

End-Point Security—Protect Your Computers and Data

Alliance Technologies' managed end-point security protects your business from malware, viruses and other undesired software. We offer several packages to allow you to choose the appropriate level of security and control. Our solutions are built upon industry-leading software and our highly-trained Help Desk personnel.

Features

Antivirus/Anti-malware

Anti-malware software monitors machines for viruses, trojans, worms, spyware and adware. Computers are managed from a centralized console to ensure that the software is protected against new threats. Real-time protection blocks known malicious websites. Monitoring of updates and security status, and malware detection is performed daily by Alliance Technologies. In most cases, the software automatically remediates issues in which malware is detected. If significant issues occur, clients are notified quickly.

Host Intrusion Prevention System (HIPS)

HIPS is a second layer of defense against malware, and works by monitoring applications for suspicious behavior. This allows the system to block new malware families that do not yet have definitions. Poorly written applications that must be used for business reasons can be allowed, while suspicious new files can still be blocked.

Firewall

Malware will often try to spread within a network, so if it infects one system, all systems are at risk. It is no longer sufficient to rely solely on the perimeter firewall to protect your business; internal firewalls are required as well. The firewall included with the *Full Control* and *Compliance* packages protects against internal attacks, and protects laptops that leave the network. There are both strong and weak policies available, so the firewall can be tuned to needs of the business.

Device Control

Storage devices (such as thumb drives and removable hard drives) and network interfaces (such as Bluetooth or Wi-Fi) can be blocked or allowed as part of a strategy to reduce the risks of data loss and malware infection. They can also be prevented from "bridging"—allowing your primary network to communicate with wireless networks. Device control allows you to define which employees are trusted with the ability to copy data from your network and which ones are not.

Application Control

If users have administrative privileges, malicious software can be run that disables the existing anti-malware system. Since many older applications require these administrative privileges, this is a very common attack technique. Application Control helps by allowing employees to run what they need while blocking applications that could impact security or productivity.

At the lowest tier, Alliance defines a standard set of blocked categories, such as older browsers and readers, file sharing applications and applications that could bypass security controls. At higher tiers, Alliance will work with you to define rules that best meet the business needs. At present, Alliance recommends that the only browsers used in a business be Firefox 3.5 and up and Internet Explorer 7 and up. Similarly, we block all versions of Adobe Reader older than 8.

Data Loss Prevention (DLP)

DLP monitors the transfer of sensitive data, such as credit cards numbers, Social Security numbers and personally identifiable information (PII), and attempts to prevent them from leaving the network. Such transfers can be allowed, blocked or simply reported to an HR or data owner within your organization.

Note: Some uses of this technology may affect common tasks such as using media players from a protected system. Business goals should be discussed before this feature is activated.

Supported Platforms

Alliance Technologies provides this service for all versions of Windows that Microsoft maintains. At present, that includes Windows XP SP3 systems and newer. If you wish to protect non-Microsoft systems such as Linux or OSX, please contact us.

Package Tiers

| Service | Basic | Full Control | Compliance |
|--|-----------------|--------------|------------|
| Anti-malware | ✓ | ✓ | ✓ |
| HIPS | ✓ | ✓ | ✓ |
| Firewall | – | ✓ | ✓ |
| Device Control | – | ✓ | ✓ |
| Application Control | <i>see note</i> | ✓ | ✓ |
| DLP | – | – | ✓ |
| Setup Fee (once per device) | \$15.00 | \$15.00 | \$15.00 |
| Configuration Setup (once per package) | – | \$450.00 | \$950.00 |
| Price Per Month (per device) | \$3.00 | \$5.00 | \$7.00 |

Basic—Our basic offering includes anti-malware protection with limited application blocking. It is best suited to businesses on a budget that are willing to accept an increased level of risk in exchange for a reduced monthly cost. These businesses should be unregulated, not run with local admin rights and not use laptops from other networks.

Note: Application control in this package is maintained by Alliance Technologies. We choose the applications to block based on our experience with applications that affect security and workstation performance. While a business may request changes to this list, the final decision is up to Alliance. Custom lists require either the Full Control or Compliance packages.

Full Control—Our mid-tier package includes *Basic*, but also adds tighter security through client-configurable application blacklisting, a software firewall and device control. This is a good fit for unregulated businesses, and is strongly recommended for any business that grants users local admin rights or allows its laptops to leave the office.

Compliance—Our top-tier package includes *Full Control* and adds data-loss prevention (DLP). Businesses required to protect health, financial or privacy information can use the reports to demonstrate compliance. It is strongly recommended that regulated businesses accept credit cards or work with health and financial data choose this package.