

Endpoint Security Services

CGI's MSS Endpoint Security solutions help to protect government's data, both on and off the network. Endpoint Security provides protection against malicious software behavior and enforces usage policies on laptops, workstations, and servers. Endpoint security services provide protection against viruses, Trojan horses, backdoors, potentially unwanted programs, poorly behaving programs and "adware".

Mail servers, workgroup servers and databases can also carry malicious software through environments without infection or detection. This causes potential damage to other organizations and harms the reputation of the source organization. CGI MSS can scan data passing through your infrastructure and eliminate outbound threats to your clients, customers and business partners.

Misplaced, lost and stolen laptops, hard drives and the data they contain is a serious concern. This is a risk to confidential and private data of governments, citizens and employees. Additionally, many jurisdictions require the disclosure of data loss, blemishing your reputation. Full disk encryption on the endpoint can protect this data, thus minimizing the risk of losses to the nominal value of the lost or stolen device. Optionally, the service can be extended to protect middleware from viruses and other malware.

Host-based Intrusion Prevention Systems (HIPS) stop intrusions and infections at the individual workstation or server level, and are much more effective at blocking, or at least containing, threats. HIPS are becoming a standard component of the end point safeguard, as zero day viruses and "bot-nets" are more commonplace.

The HIPS component also provides the following personal firewall functionality:

- Prevention - prevents the transfer of files to or from unauthorized devices
- Visibility - provides complete visibility of device and file accesses on the network
- Flexibility - provides granular control over who has access to what devices and for how long
- Device control - Prevents the unwanted transfer of data to or from portable devices – such as USB flash drives, iPods, PDAs and even CDs – by automatically enforcing security policies. User access can be blocked, limited to read-only or left unrestricted according to the individual's security privileges and device type in use.
- Access Auditing - The solution provides visibility of all user and administrator actions, recording everything from individual device connections

Features

- Centrally managed or unmanaged
- Identifies device coverage
- Prevents unknown, potentially unwanted software from operating
- Eliminates known malicious software
- Manages and controls connection of portable media devices to your organization's PC

Benefits

- Secures network environments
- Protects data and staff
- Complies with regulations
- Guaranteed and measured service availability
- Minimal management
- Shared solutions – fast, effective and replicable, proven by thousands
- Dedicated leading edge solutions with 99.5 % availability
- 24x7 coverage through the MSS SOC