CSP Managed Endpoint Protection:
Bitdefender Cloud Security for Endpoints

Bitdefender®

New ransomware variants and other zero-day threats routinely bypass traditional anti-virus / anti-malware security.

Using advanced behavior-based technologies, Bitdefender detected 99% of unknown threats in independent trials run by reputed independent testing organization, AV-Comparatives.

Bitdefender's centralized, cloud-management platform links directly with CSP's remote monitoring and management solution, Solarwinds MSP. Rest easy knowing CSP's NOC is monitoring your devices 24x7 for security threats.

Why Bitdefender:

Advanced Application Behavior Monitoring
Bitdefender Advanced Threat Control (ATC) permanently monitors running processes for signs of malicious behavior. A pioneering technology launched in 2008 as AVC, ATC has constantly been enhanced, keeping Bitdefender one step ahead of emerging threats.

Largest Security Intelligence Cloud
With over 500 million machines protected, the Bitdefender Global Protective Network performs 11 Billion queries per day and uses machine learning and event correlation to detect threats without slowing down users.

AI and Machine Learning Perfected
Artificial Intelligence and machine learning are essential to combat a threat landscape that is larger and more sophisticated than ever. Unlike other vendors, Bitdefender has years of experience in perfecting these technologies and the results clearly show this: better detection rates with fewer false positives.

BITDEFENDER IN NUMBERS

- 500 Million: Endpoints Protected
- 11 Billion: Security Queries Per Day
- #1 Ranking: Size of Worldwide Security Infrastructure

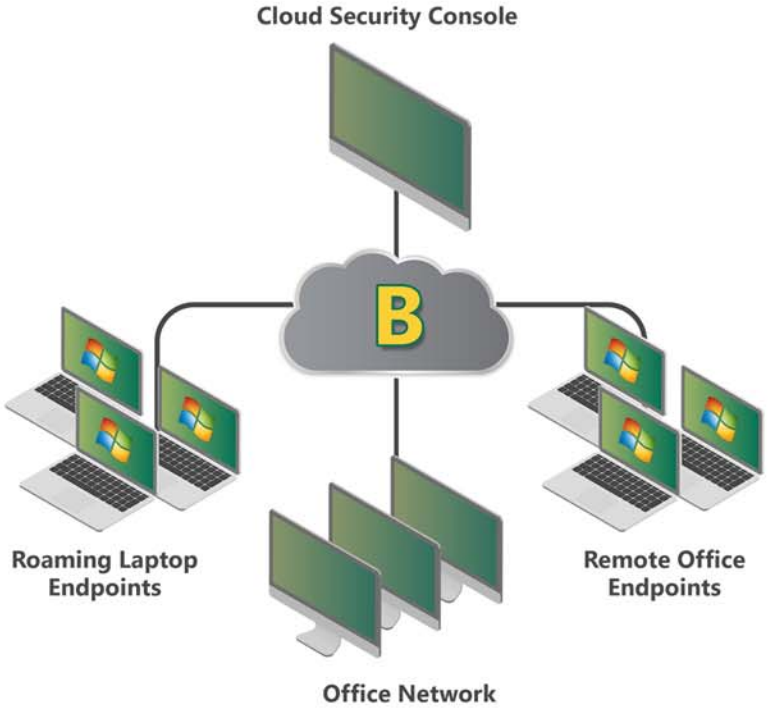
KEY BENEFITS

- Seamless integration with Solarwinds MSP for 24x7 monitoring by CSP's NOC
- Provides number-one-ranked anti-malware technology
- Protects and controls laptop, desktop and server endpoints
- Offers instantly available enterprise-class endpoint security with no on-site management server overhead
- Centrally manages any number of endpoints distributed across any number of locations

CSP
Your IT Partner

CLOUD SECURITY FOR ENDPOINTS

Organizations that thrive on being agile will find the Cloud Security for Endpoints service ideal for their needs. While it provides robust security, the solution does not require a highly technical person to deploy, manage or maintain. Immediately after subscribing to the service, Cloud Security Console becomes available allowing centralized deployment within the network using the automatic network discovery feature. After defining policies for the company or user groups, additional actions are required only to monitor reports and respond to incident alerts.



Reduced costs through simplified infrastructure

Cloud Security for Endpoints is a hosted service that offers a high level of security for business systems without introducing complex and costly infrastructure within the business. Companies can thus save money by eliminating the need for onsite hardware and associated maintenance. Dedicated IT staff is not required to manage and maintain Cloud Security for Endpoints because the interface is highly intuitive and there is no effort required to upgrade to a new version as the console is based in the service provider datacenter and is always up-to-date. Organizations can quickly deploy and adopt the enterprise-level security solution while maintaining a lean structure and avoiding vendor lock-in.

CSP
Your IT Partner

cspinc.com | 1310 Nowell Road | Raleigh, NC 27607 | (919) 424-2000

CLOUD SECURITY FOR ENDPOINTS

Number-one-ranked security

All of our AV solutions include B-HAVE, a patent-pending technology which analyzes the behavior of potentially malicious codes inside a secure virtual computer environment, eliminating false positives and significantly increasing detection rates for new and unknown malware.

Our AV has won the AV-TEST Best Protection 2011 award for consistently achieving superior results in independent comparative tests throughout the year.

System Requirements

Cloud Security for Endpoints is intended for workstations, laptops and servers running on Microsoft® Windows. All of our Cloud Security solutions are managed by Cloud Security Console. Since Cloud Security Console is hosted, there are no onsite hardware or software requirements for managing Cloud Security for Endpoints. All that is needed is an Internet connection.

Minimum Endpoint Requirements:

Workstation: Windows 7, Vista (SP1), XP Home/Professional (SP3), Embedded Standard 7/2009

Server: Windows SBS 2011, 2008 R2/ SBS, 2003 SP1/R2/SBS, Home Server

Internet connection: Internet Explorer 8+, Mozilla Firefox 4+, Google Chrome, Safari or Opera for endpoint browser security or accessing the Cloud Security Console

Processor: Intel® Pentium compatible (32/64-bit), 800 MHz (Windows XP), 1 GHz (Windows 7, Vista), 1.5 GHz (Servers)

Memory: 256 MB (Windows XP), 1 GB (Windows 7, Vista, 2008, 2003), 1.5 GB (SBS 2003), 4 GB (SBS 2008), 8 GB (SBS 2011) Hard disk: 1 GB

Optimized to minimize resource consumption

Optimized detection and scanning technology inside Cloud Security for Endpoints minimizes the system's memory footprint. Together with the silent security philosophy, this ensures that business data and systems are protected without users noticing or taking any action. The impact of Cloud Security for Endpoints on network traffic is also minimized as new product or signature updates can be propagated with small, incremental updates and optimized local update distribution options are available.

Advanced protection through proactive detection

Our industry leading provides organizations with multiple levels of advanced protection: Antivirus, Antispyware, Antiphishing, Trojan / Rootkit detection and a fully featured two-way personal Firewall with intrusion detection. Cloud Security for Endpoints also includes an innovative and proactive detection technology called Active Virus Control which leverages advanced heuristic methods to detect new potential threats in real time. Unlike typical heuristic technologies which are limited to checking files when they are accessed or first started, Active Virus Control monitors all application activity throughout the lifecycle of the application processes. Productivity and protection are enhanced through centralized confi gurable security policies that can be used to remotely control user access to local applications, block access to certain websites or restrict Internet access within certain time intervals.

For more Information
Contact CSP at (919) 424-2000
or info@cspinc.com

CSP
Your IT Partner