



SYGATE SECURE ENTERPRISE

Sygate Secure Enterprise eliminates the damage or loss of information, cost of recovery, and regulatory violation due to rogue corporate computers, applications, and behavior. Unlike any other solution, Sygate Secure Enterprise ensures that only compliant, protected devices connect to the corporate network.



“In a recent survey by the Computer Security Institute, 90 percent of respondents used antivirus software, but 85 percent had been damaged by a virus. In the same survey, 89 percent had installed computer firewalls and 60 percent had intrusion detection systems, yet 90 percent reported security breaches had taken place and 40 percent had their systems penetrated from outside their network.”

PRESIDENT'S CRITICAL
INFRASTRUCTURE PROTECTION
BOARD

THE PROBLEM

Today's enterprise networks have evolved into open environments in which virtually every computer (endpoint) connected to the corporate network is exposed to the outside world through the Internet. In this new environment, perimeter-based security models are no longer effective.

Many enterprises have taken a more layered approach to securing open networks by implementing security products, such as antivirus software, host firewalls, host IDS, and patch management systems on endpoints (laptops, desktops and servers).

No matter how much information security budgets are increased to include these new tools, or how hard or fast today's information protection processes are cranked, hackers and thieves continue to disrupt our networks, steal valuable information, and expose us to regulatory violation. One reason for their continued success is that there hasn't been a solution capable of enforcing continuous policy compliance.

THE SYGATE SOLUTION

Sygate changes the game. For the first time, commercial and government enterprises get strategic advantage over hackers with the industry's first enterprise security solution that ensures that both company-owned and third-party-owned devices are uncompromised, continuously compliant with security policies, and protection of confidential data. Sygate Secure Enterprise delivers continuous compliance and the resultant dramatic improvement in protection to corporate-owned devices, such as laptops, desktops, servers, or embedded devices. Sygate On-Demand extends this protection to web applications, such as SSL VPN, Web Mail, and Extranets, accessed from third-party-owned equipment. Sygate Magellan eliminates Network Dark Matter™ to ensure that no endpoints or exposures escape detection and management.



“Prudential Financial is using Sygate Secure Enterprise to create, automate, and enforce corporate security policies. With Sygate, all Prudential Financial’s remote workers are guaranteed to be in a trusted state before gaining network access.”

TECHDECISIONS FOR
INSURANCE, APRIL 2003

Sygate’s customers have achieved far better results than others because they are pursuing a different strategy. Using Sygate Secure Enterprise, customers are putting in place a system that eliminates the fundamental exposures of open networks:

- Rogue users
- Compromised systems and applications
- Unsafe or incorrect user behavior

Sygate Secure Enterprise eliminates the damage and loss of information, as well as the costs of recovery and regulatory violation due to rogue corporate computers, applications, and behavior. Unlike any other solution, Sygate Secure Enterprise ensures that only compliant, protected devices connect to the corporate network.

The SSE solution combines a sophisticated security agent that runs on each end-point with one or more policy management and enforcement servers distributed across the enterprise, that work together with existing security and infrastructure investments to detect, enforce, remediate, and protect non-compliant devices.

BENEFITS

Minimizes network downtime and business disruption

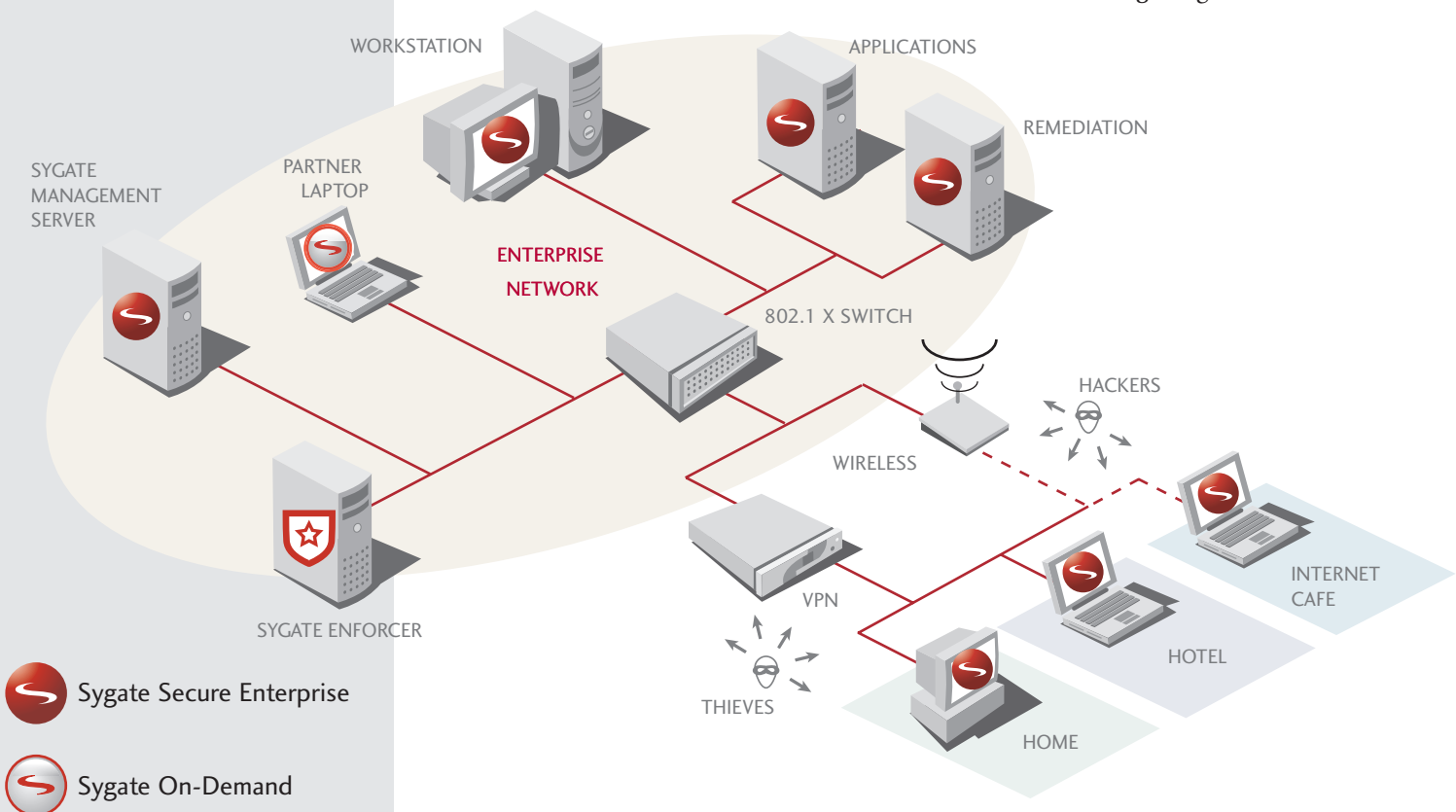
- Protects infrastructure from rogue users, compromised devices, and applications
- Strategic platform that addresses today’s urgent needs and tomorrow’s evolving needs. Continuous compliance provides a framework for addressing current and future security requirements.


Reduces security costs


- Automates compliance checking, enforcement and remediation
- Automation reduces help desk costs and protects user productivity
- Leverages existing infrastructure by interoperating with other vendors’ products

Ensures regulatory compliance

- Protects customer, patient, and employee privacy
- Achieves continuous compliance, thus assuring the integrity of internal controls and good governance



 Sygate Secure Enterprise

 Sygate On-Demand

HOW DOES SECURE ENTERPRISE WORK?

Sygate Secure Enterprise combines a sophisticated security agent that runs on each client with one or more policy management servers distributed across the enterprise, and enforcement on servers inside the network and on endpoints.

Sygate Security Agents

Sygate Security Agents protect all network-enabled endpoints (laptops, desktops, servers, and embedded devices) in an enterprise through an application-centric firewall and intrusion prevention engine. The Sygate Security Agent automatically adapts its security policies based on the vulnerabilities and threats of each endpoint's network environment. Using Endpoint Enforcement, Sygate Security Agent can automatically check compliance at a configurable interval and quarantine non-compliant endpoints to a remediation area. Endpoint Enforcement ensures compliance for all endpoints whether they are local, remote, or not currently connected to the corporate network.

Sygate Management Server

Sygate Management Server learns the current state of the network and reports on the security posture of the enterprise network. In addition, Sygate Management Server automatically creates security policies that link users, connectivity technology, applications, and network communication to best practices. Sygate policies are managed and inherited through group structures of users, workstations, and servers that can be imported and synchronized with NT Domain, Active Directory, and/or LDAP. Sygate Management Servers can be centralized or distributed in a global enterprise to provide scalability, fault tolerance, load balancing, and policy replication.

Sygate Universal Enforcement

Sygate Universal Enforcement™ ensures that all endpoints are compliant with security policy before permitting network access. Policy compliance is enforced

regarding patch levels, operating system configurations, and the correct versions of and up-to-date signature files for applications such as antivirus software, personal firewall, and intrusion prevention. Devices that fail to meet enterprise security policy can be flagged for network administrators, blocked from network access, or only granted access to remediation resources for automated remediation. Sygate Enforcers are placed at network entry points, such as VPN, wireless access points, RAS dial-up servers, on the internal LAN using 802.1x EAP authentication, or on the endpoints themselves, via Endpoint Enforcement. Sygate Enforcers communicate with Sygate Management Server to obtain security policies and agent authentication information. They ensure the integrity of the agent and its adherence to corporate security policies.

SYGATE ADVANTAGE:

Best product

- Award-winning product (Gartner Group and Network Computing Magazine)
- Strategic platform - automatically achieves continuous compliance
- Power and flexibility of the Agent delivers best security and protects user productivity

Best economics

- Automates compliance checking, enforcement and remediation
- Reduces help desk costs and protects user productivity by automating remediation
- Leverages your existing infrastructure by interoperating with other vendors' products

Best enterprise customer experience and success

- Largest policy enforced networks
- Designed with some of the largest enterprises to meet their own needs
- Most mature product - resulting from being the first mover in this market

FEATURES

Adaptive Protection

Sygate Secure Enterprise dynamically adapts security policies based on the user, the hostility of the network environment, and the access method. Policies can be triggered based on DNS IP, WINS IP, DHCP server, gateway address, VPN connection status, and dial-up networking status. In addition, administrators can give users limited, context-based control over security policy while retaining a baseline of enterprise security policy control. Sygate Security Agents can also detect the presence of a Trusted Computing Group (TCG) security chip and adapt their policies accordingly.

Application-Centric Firewall

Sygate Security Agent incorporates an application-centric firewall that stealths host systems, provides stateful firewalling, applies rule-based security policy, and controls application usage.

Intrusion Prevention Engine

Sygate Security Agent's intrusion prevention engine applies patterns of known attacks to all incoming and outgoing traffic as a second layer of defense. Sygate's unique application-based approach to intrusion prevention uses application layer information and deep packet inspection to more effectively identify and block known and unknown attacks.

Host Integrity Checking

Sygate Security Agent can check the security status of the endpoint, including: the status of executables (antivirus, host firewall, host IPS, sandbox), files (antivirus signatures, host firewall policies, host IDS signatures, MD5 checksum, file version), registry values, versions, patches, and operating system configurations.

SYSTEM REQUIREMENTS

SUPPORTED PLATFORMS

Sygate Management Server

Operating Systems:

Windows Server 2003
Windows 2000 Server
Solaris 9

Web Servers:

Internet Information Systems
Sun Java System Web Server 6.1

Database:

Microsoft SQL 2000
Oracle 9i

Sygate Security Agent

Operating Systems:

Windows 95
Windows 98 SE
Windows Millennium
Edition (ME)
Windows NT 4.0 Workstation
or Server
Windows 2000 Professional
or Server
Windows XP Home Edition
or Professional
Windows Server 2003
Windows XP Embedded

Sygate Enforcer

Operating Systems:

Windows Server 2003
Windows 2000 Server
Redhat Linux 7.3

Universal Enforcement (including 802.1x support)

Universal Enforcement ensures that all endpoints are 100% compliant with security policies before permitting network access. Enforcement can be accomplished through Endpoint Enforcement, LAN Enforcer (full 802.1x support), Gateway Enforcer, and enforcement in conjunction with third-party products, such as VPNs or wireless access points. Policy compliance is enforced regarding patch levels, operating system configurations, and application configurations (ensuring that software such as antivirus, personal firewall, and intrusion prevention is running the correct versions and has up-to-date signature files). Devices that fail to meet enterprise security policy can be monitored, blocked, or sent for automated remediation.

Automated Remediation

Sygate Secure Enterprise automatically repairs the security integrity of authorized endpoints that are denied access due to non-compliance with security policies. Sygate Security Agent can automatically initiate a remediation action, such as downloading and installing a software patch or update, executing command-line instructions, turning applications or OS features on or off, thereby returning the endpoint to policy compliance without user or help desk intervention.

Enterprise Policy Management

Sygate Secure Enterprise enables enterprises to create policies about applications, data, and configurations that must be in place for secure communication. Based on a fault-tolerant, multi-server architecture with outstanding performance and unlimited scalability, Sygate Secure Enterprise provides a reliable foundation for creating and managing policy across global enterprise networks.

Highly Scalable Architecture

Sygate Secure Enterprise is designed for deployment in large and distributed enterprise networks. Sygate's multi-server architecture provides outstanding performance and unlimited scalability, fault-tolerance, performance optimization, and policy uniformity across global enterprise networks.



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

SYGATE TECHNOLOGIES

6595 Dumbarton Circle,
Fremont, CA 94555

Telephone: 510.742.2600

Facsimile: 510.742.2699

www.sygate.com