



MANAGED SECURITY SERVICE

Savvy executives and regulators realize that monitoring and **immediate response** to security events is critical to protecting the organization's information assets and ensuring business continuance. The rapidly growing level of sophistication found in today's security threats has mandated vigilant 24x7 security programs.

The Managed Security Service offered at BAI Security was designed to meet the monitoring, response, and reporting requirements of today's highly regulated industries. By utilizing our Managed Security Services you're helping to assure your organization is protected at the highest level and providing peace of mind to everyone from your customers to your organization's board of directors.

Managed Firewall: One of the most basic and mandatory security devices in your network is the traditional firewall. The firewall is generally the first roadblock to malicious attacks and random security events against your organization. If your staff is not monitoring for these initial signs of unauthorized access and denial-of-service, you are far more likely to become a victim. If you are not monitoring and your organization is subject to government regulation, you are likely non-compliant.

Actively monitoring your firewall takes expertise and resources to filter out the massive amounts of data collected by these devices. BAI Security utilizes expert systems backed by security engineers to ensure that attacks against your organization are not overlooked and you meet compliancy guidelines.

Virtual Private Network (VPN): Virtual Private Networks (VPNs) are essential for protecting data transmitted across public networks, such as the Internet. In addition, encrypting data by using VPN technology is required in highly regulated industries. BAI Security takes VPN technology a step beyond typical implementations by actively monitoring the transmissions to ensure they do not contain security threats, viruses, spyware, or inappropriate content.

BAI Security is also one of the first Managed Security Service Providers (MSSP) to provide SSL-based VPNs. This technology allows remote users to connect into the organization from any PC on the Internet after proper authentication. This is a major breakthrough as many users access internal systems from coffee shops and popular eateries and now it can be done securely.

Intrusion Detection / Prevention: Today the vast majority of security threats are designed to circumvent the firewall by disguising themselves in legitimate network traffic (i.e., email, web browsing, data transfers, etc.). The Intrusion Detection / Prevention System (IDS/IPS) monitors the traffic allowed by the firewall and looks inside it for threats, which makes it the perfect compliment to the firewall.

It is critical and required for regulatory compliance to monitor the IDS/IPS system so that you are aware of what malicious activity is threatening your organization. Monitoring the extensive data from an IDS/IPS system takes highly trained staff and significant resources. BAI Security utilizes expert systems and senior security engineers to identify the true risks and ensure your systems stay secure and your organization stays compliant.

Antivirus Protection: The importance of AntiVirus Protection is now common knowledge and most



organizations have it in place, and of course regulated industries are required to have it in place. One of the downsides to traditional AntiVirus is that they can be updated only by the AV vendors, which can cause delays.

BAI Security's AV protection is also unique in that we monitor not only email, but other data such as file transfers and web browsing. We block all viruses at the Internet gateway before they enter your internal network.

Data Leakage Protection (DLP): With increasingly sensitive, confidential, and proprietary data being communicated across networks, the ability to keep that information within defined network boundaries is imperative. Working across multiple applications (including those encrypting their communications), BAI's Data Leakage Protection (DLP) uses a sophisticated pattern-matching, as well as a regular expression engine to identify then prevent the communication of sensitive information outside the network perimeter.

In addition to protecting an organization's critical information, BAI-DLP also provides audit trails for data and files, which can aid in legislative compliance. With configurable DLP actions, BAI's Managed Security Service can log, block, and archive data, as well as ban or quarantine users.

Spyware / Malware Protection: One of the fastest growing threats to information security today is Spyware and similar malicious code deemed "Malware". These bits of code and data most commonly find their way into your environment by being embedded in seemingly legitimate web sites. Once resident on PCs inside your network they monitor activity and occasionally report back to central data warehouses where, at best, the information is used for marketing purposes. However, a growing threat today is the data collected

includes account, logons, and possibly password data collected from production PCs.

BAI Security's Managed Security Service protects against Spyware/Malware and helps organizations stay compliant by blocking the Spyware/Malware before it reaches the internal PCs.

Email Content & SPAM Protection: Email has become one of the most common forms of communication within organizations. It has also become one of the most common ways that legitimate and more importantly non-legitimate vendors market to a world-wide audience. As most people know, unwanted email (SPAM) can be a major waste of time. What many people do not realize is that unwanted email can also be a security threat to an organization by containing malicious code.

BAI Security helps to nearly eliminate SPAM before it reaches and overwhelms your internal email server and/or fills your already full inboxes. Our Managed Security Service validates each piece of email in real-time and discards SPAM before it wastes your resources or it's payload infects your network.

Website Filtering: Web access is a key vulnerability point for your organization. Inappropriate employee behavior can expose your network to security threats and legal and regulatory liability, as well as impairing both productivity and system performance. To protect your business integrity, you need a solution that can monitor and detect policy violations across the full spectrum of Web-based content: IM, P2P, streaming media, file downloads, and Web-based e-mail.

BAI Security's Managed Security Service provides this protection in real-time and actively blocks unauthorized applications and/or inappropriate websites. In addition, we provide detailed reporting to help identify problem users and demonstrate compliance to regulations and company policy.