



## Sygate Prevents Known and Unknown Attacks

---

Sygate's solution detects and blocks compromised, misconfigured and unauthorized endpoints before they can damage your corporate network. Sygate Secure Enterprise checks for security policy compliance before allowing network connections to be established by endpoints. This solution automatically remediates those authorized endpoints that are compromised or misconfigured, thus protecting employee productivity while enforcing policy compliance. Sygate's solution eliminates business disruption, recovery costs and regulatory violations due to rogue and compromised devices.

To protect against both known and unknown exploits, Sygate uses two approaches: signature-based protection and behavior-based protection (sometimes called Zero-Day protection because of its capability to protect against exploits that attack previously unknown vulnerabilities). Our hybrid approach offers superior protection by drawing upon the strengths of both approaches.

### **Behavior-Based Protection (Zero-Day Protection)**

The Sygate Agent achieves strong zero-day protection using four techniques:

- Looks for anomalies in the network traffic of every application
- Blocks malicious drivers at the lowest level possible in the operating system
- Ensures that each application uses only known good DLLs and code modules
- Inspects the security and patch level before allowing the computer onto the network

Sygate's products monitor all applications on the host and block any application from accessing anomalous ports or services. By monitoring drivers that are sending or receiving traffic, Sygate blocks malicious or unknown drivers from bypassing the firewall, in addition to blocking protocol attacks or malformed packets. Using a sophisticated application monitor, Sygate detects and blocks any unknown or malicious modules, DLLs, or code that tries to inject itself into an application.

Before allowing a computer onto the network, the Sygate Agent initiates a host integrity check to verify that all security measures, such as antivirus software, personal firewall, intrusion protection system or operating system patches, are in place, active and up to date. If the Sygate Agent detects that security applications are turned off, or are running files that are out of date, or that certain patches are missing, it can automatically turn applications on, download the latest files, or install specific patches before allowing the device access to the corporate network.

The Sygate Agent adapts its security policy to the type of network connection, such as wireless, Ethernet or VPN, plus the location of the network connection, such as home, an Internet café, or the office. Sygate eliminates rogues that expose the organization to hackers while automating the process, thus enhancing not only protection but cost effectiveness.

### **Signature-Based Protection**

The Sygate Agent provides strong signature-based protection with an extensive, Sygate-updated signature base, which enables the Agent to detect and protect against known vulnerabilities and known exploits, as well as any unknown or new exploit that targets a known vulnerability. Signatures are the most effective way to block known exploits and they minimize false positives. False positives are expensive because of the staff time expended tracking them down.

Signatures enable the Sygate Agent to block and report on any exploits that are attempted. Solutions that rely solely on behavior-based protection are not as effective, because they are unable to identify exploits by name, and unable to report on the security events that occurred. For instance a solution will report, "IIS tried to execute CMD.EXE." However, the



## Sygate Prevents Known and Unknown Attacks

---

reason for the attempt may be missing or lacking. Any number of exploits may have been involved, or what appears as an exploit may in fact have been something that your Webmaster did on purpose. With Sygate's reporting, you know the source of the possible attack, and can thus defend your system from further attacks.

### Protection Feature Summary

#### Behavior-Based Protection Features (Zero-Day protection)

- **Application-Centric Policy Control** – Blocks anomalous behavior, preventing code injection and application compromise, thus ensuring that applications only utilize correct ports, services and DLLs.
- **Smart Protocol Filtering** – Behavior-based protection from protocol-borne exploits
- **Anti-IP and Anti-MAC Spoofing** – Prevents hackers from masquerading as an authorized user, using that user's IP and MAC addresses.
- **Driver Level Protection** – Blocks hackers from loading their own protocol drivers by bringing drivers under policy control and monitoring.
- **Port Scan Protection** – Behavior-based protection that blocks hackers from port scanning, which is often used to discover open ports for exploit.
- **Host Integrity Checking** – The Sygate Agent tests the endpoint's compliance with the complete set of security policies prior to network access and only grants access if the endpoint is 100% compliant.

#### Signature-Based Protection Features

- **Deep Packet Inspection** – Filters packets based on any part of the packet, including the header and data portion, to block known exploits.
- **Trojan Protection** – Monitors every running application to verify that no Trojan is running.
- **DoS Protection** – Protects against DoS attacks by blocking anomalous network traffic patterns.

### Conclusion

Sygate's unique hybrid approach brings the power and efficiency of signatures to bear against known exploits and behavior-based protection to bear against unknown exploits. In this way the solution achieves more comprehensive protection than could be obtained using either individual approach. Sygate's hybrid approach also avoids the shortcomings of using signatures against zero-day exploits or the false positive problems associated with behavior-only approaches.