The greatest threat to your organisation's information system integrity is the undetected breach of your I.T. controls. Timely detection and response to information security breaches can mean the difference between a minor inconvenience and a catastrophic failure of the organisational information environment.

We realise that to maintain an effective in-house 24x7 Information Security Management system is a costly, resource-heavy and an unrealistic exercise well beyond the budget of most organisations.

The widely accepted security posture paradigm embraced by most organisations seeking to be proactive in securing their information systems is to take the position of “Assume we are breached, and assume they will get in through our perimeter defences”.

IPSec Guard is your entire Information Security Management department, expertly providing the detection & prioritisation of security tasks, freeing up your IT team to focus on what they do best.

IPSec Guard is designed to provide your organisation with a 24x7 Security Operations Centre monitoring your IT systems for indicators & evidence of information security breaches. IPSec Guard can receive all of your IT system log information; will process and correlate that information in real time identifying data and trends that may suggest an impending security threat; and will notify you when a potential threat warrants investigation and response.

**Features & Benefits:**

- Your 24x7x365 manned security operations centre
- 24x7x365 monitoring of your IT systems logs for security events
- Real-time awareness of impending or active information security threats
- 24x7x365 access to your correlated log data via the IPSec Guard customisable web console
- Access to the world’s leading SIEM log management & correlation engine.
- Access to an extremely powerful log search engine

IPSec Guard offers piece of mind for an affordable fee.

**IPSec Guard addresses five key issues:**

1 - **Always On**

Information security threats are a 24x7 issue for every organisation.

2 - **Big Data Analytics**

Processing 100’s of millions of log entries every day is impossible without powerful big-data processing tools.

3 - **Powerful Correlation**

Identifying priority security events is like searching for a needle in a haystack.

4 - **Greatly Reduce Cost**

Establishing and maintaining a team of information security specialists to respond to incidents is expensive and time consuming.

5 - **Knowledge is Power**

Security events are most often hidden amongst the logs of many sources and are rarely evident from one data source alone.
About IPSec

IPSec are specialists in information asset security; technology experts who know how to mitigate risk to business by implementing end-to-end solutions that protect invaluable intelligence, data and information.

Their capabilities extend from assessing vulnerabilities and threats, to designing and implementing customised security strategies, to managing execution and optimising results. IPSec are guardians of business confidence, providing high levels of protection and optimal assurance of an organisation’s security posture.

IPSec is about mitigating risk, enabling confidence and agility by ensuring a reliable IT environment that allows business to get on with business.

Reduced Time to Detection & Response

IPSec Guard is designed to provide your organisation with powerful tools and a manned 24x7 security operations centre (SOC) to dramatically reduce the time to detecting breaches of your IT environment, to dramatically reduce the time to response & mitigation, and thereby to dramatically reduce the potential exposure and cost of an information security event.

Compliance

Many organisations are pursuing compliance objectives for standards such as ISO27000, PCI-DSS and many others; each of the standards targeting information security outcomes include the need for effective log management and reporting. IPSec Guard is designed to assist organisations seeking compliance with most information security standards by providing a robust log management platform, combined with a powerful search and correlation engine, delivering useful information via a user-friendly web console and highly configurable reporting.

Cost Savings

Most organisation IT environments generate millions and potentially billions of log events every day, with each individual log attempting to convey an important message and combinations of logs undertaking to inform IT administrators of threats to their environment. Requiring personnel to process such volumes of logs would cost the organisation 100’s of thousands of dollars annually, let alone if they desire to do this on a 24x7 basis.

IPSec Guard provides a powerful log management & correlation solution capable of processing vast amounts of IT solution event logs and presenting a user-friendly interface capable of highlighting important issues occurring within the organisation’s IT environment. IPSec Guard provides a manned 24x7 security operations centre (SOC) that will respond when an event of sufficient priority occurs, allowing your staff to sleep soundly knowing that the IT environment is being monitored.

IPSec Guard will significantly improve the visibility of important events, will dramatically reduce the time to respond to & mitigate threats, whilst saving the organisation significant costs.

Data Sources

IPSec Guard is capable of receiving logs and events from a huge number and variety of data sources and data source types. A single IPSec Guard data collection point is capable of collecting and transmitting up to 10,000 messages per second from thousands of devices.

IPSec Guard is capable of collecting, correlating, and analysing logs and events from 750 unique data source types and is capable of being configured to handle events from your bespoke IT applications. IPSec Guard is capable of processing almost any data source type utilising any of the following log/event communication mechanisms:

- UDP/TCP and Secure Syslog
- Windows Event Log
- Single & Multi-line Flat Files
- Cloud/SAAS Solutions
- Amazon AWS
- Salesforce
- Box
- Office 365
- Database Logs
- Oracle
- SQL Server
- MySQL
- Etc.
- Vendor APIs
- Cisco SDEE
- Check Point OPSEC
- AS/400 & iSeries
- Sourcefire eStreamer
- Tenable Security Center
- McAffee ePO
- Cradlepoint
- Vulnerability Scanners
- Active Directory

Phone 1300 890 902
ipsec.com.au
enquiry@ipsec.com.au

Building 10, Omnico Business Centre
270 Ferntree Gully Rd, Notting Hill
VIC 3168, Australia