



SYGATE ON-DEMAND

Sygate On-Demand enables enterprises to secure Web applications by ensuring the integrity of endpoints and protecting the data that is transmitted to them. The Sygate On-Demand Agent is downloaded from the Web application or SSL VPN box at connection time to the endpoint.

The connection is only allowed if the endpoint is fully compliant with security policy.



Today's enterprises have evolved into open network environments where corporate data is accessed from third-party-owned devices by a combination of employees, business partners, suppliers, contractors, and customers. In this environment, enterprises have little or no control over the security of third-party-owned endpoints and the safety of the data that is transmitted to those devices.

THE PROBLEM

The fundamental shift from client-server to Web-based applications has profoundly changed the way employees, business partners, customers, and suppliers access and utilize corporate information. In a client-server world, corporate information is protected by securing corporate-owned devices (using Sygate Secure Enterprise) and authenticating the user. In contrast, clientless Web-based applications and services can be accessed from any computer, including employee-owned computers, airport kiosks, hotel business center computers, and supplier systems. On these third-party-owned computers, the corporate security organization has no method to verify the security of that computer, to protect the information provided by the Web application, to erase the information at session termination, or to protect the entire session from malicious code.

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 always uncompromised, compliant with security policies, and protecting confidential data. Sygate On-Demand provides this protection for Web applications such as SSL VPN, Web Mail, and Extranets accessed from third-party-owned devices. Sygate Secure Enterprise extends the solution coverage to corporate equipment. Sygate Magellan eliminates Network Dark Matter™ to ensure that no endpoints or exposures escape detection and active management.



“Extending access of Web-based applications outside the organization introduces the potential for exposure from non-corporate owned devices, which can lead to numerous security breaches including financial fraud, password theft, and leakage of confidential information, as well as exposure to regulatory penalties.”

ZEUS KERRAVALA
VICE PRESIDENT OF
ENTERPRISE INFRASTRUCTURE
YANKEE GROUP

Sygate On-Demand enables enterprises to secure Web applications by ensuring the integrity of endpoints and protecting the data that is transmitted to them. The Sygate On-Demand Agent is downloaded from the Web application or SSL VPN box at connection time to the endpoint. The connection is only allowed if the endpoint is fully compliant with security policy. When the connection is allowed, a secure desktop is created to protect downloaded information.

BENEFITS

Protects Patient, Customer & Employee Privacy

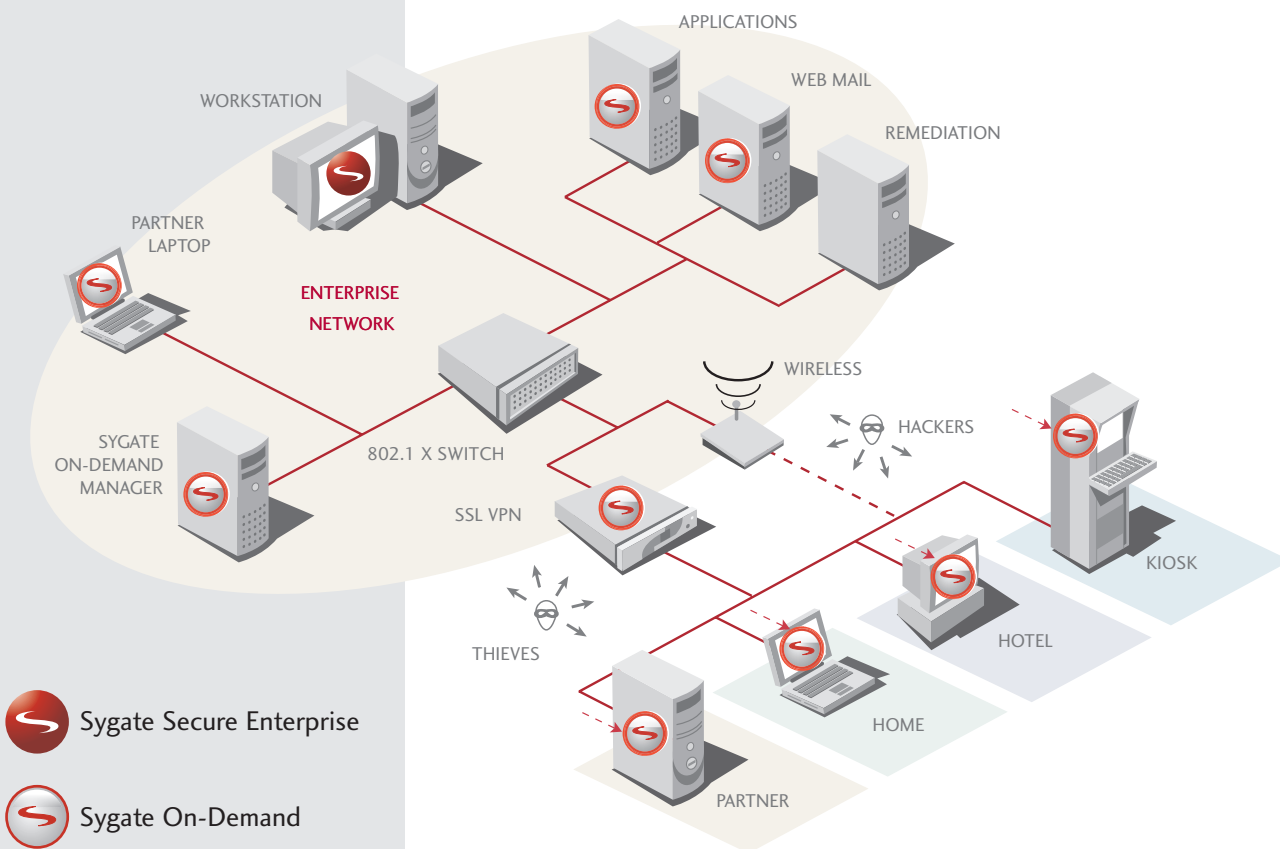
- Customer information - Protects the confidentiality of customer records and financial information. (California SB 1386)
- Medical diagnosis or claim processing - Ensures compliance with HIPAA and other regulations that protect patients' medical records privacy rights.


Protects Sensitive Business Information


- Financial Systems - Protects the confidentiality of remotely accessed financial information (GLBA, Sarbanes-Oxley).
- Web E-mail - Prevents theft of email passwords and information leakage through attachments being left on kiosks or Internet café computers.

Prevents Business Disruption

- SSL VPN - Protects the enterprise network from compromised endpoints.
- Business portals - Ensures that business partner computers are secure prior to accessing corporate networks, and thus do not compromise the security of the company's network.



 Sygate Secure Enterprise

 Sygate On-Demand

HOW DOES IT WORK?

Sygate On-Demand Manager creates a Web page containing the Sygate On-Demand Agent download. The Sygate On-Demand Agent download Web page is then placed on the Web server and configured to be the default page of the Web application, such as mail.company.com. When a user connects to this Web page located on an SSL VPN, Web mail server, or Portal Web server, the Sygate On-Demand Agent (SOA) is downloaded and launched on the endpoint. Once launched, SOA verifies the integrity of the endpoint including antivirus software, personal firewall, service pack, and patch/hotfix policies. After completing the Host Integrity verification process, SOA creates a Virtual Desktop environment. From within that virtual environment, SOA launches the login process to the Web application through a Web browser in the Virtual Desktop. The SOA user can then access corporate resources such as e-mail or corporate servers. When the session to the Web application is complete or times out after a configurable interval, SOA can either automatically erase all data from the session or create an encrypted and password-protected virtual desktop environment that remains on the computer.

THE SYGATE ADVANTAGE

Sygate On-Demand uniquely addresses the four critical requirements for safe access to the corporate network from third-party-owned devices.

On-Demand Deployment in any Environment

The key to implementing On-Demand successfully is the ability to deliver the security solution to every endpoint that needs to access the target Web application. Sygate On-Demand can be delivered with guest rights, ActiveX disabled,

and the endpoint's browser security at high. No other solution offers the ability to install on-demand security on locked-down systems such as kiosks, partner computers, and at hotel business center computers.

Verifying the Security of Endpoints

In order to make an informed decision on whether to allow or deny access to the corporate network and information, it is critical to verify the level of security on the endpoint by checking for the presence and status of antivirus software, personal firewalls, service packs, and patches prior to allowing access. Without the ability to check for host integrity, it is impossible to eliminate the risks of compromised endpoints accessing corporate resources. Sygate provides the ability to accurately determine the security level of a system including ensuring that any antivirus product is running with up-to-date virus definitions, a personal firewall is active, service pack levels are met, and critical patches are installed.

Preventing Information Leakage

Every day, corporate information such as business plans, financial projections, and customer information is accessed from third-party-owned computers and left unencrypted for anyone to view and exploit. Sygate On-Demand provides comprehensive protection for corporate information and sanitizes the data at the end of the Web session, preventing information leakage and protecting data privacy.

Adapting Protection to the Endpoint Environment

Every endpoint represents varying levels of risk to corporate networks and information depending on the type of device (corporate-owned vs. third-party-owned), the network environment (Office LAN vs. Internet Café), and the security protections in place on the endpoint (Host Integrity). Applying a uniform policy or security technology to every endpoint

leads to either reducing the productivity of a secure endpoint or failing to adequately protect a vulnerable endpoint. For example, when a corporate-owned desktop, running all mandated protection, connects from the office network and accesses a Web application, it would be foolish to apply the same protections to that application as are applied when it is accessed from an airport kiosk. Sygate On-Demand automatically determines and applies the appropriate policies and security technologies necessary for a given endpoint environment, always based on enterprise security policies.

Sygate's ability to deploy On-Demand protection in any environment, verify the security of endpoints, prevent information leakage, and adapt its level of protection to the environment makes Sygate On-Demand uniquely capable of protecting enterprises data and networks from the vulnerable endpoint using Web applications.

Next time you are staying at a hotel, go to the hotel business center computer and do a search for "*.doc" or "*.xls", and you may be very surprised by what you find. Even if you, as a conscientious security person, were to delete the file and empty the recycle bin, the information could still be recovered from the hard drive unless that portion of the hard drive is sanitized. With Sygate On-Demand, those files can no longer be found, once your session completes.

SYSTEM REQUIREMENTS

Sygate On-Demand Agent

Sygate Virtual Desktop

Operating System:

NT4 (SP6), 2000, XP

Sygate Host Integrity

Operating System:

Windows 98, ME,
NT 4 (SP6), 2000, XP

Sygate Cache Cleaner

Operating System:

Windows 98, ME, NT4 (SP6),
2000, XP, Mac OSX, Linux
Redhat 7.3 or later

Browser: Internet Explorer 5.0
or later, Netscape 6.0 or later,
Opera 7.2 or later, Safari 1.0
or later, Mozilla 0.9.9 or later

Sygate On-Demand Manager

Operating System:

Windows 2000, XP, Server 2003

FEATURES

Host Integrity

Ensures that devices accessing confidential data are secured by antivirus software with updated virus definitions, a personal firewall, critical service packs, and patches. This verification ensures that the corporate network won't be compromised by endpoints accessing protected Web applications.

Virtual Desktop

Sygate On-Demand Agent creates and launches a Virtual Desktop that enables users to download confidential data into a virtual environment where it can be opened by local applications, modified, and uploaded back to the Web application, or copied to a floppy disk, USB hard drive, or other removable media. The Virtual Desktop enables enterprise employees, business partners, and customers to access confidential information securely while using third-party-owned devices.

Data Sanitization

When the session is terminated or times out, Sygate On-Demand Agent will sanitize the system, removing all data generated during the network connection. Data sanitization ensures that confidential information that is downloaded to third-party-owned devices is completely removed.

Persistent Virtual Desktop

Sygate On-Demand Agent (SOA) can create a Virtual Desktop that remains on the endpoint, protected by a user-defined password. Persistence eliminates the need for users to re-download SOA each time they connect to the enterprise Web application, enables access to data stored in the Virtual Desktop after the termination of the session, and maintains separation between the host endpoint and the Virtual Desktop.

Adaptive Policies

Sygate Virtual Agent has the ability to adapt security policies based on identification of the specific network locations and the type of network device (corporate-owned vs. third-party-owned) to ensure that all confidential data is protected without affecting the productivity of the user. Adaptive Policies ensure that users accessing the corporate site have the appropriate level of security according to the type of device they are using to connect, and the network location.

Cache Cleaner

Sygate Cache Cleaner ensures that Web browser information, such as cookies, history, auto-complete, stored passwords, and temporary and downloaded files, are erased or removed upon termination of the session, inactivity timeout, or closing of the browser. Cache Cleaner can either work in conjunction with Sygate On-Demand Agent to clean the browser cache on additional operating systems such as Mac OS X, Linux, and Windows (98,ME), or as a standalone module.

Malicious Code Protection

Sygate On-Demand Agent protects confidential information from malicious code by ensuring that antivirus software, personal firewalls, and service packs are compliant before allowing the user to authenticate through the Web application, and by encrypting all data that is downloaded into the encrypted and password-protected Virtual Desktop. Without Sygate On-Demand Agent's protection, allowing third-party-owned devices to access the enterprise network and confidential data can result in network disruptions, data theft, information leakage, and fraud.



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