



SYGATE MAGELLAN

Sygate Magellan creates a comprehensive and detailed census, tracks current network state and measures policy compliance for network connected devices. The database tracks connected devices and records changes, additions and deletions to their configurations over time. External information sources such as Network Management Systems and Asset Management Systems can be aggregated into the database.



Magellan ensures no devices elude the corporate information protection process. Designed for deployment in the world's largest networks, Sygate Magellan has a distributed appliance-based architecture comprising three elements: multiple Sygate Discovery Engines, which detect and probe for Network Dark Matter; the Sygate Correlator, which aggregates information gathered by Discovery Engines; and the Magellan User Interface that administrators use to interact with Sygate Magellan.

THE PROBLEM

It is both a great advantage and disadvantage that today's corporate networks are fundamentally open. While open networks enable global access they offer little to prohibit access by rogue or compromised devices. Hackers and thieves exploit these devices for access to corporate information assets. Corporations have implemented processes to identify these unwanted devices; however, many elude detection, assessment, or management, thus leaving hackers a way in.

The now-infamous Slammer worm exploited a long known exposure in MS SQL Server. Organizations patched the machines they knew about, but Slammer found the ones they didn't know about. We call these unmanaged resources Network Dark Matter. They include rogue servers added by consultants working on rush projects, devices with embedded OSs like network printers, point-of-sale systems, or ATMs. Enabling new services or adding a network adapter to a previously compliant device also can create Network Dark Matter. As enterprises move more assets to open networks, hackers become more sophisticated, and privacy and governance regulations expand, more is at stake than ever before.

THE SYGATE SOLUTION

Sygate Magellan maintains the most complete, accurate, and detailed information about the current state of the network, measuring the level of policy compliance for network assets. Sygate Magellan tracks all IP-addressable devices on a network and identifies when those devices appear or disappear, identifies the software that runs on them, probes their configurations and capabilities, and identifies their de facto compliance



Sygate Magellan provides pre-defined reports, drill-down capabilities, and data export features. Security and network administrators can use these capabilities to determine the security implications of network events.

Magellan provides pre-defined reports that answer the following questions:

- What is on my network today?
- What has changed on my network?
- What devices are manageable/unmanageable?
- What devices are compliant/non-compliant?
- What devices are business critical?

with security policies. Administrators can bring them into compliance based on asset class and exposure priority.

Enterprises that also implement Sygate Secure Enterprise or Sygate On-Demand ensure both corporate devices and third-party-owned devices are continuously compliant with security policy. Sygate On-Demand provides this protection for Web applications such as SSL VPN, Web Mail, and Extranets accessed from employee, partner or customer owned computers, and public kiosks. Sygate Secure Enterprise extends the solution coverage to corporate equipment - laptops, desktops, and servers.

Reduces security costs

- Automates detection of rogue devices and compliance checking of compromised devices.

Ensures Regulatory Compliance

- Ensures compromised and rogue devices do not escape the information protection process
- Creates an audit-quality historical log of changes to the network, devices and security policy.

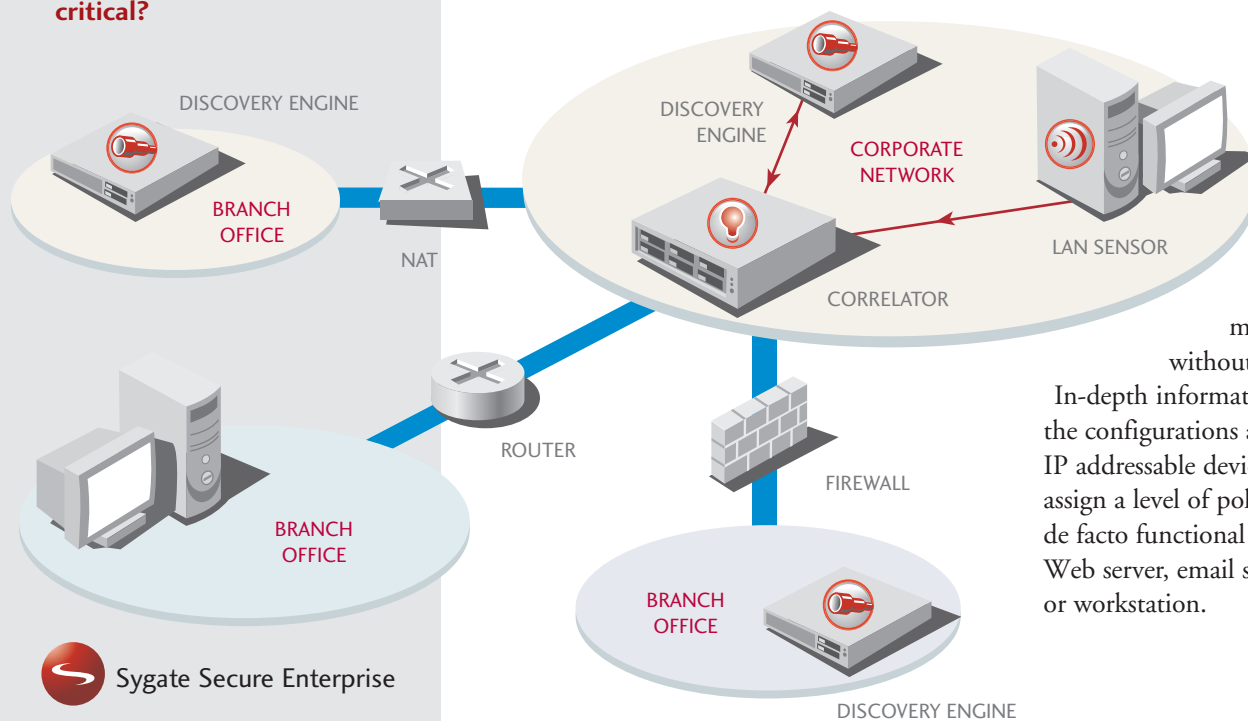
HOW DOES MAGELLAN WORK?

Magellan ensures that no devices elude the corporate information protection process. Designed for deployment in the world's largest networks, Magellan has a distributed appliance-based architecture comprising three elements: multiple Sygate Discovery Engines that detect and probe for Network Dark Matter; the Sygate Correlator that aggregates information gathered by the Discovery Engines and the Magellan User Interface with which Administrators manage Magellan.

BENEFITS

Minimizes Network Downtime, and Business Disruption


- Ensures timely discovery of compromised and rogue devices before they can be exploited to bring down networks and application services



Intelligent probes use a combination of credentialed and non-credentialed techniques in a 'cascade' fashion to ensure detailed information is gathered without crashing systems.

In-depth information is collected on the configurations and capabilities of each IP addressable device to automatically assign a level of policy compliance and a de facto functional classification, such as Web server, email server, firewall, database, or workstation.

 Sygate Secure Enterprise

 Sygate On-Demand

Security managers and administrators generate reports that identify progress toward policy compliance, flag compliance exceptions with specific information on exposure, and provide prioritized remediation recommendations based on asset values.

Magellan manages a database of all connected devices, containing a record of changes, additions, and deletions to device configurations over time. This database is extensible to include feeds from external information sources including Network Management Systems and Asset Management Systems, and is open to report writers for custom reports.

THE SYGATE ADVANTAGE

Best product

- Intelligent, credential-based discovery enables deeper endpoint policy compliance checking without crashing endpoints
- Correlation-based architecture enables rapid identification of Network Dark Matter that poses a threat to the network
- Audit-quality historical log tracks changes to network and security policy for regulatory compliance

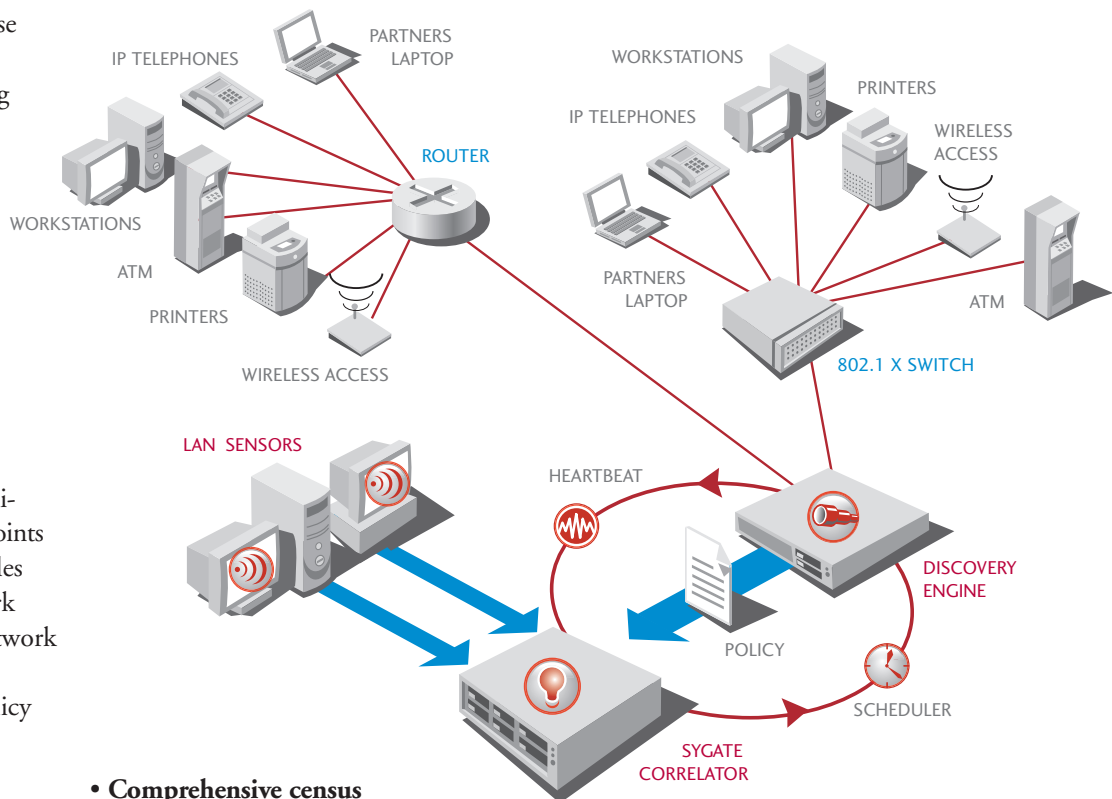
Best economics

- Automates discovery process, which is often performed manually with multiple products.
- Automates analysis of network and device changes by asset class
- Automatically identifies Network Dark Matter for network eviction or security management
- Architected to aggregate information from other business systems such as Network Management Systems or Vulnerability Assessment systems.

FEATURES

Automated Discovery

Sygate Correlator manages multiple Sygate Discovery Engines in a distributed architecture to achieve an in-depth network census using intelligent probes. LAN Sensor provides Sygate Correlator with real-time knowledge of devices connecting to the network.



Comprehensive census

from polls of all IP-addressable devices, including Windows, Linux, Solaris, wireless access points, routers, switches, printers, firewalls, IP phones, etc.

- **Intelligent probes** use a hierarchical approach to ensure that systems are not shut down. For example, Magellan won't use an SNMP community string (intended for network devices) on a system that is found to have a NetBIOS name and current domain (characteristic of a Windows device).
- **In-depth identification** of each device includes IP address, MAC address, ports, services, NetBIOS name, current domain, SNMP MIB info, and OS fingerprint.

- **Credential probes**, using administrative privileges, produce a rich inventory of targeted systems, including applications, active accounts, patches, and service packs.
- **Distributed discovery**, deploying Sygate Discovery Engines beyond firewall and NAT devices, enables probing on remote networks and returns results to the Sygate Correlator.

- **Device classification** automatically organizes discovered devices into function-specific sets such as firewall, Web server, database, or workstation. Specialized probes can be scheduled to run on these classified sets, thereby automatically including devices discovered in the future.
- **LAN Sensors** are part of the Sygate Secure Enterprise solution, LAN Sensors monitor ARP traffic to identify, in real-time, all IP-addressable devices trying to connect to the network. Sygate Magellan automatically stores this information, by subnet, for later probing.

SYSTEM REQUIREMENTS

Magellan User Interface

Supported Operating Systems:

Windows 95/98, ME, NT, XP,

2000, 2003

Red Hat Linux 7.3, 9.0

SYSTEM SPECIFICATIONS

Sygate Correlator¹

Hardware:

2U, 19" rack-mount server
appliance

1 - 36GB pluggable drive

2 - Gigabit Ethernet interfaces

AC Power, redundant,

hot pluggable

Redundant fan

24X CD-ROM Drive

Software:

Correlation Engine

MySQL Database

Sygate Discovery Engine

Hardware:

1U, 19" rack-mount server
appliance

1 - 80GB integrated drive

2 - Gigabit Ethernet interfaces

24X CD-ROM Drive

Software:

Discovery Engine

Note

1: Sygate Integrated Magellan has the same hardware configuration as the Sygate Correlator with an additional software component, the Discovery Engine

Compliance

Security managers can measure progress toward ensuring compliance on all connected devices.

- Maintain an audit-quality, historical log of changes to the network, security policy, and operation of the product - monitoring capabilities that are key to effective governance.
- Dashboard uses graphs and charts to show aggregate analysis of compliance, manageability, and census of IP addresses, devices, operating systems, and services.
- Administrator can define policies for applications (including service packs and patches), services, ports, and specific devices.
- Administrator can classify devices by business asset value, enabling prioritization of remediation tasks
- Identifying Network Dark Matter enables enterprises to bring devices into continuous compliance by flagging them for control using Sygate Secure Enterprise.

Data Analysis and Reporting

Sygate Magellan provides pre-defined reports, drill-down capabilities, and data export features. Security and network administrators can use these capabilities to determine the security implications of network events.

- Network events include the addition, movement, or change of device attributes such as applications, services, IP addresses, ports, and network interfaces
- Pre-defined reports answer the following questions:
 - What is on my network today?
 - What has changed on my network?
 - What devices are manageable/unmanageable?

Sygate European Headquarters

London • +44-1494-582032

Sygate France

Paris • +33 (0) 1 55 68 11 00

Sygate Germany

Frankfurt • +49 (0) 6102 29 99 40

Sygate Greater China Headquarters

Beijing • +86.10.62638951/61

– What devices are compliant/non-compliant?

– What devices are business critical?

- Report writers can be given access to the Sygate Magellan database

Data Repository

Sygate Magellan uses a database to manage the data collected from discovered assets.

It is designed to aggregate information from different data sources, such as Network Management Systems, Asset Management Systems, Trouble Ticket Systems and Vulnerability Scanners.

Management

Sygate Magellan is a scalable, appliance-based solution that can be deployed in large, distributed networks and managed via the Magellan User Interface from any supported client that can connect to the Sygate Correlator.

Log files detailing access to the Sygate Magellan system and its components are collected, viewable via the Magellan User Interface, and exportable to files.

A hardened appliance platform, system integrity checks, and heartbeat mechanisms between the Sygate Correlator and Sygate Discovery Engines ensure robust operation in mission-critical enterprises.



SYGATE TECHNOLOGIES

6595 Dumbarton Circle,
Fremont, CA 94555
Telephone: 510.742.2600
Facsimile: 510.742.2699
www.sygate.com