

Services

Business requirements drive security and not the other way around

We do not come in with a standard set of predetermined recommendations or solutions and then fail to take into account what actually drives any particular client's business. Our methodology starts by focusing on our client's business. Only when you understand how the systems and networks are used, the value and sensitivity of the information on them, and the client's budget and time constraints, you can begin to make meaningful technical recommendations.

Security Solutions

Security is a continual process, and proper knowledge, practices, and tools are imperative to its success. Bsecure offers the services and tools to facilitate the job, and delivers the expertise to provide a complete solution that will grow with your environment. Proper implementation typically consists of several components, which used properly provide you with a platform that can be grown as business dictates.

Audit & Assessment

The Risk Assessment, Penetration Testing, and Health Checks performed by Bsecure enable our clients to identify the weak and high risk components in applications, networks, data bases, and operating systems, these assessments and audits are essential and provide a "Health status" to confirm that the information security and the risk management processes are implemented and are properly functioning. By mimicking hacker's techniques, the professionals of Bsecure try to penetrate Data bases, application servers, web servers, file servers, mail servers, and other assets VIA remote access servers, internet, intranet, and wireless networks.

We provide Social Engineering services in Australia which revolves around human interaction and primarily involves tricking your staff into breaking security procedures. Social engineering techniques can be integrated into our security testing method if required. Our services are catogrised into two group:

Internal Social Engineering

External Social Engineering

These services are unique in australia and will test your organisatio's security awareness and how much information your staff will divulge. For more information about this service please email us at sales@bsecure.com.au.

Firewall Service

Today's organizations rely on highly available, secure computing environments to efficiently and safely conduct business. Firewalls are a key component of a secure network and must be managed properly to ensure they protect your critical information assets.

Firewalls are configured to allow "good" traffic in and to keep "bad" traffic out. Firewalls are updated continuously to support changing business requirements such as:

- New VPN users
- Employee status changes
- New partners
- New applications

Firewall management is extremely resource intensive and requires a high skill level. Because of the effort and complexity involved, a majority of firewall breaches are caused by the mis-configuration of firewall rules and policies themselves.

Service Overview

Bsecure's Managed Firewall Service provides 24x7x365 proactive administration of your firewall infrastructure. Bsecures' certified security experts will perform all activities necessary to keep these devices operating at peak performance including:

- Site assessments
- Firewall policy design, equipment installation and configuration
- Firewall monitoring and management

- Comprehensive reporting and emergency response
- Log Monitoring

Bsecure manages all market leading firewall technologies including Cisco, Check Point and Juniper. Our experts hold certifications from leading vendors and have deep experience managing these technologies in all types of environments, from the simplest to the most complex. This enables your team to make the right technology choices, while allowing us to support your current and future firewall infrastructure.

Our experts will monitor your firewall logs for security events in real-time. Firewall logs are an extremely valuable source of security information. By monitoring these logs our experts can identify malicious activity including previously unknown, zero-day attacks. Our experts will also monitor your firewalls for performance and availability to ensure your business never goes offline.

Service Features

- Rule set changes and validation
- Configuration changes
- Firewall upgrades
- Patch management
- General maintenance
- Backup and recovery
- 24x7 security event monitoring
- Performance and availability management
- Strategic network planning
- Fault analysis
- On-demand reports

Network Intrusion Prevention and Detection Service

Network Intrusion Prevention and Detection is a highly effective layer of security you can implement to protect your organization from unauthorized access. Many devices promise to provide this protection. However, it is difficult for most organizations to respond to alerts, apply continuous updates, hire and train staff, and provide vigilant monitoring 24x7.

Our customers have found it more effective to augment their staff with our team of certified Security Analysts who focus exclusively on

security.

Bsecure Managed Intrusion Prevention and Detection Service protects your critical information assets from existing and emerging threats. Our Intrusion Prevention and Detection System (IPS/IDS) experts will perform all management and maintenance of these devices including:

- Signature tuning
- Signature updates
- Configuration changes
- Security event monitoring
- Performance and availability management

Bsecure Managed Intrusion Prevention and Detection Service supports market-leading IPS/IDS technologies including Cisco, Juniper, Sourcefire and others. All alerts generated from across your IPS/IDS infrastructure are aggregated and correlated in real-time. Our expert Security Analysts will monitor these alerts, eliminate false positives and escalate true threats to your organization.

Bsecure Network Intrusion Prevention and Detection Service provides comprehensive reports so that you have immediate and transparent access to your security status. All reports are based on real-time information and can be accessed on-demand through the secure, web-based Portal.

Service Features

- Total lifecycle management of your Intrusion Prevention and Detection infrastructure
- Support for all market leading Intrusion Prevention and Detection technologies
- 24x7 live monitoring from the Security Operation Center
- Protection against hacker attempts before they compromise your network
- Continuous research and updating of attack signatures
- Customizable escalation matrix

Encrypted Email Service

With increasing concerns for protecting confidential customer information as well as patient privacy, companies are turning to Encrypted Email Service to ensure that all emails containing sensitive information are automatically encrypted based on central policies.

Benefits

- Increase customer confidence
- Protect customer account, identity and health information
- Keep information safe from outsiders including: intellectual property, strategy, pricing, launch schedules, blue prints, etc.
- Keep information safe from insiders including: reorganizations, staff reductions, plant closures, acquisitions & mergers, personnel actions, etc.
- Keep track of activity, measure effectiveness of privacy controls, and refine policies with easy-to-use reporting

Service Overview

Whether driven by regulation or simply good security practice, encrypting data in transit is an important part of corporate security. Bsecure Encrypted Email Service provides airtight security for email messages without burdensome processes for email administrators or end-users. This service:

- Automatically encrypts email using centralized policies to define confidential information
- Ensures that end-users do "business as usual" and do not require training
- Allows Recipients to open encrypted email from a secure portal
- Provides reports for operational oversight and compliance readiness