

Allied InfoSecurity Managed Security Services: Meeting your needs for comprehensive, high-value security services

Effectively managing your organization's information security program can be complex, overwhelming, and costly. You may find it difficult to focus on your core business and strategic goals while juggling ever-increasing day-to-day security demands. If you're continually challenged by the demands of your information security program, consider Managed Security Services from Allied InfoSecurity.

Allied InfoSecurity provides a flexible and comprehensive suite of management and monitoring services that we can quickly adapt to your organization's specific needs. Just as important, you save time and money because we deliver this extensive suite of services using your existing infrastructure. There's no need to change your Internet Service Providers (ISPs) or replace your current security investments.

Choose Allied InfoSecurity Managed Security Services when you need to address any or all of the following aspects of your information security program:

- Firewall monitoring and management
- IDS/IPS monitoring and management
- Continuous threat management
- Security Information and Event Management (SIEM)
- Additional security device monitoring and management
- Policy compliance monitoring
- Archiving and management of security logs

Allied InfoSecurity delivers Managed Security Services through three core elements: the Security Operations Center (SOC), the netSensor™, which is placed on your network, and the Security Information and Event Management (SIEM) system.



“With Allied InfoSecurity Managed Security Services, you can quickly deploy a customized suite of services to meet your organization's specific day-to-day security needs.”

About the Security Operations Center

Allied InfoSecurity supports managed security clients through a Security Operations Center (SOC) housed in a SAS70 certified data center. This state-of-the-art facility has been designed to support security, redundancy, and reliability through:

- Access to multiple fiber networks
- Redundant commercial power grids
- Uninterruptible power and backup power generation systems
- Video surveillance and biometric security

Maintained to the highest security standards—including hardening, backup, and redundancy—the SOC is designed to operate as a “virtual SOC”. Thus, in the event of a disaster or other incident, our security analysts can securely operate from any location. With this technology and supporting processes, Allied InfoSecurity is able to provide a 99.9% service level guarantee on our managed security services.

In addition to the SOC, Allied InfoSecurity maintains an isolated security lab environment. Equipped with a variety of leading-edge commercial and open-source technologies, this lab enables our analysts to research the latest trends and threats affecting our clients. We use those insights to support prevention and faster detection of threats on your network.

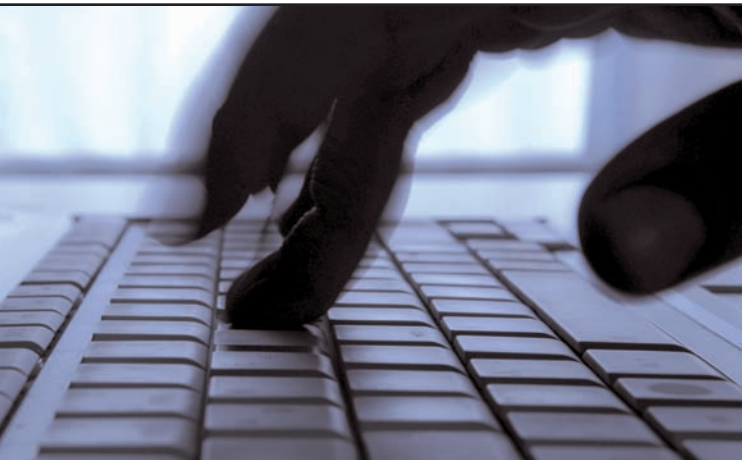
About the netSensor™

Allied InfoSecurity has designed the our Managed Security Services to facilitate information security management of distributed networks. At the heart of this solution is the netSensor™—a rack-mountable, secure, and hardened Linux-based appliance. The netSensor™ is installed on your network and acts as the centralized point of security management and monitoring for your network—and is the key to providing secure, remote managed security services.



Depending on the package of services you select, we inspect all traffic, detect attacks through various methods, and collect information on attack context without affecting your network performance.

We compress the data we collect or generate through the netSensor™ and then use point-to-point Secure Socket Layer (SSL) Virtual Private Network (VPN) technology to transmit it to our SOC. This SSL-VPN communication serves as a secure outbound tunnel across the Internet—from the netSensor™ on your network to our SOC. The SSL-VPN connection uses the standard SSL port (443) so generally there no changes to your infrastructure required to support this secure communication tunnel.



The Allied InfoSecurity Value Proposition

- Highly trained, certified security analysts
- 24x7x365 service and support
- Guaranteed service levels
- Support for all popular security hardware and software
- Flexible, tiered service options

Security Information and Event Management: Part of every Managed Security Services agreement

Using best-of-breed open-source technologies, Security Information and Event Management (SIEM) provides a complete security information correlation solution—from low-level detection to high-level reporting. Allied InfoSecurity includes this capability with all of our Managed Security Services agreements.

Through SIEM, we collect and analyze logs from your netSensor™ or any number or type of network devices, such as firewalls, IDS/IPS, routers and switches, operating systems, or applications. Thanks to integrated management tools, our analysts are able to make sense of vast amounts of data—rapidly analyzing and responding to immediate threats and gaining visibility into the risks that apply to our customers.

Automated tools simultaneously collect vast quantities of data about an enormous number of events. They also enable our analysts to find patterns and to filter, clean, and analyze all that data—so they can help you formulate a rapid and effective response. Through the ongoing collection, correlation, and analysis of data from distinct sources, the SIEM also provides intelligence for prioritizing or ruling out a potential attack.

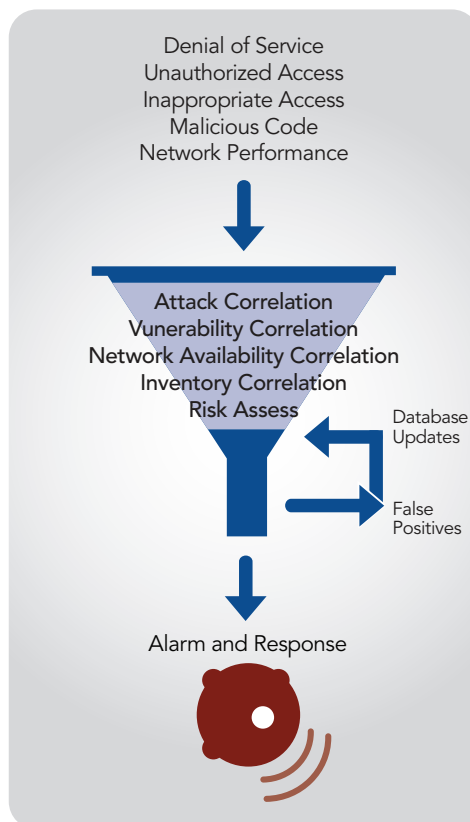
This sophisticated event detection and management differentiates Allied InfoSecurity Managed Security Services from competitive offerings. Our approach delivers near-real-time situational analysis and risk assessment for each event received.



The correlation engine is able to track complex patterns across multiple variables—from vulnerability, degree of anomaly, and network status, to service availability, inventory, and value of the equipment and assets involved.

Discovering and tracking new patterns is critical to our ability to identify the distributed or abstract attacks that classic detection systems miss. A number of powerful threat-mitigation tactics are made possible through the correlation of contextual data. For example, combining

knowledge of known vulnerabilities, inventory and asset value, and network data allows us to filter out a large number of attacks that will not affect a target operating system; to prioritize attacks involving a service known to be vulnerable; or to monitor the status of a network or service subject to a denial of service attack. In other words, not all threats are created equal. We've designed our Managed Security Services with sophisticated capabilities that uncover these nuances and allow them to be addressed appropriately. And the more managed security services you retain, the more comprehensive and accurate your SIEM program will be.



The bottom-line benefits

Whether you retain Allied InfoSecurity for a single capability or a comprehensive suite of services, our Managed Security Services can deliver a number of compelling benefits to your organization, including:

- Reduction in total cost of ownership (TCO). Managing a world-class, 24x7x365 information security program is typically an expensive and resource-intensive undertaking. Costs for staffing, equipment, support, and maintenance often spiral out of control. Outsourcing your critical information security functions to an industry leader can help reduce TCO while improving your overall information security posture.
- Ability to refocus in-house resources. You know your business and at Allied InfoSecurity, we know security. Through our Managed Security Services, your organization can transfer the burden of day-to-day security management to our focused and experienced security experts—freeing up your people to focus on your core business objectives.
- A proactive approach to security. In today's challenging environment—where resources are tight and in-house personnel are overwhelmed with responsibilities—security often takes a “back seat” to core business objectives. But that can lead to increased risks and potential compromise of your systems and data. At Allied InfoSecurity, our analysts have a singular focus: providing world-class security monitoring and management. We keep a close watch on your security—helping prevent incidents and saving you from the often costly and damaging task of “cleaning up” after a breach.
- Dedicated security professionals. Information security technologies change as quickly as the threats they're designed to prevent and detect. It isn't easy to keep up with the continual change. By combining open-source technologies and a team of dedicated, certified information security specialists, Allied InfoSecurity helps keep your organization ahead of the curve.

To learn more about Allied InfoSecurity Managed Security Services, please visit our website at www.alliedinfosecurity.com or call us at 866-240-0094.



About Allied InfoSecurity, Inc.

An independent company focused only on security and staffed by certified security professionals, Allied InfoSecurity is a consulting and outsourcing provider that helps businesses improve and manage their information security programs, mitigate risk, and respond to regulatory and marketplace demands more quickly and effectively than they could on their own.

© 2010 Allied InfoSecurity, Inc.

The above material is presented as general information only and does not constitute legal advice or a legal opinion. You should seek the advice of legal counsel with respect to your particular circumstances.

1009 West 9th Avenue, King of Prussia, PA 19406 • tel: 866.240.0094
email: ask@alliedinfosecurity.com • web: www.alliedinfosecurity.com

**Allied
InfoSecurity**
Your security is our business.