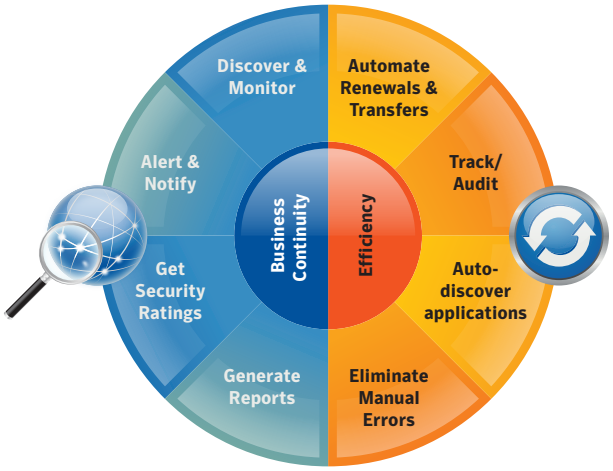
Symantec™ Certificate Intelligence Center 2

Datasheet: Symantec™ Complete Website Security Discovery and Automation

Overview

The deployment and adoption of cloud, virtualization, big data, mobile, and social media applications in recent years have increased demand for SSL certificates. Google, a popular search engine, boosted rankings for organizations that implemented always-on SSL to secure user experience from start to end on their websites. As more and more SSL certificates are deployed to secure transactions and information, the management of SSL certificates becomes more challenging. This is especially true in a mixed environment where SSL certificates are from different Certificate Authorities (CAs) or include self-signed certificates.

Without proper certificate management, organizations could have expired or non-compliant SSL certificates. This situation could adversely affect business continuity and erode brand value. A robust, easy-to-use SSL certificate management system could help an enterprise avoid the consequences of loss of business, productivity, non-compliance, and risks of security breach.



Leverage SSL certificate discovery, monitoring and risk assessment for business continuity and industry compliance

Automate SSL certificate lifecycle management to increase resource efficiency

Discover and monitor all SSL certificates to help avoid certificate expiration

Expired, high-risk, rogue or unknown certificates could adversely affect business and erode brand value. In a U.S. consumer study[1], ninety one percent of respondents will not continue a transaction if they see a browser warning page on the SSL security of a website. Symantec Certificate Intelligence Center

[1] Based on Symantec Online Consumer Study, November 2013

Key Benefits

Increase Operational Efficiency

- Automate lifecycle management including installation and renewal
- Automate upgrades from non-Symantec to Symantec Certificates

Maintain Business Continuity

- Receive notifications, alerts, reports on all SSL certificates, including self-signed certificates, and from any Certificate Authority
- View summary and detailed information on all SSL certificates using a central dashboard

Mitigate Security and Non-compliance Risks

- Catalog and monitor all SSL certificates
- Get security and compliance rating, as well as recommended actions on all SSL certificates based on industry best practices and standards

Leverage Best-in-Class Service

- Leverage a proven, global PKI infrastructure with 100 percent uptime since 2004
- Scan from tens to thousands of servers across large networks by leveraging a distributed and high-performance architecture
- Leverage a configurable system and avoid customization to enhance business agility
- Use innovative mobile extension of the system to quickly identify and remediate potential issues

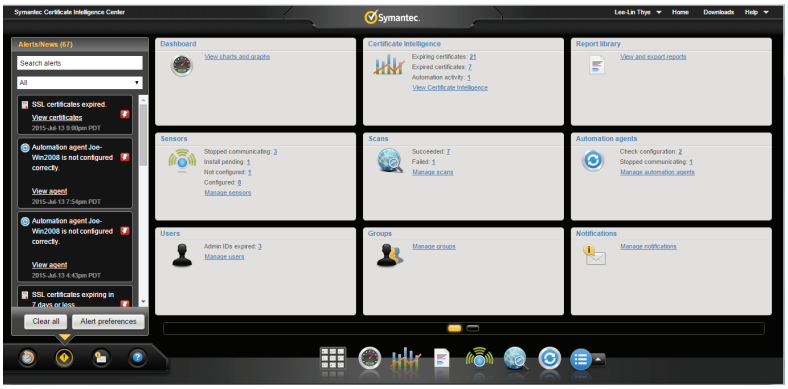
Symantec™

Norton™ SECURED
powered by Symantec

cloud-based service helps organizations have central control over all their SSL certificates. Administrators can get summary and detailed information via a central, easy-to-use dashboard. Notifications, alerts and reports help facilitate timely interventions to prevent business disruptions.

Assess compliance status and security risks

Industry standards and best practices, for example SHA-1 deprecation, are constantly evolving to help organizations stay ahead of cyber threats. In addition, hard-to-discover critical vulnerabilities such as POODLE add to the challenges of securing the SSL environment. This fluid and dynamic environment creates challenges for organizations to monitor and maintain compliance for all SSL certificates at any given time, including self-signed certificates, and certificates from any CAs. Symantec Certificate Intelligence Center helps discover, catalog and assess the compliance and security of all SSL certificates so that organizations can mitigate the risks of non-compliance and incompatibility with industry best practices and company's policies. Standard and customized reports provide visibility to administrators, users and other stakeholders including security ratings on all SSL certificates help administrators ensure that all SSL certificates in the organization are compliant with corporate policies and industry standards.



Easy-to-use dashboard provides administrators quick access to perform SSL certificate lifecycle management

Automate SSL certificate lifecycle management to increase operational efficiency

Organizations are facing increasing demand for their IT services to manage industry trends that add to the complexity of their environments. At the same time, budgets are constrained and resources are reduced or have remained the same. Symantec Certificate Intelligence Center end-to-end SSL certificate lifecycle management includes automation of manual, routine actions that helps ensure efficiency, consistency and accuracy. As an example, SHA-1 and

Key Features

- Cloud-based, and easy-to-use dashboard with summary and detailed views
- Configurable and high-performance scanning
- Large selection of templates for executive and operational reporting
- Configurable notifications and in-console alerts
- SSL security ratings and recommendations based on industry best practices
- Detailed reports and audit trails for accountability and compliance verification
- Automated lifecycle management including SSL certificate installation and renewal
- Agent and agent-less deployment options
- Support for major servers and load balancer platforms including Apache, Microsoft®, F5®, A10 AX and Thunder Series ADC, and Citrix®
- Robust and scalable service to manage from tens to thousands of SSL certificates
- Symantec Certificate Intelligence Center for Mobile available on the Apple iPad® for instant access to Symantec Certificate Intelligence data
- Available for Symantec Managed PKI for SSL customers

SHA-2 end-entity certificates can be automatically chained to SHA-2 intermediate certificates. This capability allows IT teams the time to focus on other mission-critical tasks while providing auditable records for accountability. In addition, administrators could run automated upgrades of non-Symantec to Symantec SSL certificates allowing management to further streamline the SSL environment and take advantage of vendor consolidation. Symantec, the leading source of trust online, Symantec SSL Certificates secures 91% of Fortune 500 companies.[2]

Deliver SSL Security, Always

Organizations rely on SSL certificates to protect information and assure customers of their authenticity. Maintaining a secure environment with 24x7 SSL protection requires a dependable and scalable certificate management service. Symantec Certificate Intelligence Center enables enterprises to deliver SSL protection and trust, always. Symantec was the first Certificate Authority to provide commercial SSL protection with their military-grade infrastructure. 94 of the 100 largest financial institutions worldwide are secured by Symantec SSL[3]. Easy deployment, configurable controls, and fast scanning are capabilities ideal for large and growing organizations. In addition, Symantec Certificate Intelligence Center for Mobile, the first mobile capability for SSL certificate management, provides actionable intelligence anytime, anyplace.

Symantec Certificate Intelligence Center lets administrators track SSL certificates anyplace, anytime

[2] Includes Symantec subsidiaries, affiliates and resellers. Based on internal customer analysis, July 2013 against Fortune 500 2013 list

[3] Based on Forbes Global 2000 list published in 2013 and internal customer analysis conducted in July 2013

Symantec™

Norton™ SECURED
powered by Symantec

More Information

Visit our website

North America: http: //go.symantec.com/CIC
EMEA: http://www.symantec.co.uk/certificate-intelligence-center
APAC: http://www.symantec.com/en/aa/ssl-certificates/certificate-intelligence-center

Follow us on Facebook
Chat with us on Twitter @nortonsecured
Join the discussion at Website Security Solutions Forum

To speak with a Product Specialist

North America:	+1(866) 893-6565 or +1(520) 477-3135	SSL_EnterpriseSales_NA@symantec.com
U.K. and Ireland:	+0800 032 2101	sslsales-uk@symantec.com
Rest of EMEA:	+353 1 793 9053 or +41 (0) 26 429 7929	sslsales-ch@symantec.com
Asia Pacific:	+61 3 9674 5500	ssl_sales_APAC@symantec.com

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

To speak with additional product specialists around the world, visit our website for specific offices and contact numbers.

About Symantec

Symantec protects the world's information and is the global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device to the enterprise data center to cloud-based systems. Our industry leading expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at: go.symantec.com/socialmedia.

Symantec Corporation World Headquarters

350 Ellis Street
Mountain View, CA 94043 USA
1-866-893-6565
www.symantec.com

Symantec

Norton SECURED
powered by Symantec

UID: 140/05/15