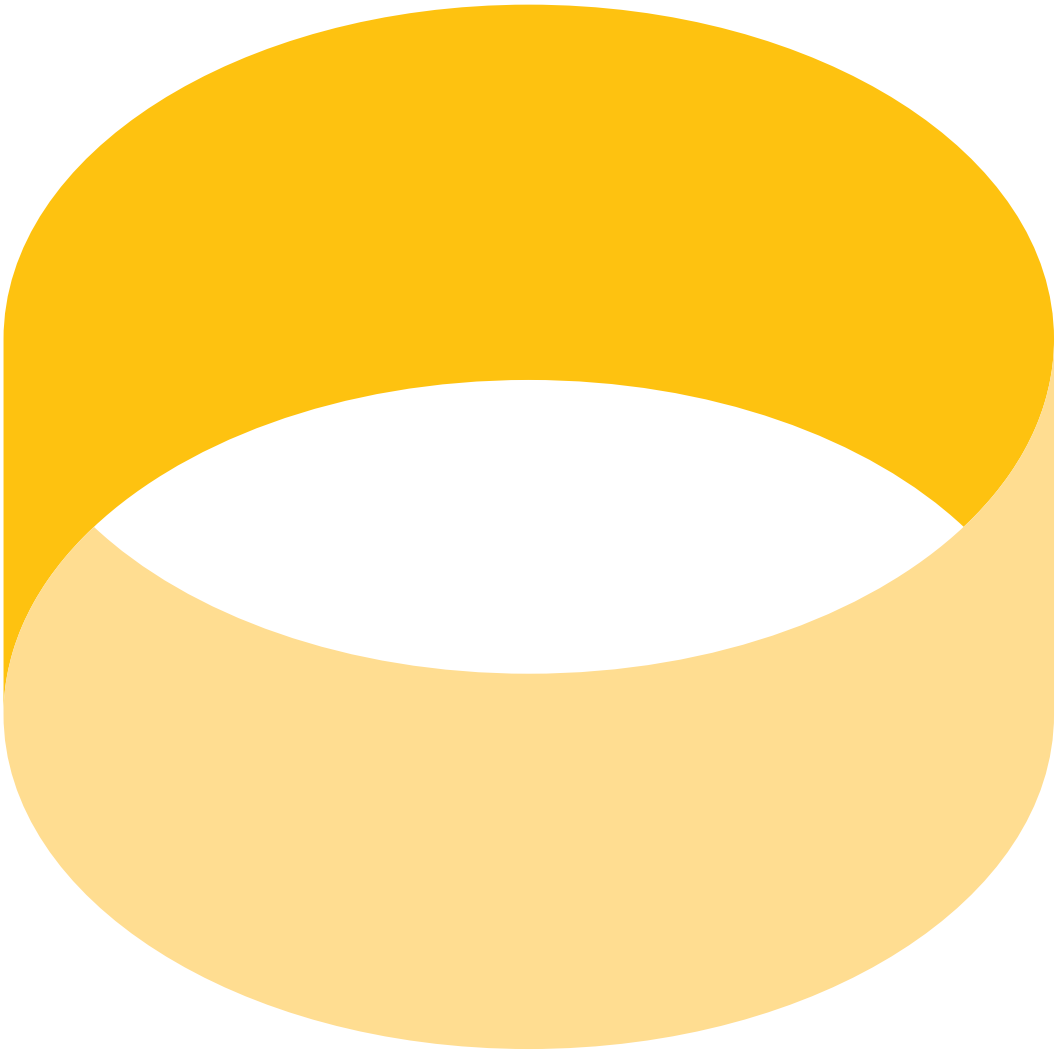


Asset Discovery with Symantec Control Compliance Suite

WHITE PAPER

Who should read this paper:

- IT Operations
- IT Security

Symantec™

Abstract

"Know Your Assets, Know Your Risk".

A robust and easily managed host discovery schedule provides for continuous visibility of both authorized and unauthorized assets.

Symantec Control Compliance Suite Standards Manager (Symantec CCS SM) features asset discovery, which rapidly discovers and inventories all networks and assets, including managed and unmanaged devices, and allows for network leak detection. This patented technology helps discover the assets quickly without impacting the network performance. Its seamless integration with other modules of Control Compliance Suite (CCS) helps offer a complete and comprehensive security assessment and compliance solution.

Security Challenges in the Modern Data Center

For IT security professionals today, the pace of change has accelerated dramatically. Trends such as virtualization, cloud computing, and the use of consumer mobile devices raise new security challenges every passing day.

Gone are the days when IT departments could afford to take days and weeks in provisioning hardware and deploying applications. Today businesses need to be able to quickly respond to customer needs. The promise of elasticity in scaling up and down the infrastructure

is underpinning the emergence of software defined data centers. As a result, Business Unit Owners want their application workloads provisioned and made available for production use in minutes and hours rather than days and weeks. While customers increasingly utilize public clouds (like AWS) and continue to build out their data centers into software-defined environments, they still need to maintain the security and compliance posture of their existing legacy virtual and physical environments. Basic security hygiene requires that customers have continuous visibility on their networks and assets, detect rogue and misconfigured assets, and correlate this with information about vulnerabilities and threats in the environment.

The following developments also contribute to the complex data center security challenges customers face today, and underscore the need for fine-grained visibility into the assets and its security posture:

- The current Internet security threat landscape continues to evolve in both volume and complexity of attacks. The level of sophistication of new attacks is unprecedented. The market for intellectual property and access to critical infrastructure, as well as personally identifiable information (PII) and payment card industry (PCI) credentials, is well established.
- The new virtual, cloud and mobile technology platforms force IT to carefully balance enhanced agility, potential ROI, and manageable risk.
- The proliferation of virtual machines creates a new problem for IT – how to ensure that every instance is compliant with security policies, controls, and regulations. Virtualization adds a whole new layer of infrastructure for the assignment of software patches and updates, security configuration standards, technical controls, user permissions, exceptions, and audit requirements.

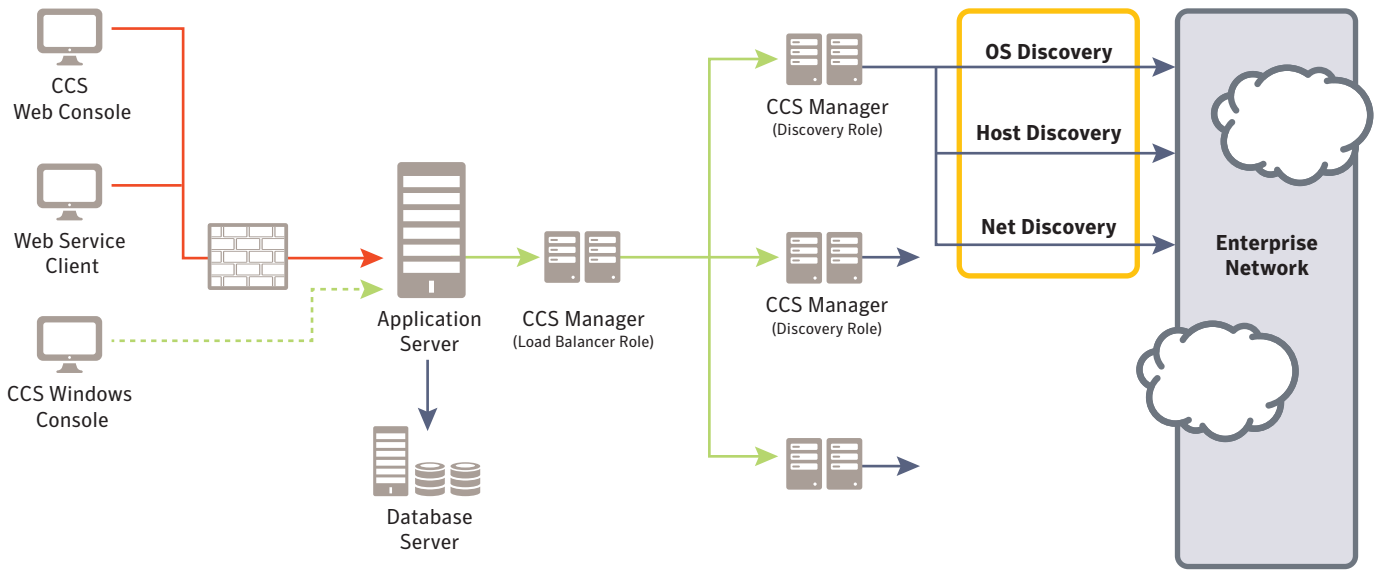
The Need for Fast, Continuous and Accurate Discovery of Assets

With the proliferation of virtualization, it is common for employees to spin off new applications using homegrown virtual machines. Open source applications, wikis, and databases spring up on new virtual machines and IT, more often than not, is caught off-guard. Since these applications are under the radar, these virtual machines are not included in normal patch cycles and protection updates and therefore vulnerable to attack.

This problem of 'under the radar' IT systems is not limited to virtual environments. There are many occasions where network administrators get surprised after running discovery tools to identify even subnets that are unknown to them.

In these scenarios, an effective asset discovery process always forms the first critical steps towards managing security risk and compliance. An effective asset discovery process must exhibit the following characteristics:

Scalable Architecture



Comprehensive

Asset discovery cannot rely on the existing inventory or scans of only "known" networks, but must also discover rogue and unmanaged assets.

Non-Intrusive

Asset discovery must be agent-less in order to run continuously without impacting the network and applications.

Fast and Accurate

Asset discovery must be incorporated as a continuous process, which requires speed. The solution should also provide the highest accuracy possible.

Flexible

IT Admins should be able to schedule the discovery scans the way they want, based on geographies, networks, scan time, etc.

Integrated

Asset discovery must be capable of integrating with downstream activities such as Vulnerability, Configuration, and Policy management.

What Makes Symantec's Asset Discovery Highly Efficient?

Knowing your network, and what assets are connected to the network, is essential to identify, prioritize, and mitigate security risks. The Asset Discovery feature in Control Compliance Suite Standards Manager performs a network-based network and asset inventory via high-speed unauthenticated agent-less network scans, delivering the data to the Control Compliance Suite asset system for automatic asset classification and categorization.

Patented Approach that is Light on Resource Consumption and Quick In Discovery

Symantec uses its patented approach, which optimizes the utilization of network connections. It offers many advantages, such as:

- **Parallel communications**, resulting in the virtual elimination of time wasted in waiting for replies when communicating with multiple computers.
- **Less memory consumption** through the elimination of a separate process for each session.
- **Less processor utilization** through the elimination of a separate process for each session.
- **Reduction of port consumption** from many to one, resulting in more available resources.

Cover All the Bases

Using the discovery capabilities in CCS, users can get an entire view of their data center deployment across their entire stack.

Network Discovery

The Network Discovery capability enables the discovery of all the subnets in the data center. This helps identify all the hidden subnets with the data center.

Asset Discovery

Once the subnets are discovered, CCS helps in discovering all the hosts / endpoints within each of these subnets. Using the light speed technology, the discovery of hosts is fast and lightweight on the network. One can scan a Class C subnet in a little over 10 seconds.

Unified View

CCS provides capabilities to tie this data to other data sources like Symantec's DLP, Symantec Data Center Security:Server Advanced (formerly branded as Critical Systems Protection), and Symantec Endpoint Protection (SEP), as well as third party data from NESSUS, Red SEAL, etc. to give a complete operational risk posture within your environment.

Integrated Solution that Assesses Configuration Risk and Security Compliance of Discovered Assets

CCS automatically identifies and catalogs global networks, hosts, and operating systems. These discovered assets are then added to the extremely feature-rich Asset System of CCS. The integrated modules of CCS then take over from there and offer comprehensive Security Compliance Monitoring and Risk Assessment on the discovered assets.

Highly Scalable, Customizable & Distributed Architecture

Today's IT environments are highly distributed across multiple sites and geographies. CCS has been architected by keeping in mind the large scale and complex deployment scenarios. CCS scales up easily to more networks as they are discovered.

CCS offers a very flexible way to discover assets. You can schedule the asset discovery operations by network, business assets, or time.

To give complete control to the administrator over the discovery process, CCS includes network/subnet blacklisting & bandwidth throttling ability. It also provides full-featured role-based access control support.

Summary

IT Security Professionals today face daunting security challenges due to rapidly changing IT environments and complexity of attacks. In these scenarios, effective asset discovery forms the first critical steps towards managing security risk and compliance. Symantec offers a highly scalable, integrated, and efficient solution for asset Discovery, which leverages its patented technology to make it the best-in-class offering.

About Symantec 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. Each of the five Control Compliance Suite Modules is available independently or as part of a broader suite.

The Control Compliance Suite Control Studio and Infrastructure 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.

Appendix Protocols Used

The following protocols are used in the discovery process:

1. Transmission Control Protocol (TCP)
2. User Datagram Protocol (UDP)
3. Server Message Block (SMB)
4. Network Time Protocol (v)
5. Simple Network Management Protocol (SNMP)
6. NetBios Session Service (NBSS) Protocol
7. NMap (if installed on the system)
8. SinFP (OS fingerprinting)
9. DNS Lookup

The following protocols are used in network discovery details:

- TCP and UDP port scan and Echo request
  - Send TCP SYN, look for TCP SYN/ACK
  - Send empty UDP, look for port unreachable
  - Send ICMP ping, look for echo reply

The following protocols are used in host discovery:

- TCP and UDP port scan and Echo request
  - Send TCP SYN, look for TCP SYN/ACK
  - Send empty UDP, look for port unreachable
  - Send ICMP ping, look for echo reply
- DNS lookup
  - Performs DNS lookup
- UDP application scan

– NetBIOS name service – name query

– SNMP get-request

- TCP application scan
  - SMB
  - Telnet
  - HTTP
  - HTTPS
  - SSH
  - FTP
  - SMTP

The following protocols are used in OS discovery:

- TCP and UDP port scan
- SMB
- UDP application scan
- NBSS
- NTP
- DNS
- SinFP

The following are the ports used, with the respective protocols:

- 1,2,3 UDP
- 21 TCP/FTP
- 22 TCP/SSH
- 23 TCP/Telnet
- 25 TCP/SMTP
- 80 TCP/HTTP
- 135 TCP
- 137 UDP - used by the NETBIOS Name Service
- 161 SNMP
- 443 TCP/HTTPS
- 445 TCP/SMB

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Symantec

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

SYMC_WP_Asset_Discovery_Control_Compliance_EN_v1a