these potential weaknesses in a business's information supply chain and are constantly looking for ways to exploit these security gaps. Regulatory and legal standards have made it quite clear that outsourcing processes and infrastructure does not transfer risks to the service providers.

At the end of the day, the onus to protect and secure information remains with the business. Recent regulatory and standards developments, such as those stipulated in the new PCI DSS 3, HIPAA Omnibus Rules, and the CFPB and OCC Guidelines, are also expanding the scope of business partners and suppliers that must be managed for risk to include cloud service providers, third party application developers, and even physical service suppliers that have access to sensitive and protected information systems. An effective vendor risk management program is based on a process that enables a business to manage, mitigate, and remediate potential business disruptions and information loss stemming from the employment of service providers and IT suppliers.

Symantec Control Compliance Suite Vendor Risk Manager (Symantec CCS VRM) delivers the technology that enables security and compliance managers the ability to understand the risks associated with its partner and supplier ecosystems. CCS VRM automates key processes for addressing security and compliance requirements, enables the business to identify, assess, and plan for mitigating security risks associated with third-party relationships.

Symantec Control Compliance Suite Vendor Risk Manager automates many of the tasks associated with the vendor security risk management process, including variable scoping and tiering of vendors, creating assessments and standards and/or mandate-based reports, vendor response tracking and reminders, evidence collection, evidence risk analysis, email notifications to stakeholders, and scheduling. Symantec Control Compliance Suite Vendor Risk Manager provides an inventory of third parties (services and applications) and a catalog of third-party security risks. Customers are able to segment their vendors according

to the criticality of the business processes, technology, and IT services they provide and according to the security profile of the information that they access or manage.

CCS VRM enables businesses to tier vendors and partners according to their importance and potential risk to the organization. Rule-based security assessments are designed so that the most critical and high-risk tiers have the most rigorous evaluations. The solution manages each vendor independently, offering customers the ability to understand the impact of doing business with each contributor in their information supply chain. The combination of procedural and application security assessments enables a more comprehensive view of the third party's relevant security and compliance posture.

Symantec Control Compliance Suite Vendor Risk Manager is an integrated solution comprised of the components for meeting your third- party risk management needs. Included in this solution are the Symantec Control Compliance Suite Vendor Risk Manager Administrative Console, the Symantec Control Compliance Suite Vendor Risk Manager Relationship Gateway, the Symantec Control Compliance Suite framework, and assessment content from Shared Assessments.

What's New in Control Compliance Suite Vendor Risk Manager 11.1?

Control Compliance Suite Vendor Risk Manager 11.1 includes several new product capabilities:

- **VRM Dashboards** – New VRM dashboards allow VRM administrators to drill down and filter larger datasets. VRM dashboards are available for the following categories: Overview, Risk Management, and Workflow.
- **VRM Risk Score Cache** – In-memory caching of VRM Risk scores to improve UI responsiveness and facilitate faster dashboard loading for very large data sets.
- **VRM Scheduler Service** – The scheduler service is responsible for all scheduled VRM job management.
- **Support for Prevalent Vendor Threat Monitor**. Integration with VTM enhances VTM visualization for risk and event data in the vendor tab.
- **Survey Editor** – OCIL 2.0 based survey editor is available in VRM Console and allows VRM administrators to create, modify, and test surveys before assigning to evidence sources. Survey editor supports import of OCIL 2.0 surveys as well as custom extensions to the OCIL schema for risk scoring and VRM risk areas. Surveys can also be exported to OCIL (XML), Excel, and synchronized with CCS AM.
- **Flex Form Evidence Source** – the Flex Form evidence source allows VRM administrators to define specific forms and fields for evidence collection and review. Field types are define and input is assign to task assignee or risk reviewer. This is effective for document and contract management.
- **Summary and Detailed Assessment Reports** – VRM administrators can generate summary and detailed reports for a VRM assessment. The report contains scope, risk, evidence, and review details about assessment.
- **RACI Graph** – implemented a RACI graph for relationship responsibilities and activities. This allows VRM administrators the ability to understand who is responsible for activities related to a relationship.
- **Extended Language Support** – added Console and Gateway UI language support for German, French, Spanish, Portuguese, Korean, Traditional Chinese, Simplified Chinese, and Russian.

Control Compliance Suite Vendor Risk Manager Standard Features

Control Compliance Suite Vendor Risk Manager enables you manage the risks posed by your third party business process services, application developers, and cloud service providers by automating security and compliance assessments:

- Leverage Shared Assessments content for controls-based security risks assessment of third parties.
- Deploy a centralized, Web-based repository to manage the vendor assessment process and collection of evidence data.
- Display evidence requests and the status of those requests in a single management interface.
- Enable third-party providers to route requests to appropriate process, data, and system custodians within the vendor organization.
- Enable variable scoping, thus allowing the customer to scope/add multiple vendors, software, and service solutions into a single relationship assessment.
- Auto-calculate vendor risk scores based on multiple evidence sources, and enhance risk scoring by enabling risk weighting by risk areas.
- Integrate with the rest of the Control Compliance Suite applications to offer advanced compliance reporting, dashboards, and analytics, which customers can utilize to support risk remediation, operational alignment, and business planning activities.
- Create and evaluate vendors based on tiers as defined by their importance and potential risk to the organization.
- Provide industry-standard SCAP OCIL 2.0 questionnaire support.
- Integrate directly with Veracode to automate third-party application scanning of application developers and cloud service providers. Application providers are able to upload scan results directly from Veracode via the Symantec Control Compliance Suite Vendor Risk Manager Relationship Gateway. Customers can also manually upload application security reports based on their application security program.

Customer Benefits

Control Compliance Suite Vendor Risk Manager offers the following customer benefits:

- Identify and assess the risks posed by your suppliers and business partners to the enterprise's cybersecurity and data center security operations.
- Demonstrate an effective vendor risk management program to your auditors, regulators, and customers.
- Enhance the ability to monitor your risk posture by continuously assessing your third party service provider's relevant IT security policies, procedures, and web application security.
- Support planned third party cloud and software-defined data center migration by providing a hub for conducting due diligence on the security and compliance standards of cloud service providers, managed service providers, and third party application developers.
- Support regulatory requirements for vendor monitoring, and better identify potential risks before they become legal liabilities to the business.
- Receive notifications of potential data breaches without being dependent on your third-parties.
- Clearly communicate accurate and up-to-date vendor risk information to executives on short notice.
- Realize operational efficiencies and scale your vendor risk management program.
- Leverage this evidence-based approach to enable more informed business decisions during the vendor selection process.
- Leverage vendor risk assessment information to facilitate internal cross-functional collaboration and manage third-party related incidents.

- Employ vendor risk information to create internal security checklists for on- and off-boarding third party business partners.
- Support internal processes and standards for addressing and responding to third party data breaches.
- Leverage variable scoping to view and assess risks for individual relationships, as well as assess risks across the entire information supply ecosystem.

Overview of Control Compliance Suite

Symantec™ Control Compliance Suite (CCS) is a modular, highly scalable, and comprehensive solution for automating security and compliance assessments across the physical and virtual data centers, and across public clouds. Security and IT Operations Managers utilize CCS to enable basic security hygiene protocols and prioritize security remediation; while Compliance and IT Risk Managers leverage CCS to enable compliance assessments and reporting, IT security risk assessment, and IT security risk reduction. Symantec Control Compliance Suite (CCS) is part of the Symantec Data Center Security product family.

Each of the Control Compliance Suite Modules is available independently or as part of the broader CCS suite. Control Compliance Suite combines evidence from the multiple modules as well as third party systems, and maps assets and evidence to control statements, standards, and policies and regulations to enable mandate-based reporting and risk assessments. Role-based, customizable Web-based dashboards, and reports enable the organization to measure risk and track the performance of its security and compliance programs. Workflow integration with remediation ticketing systems enable organizations to align security operations with compliance and risk management operations, prioritize risk mitigation and remediation activities, and optimize security and IT operations.

Symantec™ Control Compliance Suite-Modules

Symantec™ Control Compliance Suite Standards Manager is a leading asset discovery and configuration assessment solution. Standards Manager is employed to facilitate the hardening of both physical and virtual infrastructure, detect configuration drifts, and evaluate if systems are secured, configured, and patched according to standards for security operations and compliance reporting.

Symantec™ Control Compliance Suite Risk Manager aligns security and compliance operations with business priorities by defining risks according to business thresholds, mapping risks to assets, controls and owners, calculating risk scores. This information can be used to prioritize resource allocation, enable alignment of security operations with compliance, and prioritize risk mitigation and remediation. Customers also utilize Risk Manager to measure and track the performance of its compliance and risk reduction programs.

Symantec™ Control Compliance Suite Policy Manager automates policy definition and policy life cycle management with out-of-the-box policy content for multiple mandates, automatically maps assets to controls, standards and regulatory mandates, identifies common controls to enable “assess once and report to multiple mandates”, and delivers content and technical standards updates on a quarterly basis.

Symantec™ Control Compliance Suite Assessment Manager automates the assessment of procedural controls governing employee behavior. Assessment Manager offers out of the box, comprehensive coverage for 100+ regulations, frameworks & best practices that are translated into questionnaires to assess the effectiveness of procedural controls. These questionnaires can also be used to evaluate overall employee security awareness and to support security awareness training.

Symantec™ Control Compliance Suite Vendor Risk Manager enables the assessment and monitoring of your vendor risk exposure including third party business process services, application developers, and cloud service providers by automating security and compliance assessments.

More Information

Visit our website

http://enterprise.symantec.com

To speak with a Product Specialist in the U.S.

Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses, and governments seeking the freedom to unlock the opportunities technology brings—anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company operating one of the largest global data intelligence networks, has provided leading security, backup, and availability solutions for where vital information is stored, accessed, and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2014, it recorded revenue of $6.7 billion. To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.

Symantec World Headquarters

350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

21347667 02/15