

E N E X T E S T L A B

SECURITYCAPABILITYSTATEMENT

E N E X S E C U R I T Y T E S T I N G D I V I S I O N

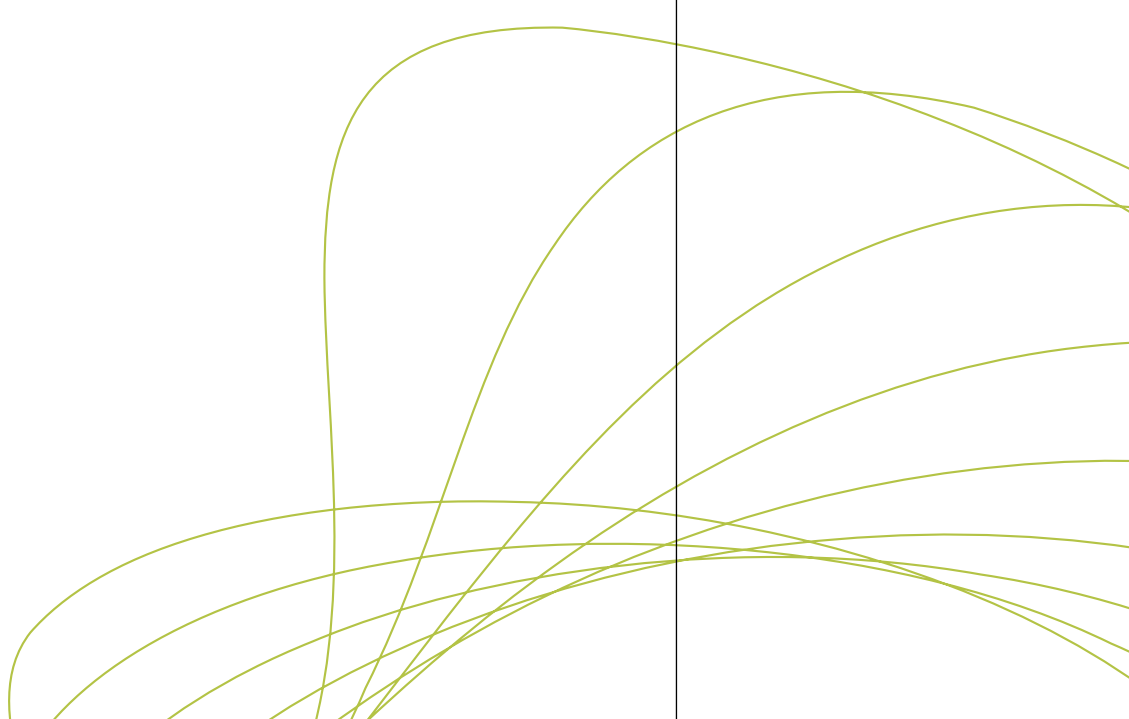
testlab
an enex enterprise





contents

ENEX TESTLAB SECURITY SYSTEM TESTING	2
WHY TEST SECURITY SYSTEMS?	3 - 6
EXAMPLE	6
SPECIAL PUBLICATIONS	8-10
NIST SP 800-42	9
ISECOM OPEN-SOURCE SECURITY TESTING METHODOLOGY	10
ENEX TESTS	11-15
LOAD AND STRESS TESTING	13
EXAMPLES OF COMMON ENEX SECURITY TESTING PROJECTS	14
SUMMARY	16





Enex TestLab has achieved an enviable reputation drawing on decades of independent ICT product testing.

Introduction to Enex TestLab Security Testing

Enex TestLab has achieved an enviable reputation over decades of independent ICT product consultancy and testing services.

With a heritage stemming directly from RMIT University, Enex TestLab's expertise reaches far beyond simple testing. We provide a complete range of high quality, independent testing services across all ICT technologies and systems for government and corporate clients internationally.

Enex TestLab is renowned for providing innovative testing services. Since 1989 Enex TestLab has been contracted to perform rigorous and detailed tests on a countless variety of technologies. We have saved huge amounts of money for organisations large and small by scientifically testing their ICT products or applications - highlighting issues before their release.

We are passionate about testing, but Enex TestLab offers more than simply reducing risk and saving you time and money. With unparalleled experience, history, independence, rigor and accuracy Enex TestLab's clear focus on customer needs makes it one of the world's leading ICT service enterprises.

Enex boasts extensive resources, with cutting edge facilities, custom developed software, comprehensive reporting and proven delivery. Enex TestLab can deliver the vital strategic edge to your security system.

Enex TestLab is certified to ISO 9001:2000 and is a ISO17025:2005 accredited test facility and NATA test laboratory. The principal Enex TestLab consultants hold high level security-specific certifications including CISSP, CISM, CISA, CSEPS as well as memberships with international IS security organisations such as ISACA, ISSA, ISC2, AISA and ISSA.

why test security systems?

Why test security systems?

The only way to ensure the quality of your security product, or service, is to test it!

Information Communications Technology (ICT) and indeed Information Systems (IS) themselves are very complex and gaps inherent in these products are vulnerable to exploitation. The gaps are easily overlooked by developers, vendors and clients.

ICT security systems are widely acknowledged by government, business and home users as key factors in any environment, yet time and time again, they are poorly procured, incorrectly deployed and severely mis-configured, leaving systems and business exposed and vulnerable. Testing proves the quality of your product. It empowers you to maximise its potential in the marketplace.

From a security users perspective

Security system vendors regularly rely on marketing and media hype to sell their products. The fear and doubt created ensures that security products sell well. Enex TestLab addresses this by providing real-world testing of the security products and services to guarantee that they;

- match the statements made by the vendors.
- meet the scope, requirements, functionality and environment the client plans to deploy them into.
- identify “hidden” issues or drawbacks that could result in simply transferring the security risks to another area within the system.

Enex TestLab provides comprehensive

independent ICT and IS security consulting services, strategic reviews, audits and reports. Augmenting this with practical, measured facts through our testing services.

We deliver a completely customised service focused on your needs, your procedures, your infrastructure and your systems.

From a security vendors perspective.

Enex helps guarantee your product. Enex can independently assure your customers they are buying a quality and verified product. Enex will reduce customers complaints, failure to convert, or worse – leaving.

Consider also the costs associated with rectifying faults and distributing patches and updates to integrate with the product once it has been deployed. Enex TestLab will save you time and money.

why test security systems?

What Enex can do for security users

The priority in any ICT or IS security system is to ensure that potential risks in an organisation have been identified. Enex will undertake a strategic review or an IS security audit.

The strategic review will be a complete overview of ICT systems and is suitable for organisations who have not previously implemented ICT/IS security programs.

It identifies risks to the enterprise under its current ICT/IS systems and security systems and can be used develop plans for mitigating and managing those risks. It takes a long term approach to addressing any issues identified and provides your organisation with a plan to work towards implementing and improving your security.

An IS security audit is for enterprises that have already defined ICT/IS security systems and have some level of understanding and control over its security program and the risks it seeks to address. An Enex IS audit provides (from an external and independent perspective) a review and evaluation of current security procedures and practices and provides indicators for improvement. It can identify undetected or changed risk profiles. IS security audits should be carried out regularly by internal staff as well as externally and independently.

Whatever stage your organisation is at, Enex TestLab's experience, skills and independence will bring quantifiable return on the investment.

ICT/IS strategic reviews and audits are fundamental strategies; however, they are only the first weapon. Enex TestLab is not just a "pure play" security testing organisation. We provide comprehensive, scientific and independent testing services that dramatically lower your risk and maximise return on investment whenever you are researching, developing, marketing, or introducing any technology product.

Enex TestLab's rigor has been widely recognised. We have regularly been contracted to bring the same diligence to testing outside of the ICT environment. In the past Enex TestLab has been commissioned to test products such as passports, crayons and office chairs. We apply the same patient rigor and careful methodology to these as we to any other.

The wealth of experience and skill at Enex adds value to our security consultancy and testing service through end-to-end testing of security technologies.

why test security systems?

Our testing services includes product testing, comparison, evaluation and benchmarking, development advice and assistance, not just for ICT/IS security but for all ICT hardware, software and systems.

Enex TestLab's services are offered across a wide range of vertical markets including;

- Public testing and content creation for media groups and publishers
- ICT procurement testing and reporting for large corporates and government departments
- ICT hardware testing for venture capitalists proof of concept (independent validation of statements), vendors research and development, simulation or emulation of client environment or on-site pilot/trial testing of new/proposed technology solutions and comparative/benchmarking of technologies
- ICT software performance, functional, load and stress, regression, compatibility, and maintenance testing. As well as test case creation, automated script programming and execution with a wide range of automated test suites
- Physical testing, environmental (eg. humidity, temperature), destructive, power consumption, weight, or if the product uses consumable components Enex TestLab can create test methodologies (to international standards) that physically test those products. In the case of consumables or power consumption results can be collected and total cost of ownership, return on investment and costs per item output can be

calculated

- Usability and accessibility testing including rapid systems and prototyping. User-centred design consultancy plays a critical component in services delivered to software, firmware and hardware developers ensuring their technologies are usable by their market
- Systems testing of end-to-end services and technologies such as networking, storage systems, broadband data managed services, Voice over Internet Protocol systems or service level agreements. Enex TestLab has developed independent tests and methodologies that can test complete end-to-end processes ensuring issues and bottlenecks are identified and addressed
- Enex TestLab's eMetric test product suite has been developed to test online systems such as websites for metrics such as performance and page load speeds from global locations. It has additional modular components such as the highly successful eMetric broadband performance test module. This can test internet data broadband networks for speed, latency and even availability from a remote end-user perspective as well as at the ISP network level including data packet transmission through the internet.

why test security systems?

An Example

Consider an electronic funds transfer point of sale terminal (EFTPOS). Enex TestLab's hardware division can test the devices functionality to ensure it complies with all requirements and functional scope as well as ensuring the device meets the vendors marketing and product statements.

Our software division can test management applications, network software and user-facing software/embedded firmware.

Enex TestLab can provide usability and accessibility tests to ensure compliance with requirements such as accessibility for users who may have vision impairment, colour blindness, motor control issues and so on, as well as providing advice on the user interface design.

Enex TestLab's physical testing division can test the terminal to destruction/end of life. This could range from day-to-day wear of the keypad and casing through to accelerated testing of the cable, drop testing or the device's reaction to a variety of substances and usage patterns it may encounter once deployed in the field. For example, if the terminal was used in a hardware store, the potential variety of substances that may come into contact with the terminal may include a variety of acids and chemicals.

Enex TestLab's systems testing division can test the end-to-end delivery system, from the terminal right back to the primary, secondary and tertiary data centres across a range of metrics.

This is in conjunction with Enex TestLab's ICT/IS security division that tests the encryption, quality and physical security of the device.

The complete test will be compiled into a converged independent product report covering, hardware, software, systems, physical and security. The report is written in plain English with executive summaries suitable for non-technical readers. It is simple to interpret and can also contain technical information for engineering/technical teams to utilise.

Testing any technology product from a security perspective decreases the risk of product failure or being compromised easily in a live environment. Security systems are costly to fix once deployed, and the risk of failure or compromise leaves the information being protected wide open. Testing by Enex will save you time and money.

testing with enex testlab

Advantages

Outsourcing your security testing to Enex TestLab offers advantages including:

- **Independence:** Enex TestLab provides objectivity and independence ensuring a realistic appraisal of where you are now with your security systems, and what is required to maintain or improve it.
- **Expertise:** Enex TestLab employs experienced security personnel. Enex TestLab staff have extensive security qualifications as well as proven real-world practical hands-on security experience. Several staff members are experienced ex-defence personnel who have worked in the technology research and development arenas. We have security specialists who have worked as Chief Security Officers in financial institutions. We understand ICT and IS security systems. We understand hardware and software and most importantly we understand how testing methodologies are applied to maximise results.
- **Outcomes focus:** We determine clear, practical and commercial action steps to ensure security systems are tested in accordance with your defined risk assessments and profiles.
- **Resources:** Our test environments represent the vast range of hardware and software that comprise your marketplace. We replicate prototypes or concepts of security environments or systems before they go into a live environment.

We also test in live environments. We have a wide range of automatic test tools that speed up the testing process or provide specific testing services.

- **Confidentiality:** Enex TestLab adheres to strict security, confidentiality and non-disclosure agreements protecting your security investment and edge.
- **Quality:** Enex TestLab is an ISO 9001:2000 quality controlled company, dedicated to continual improvement of its quality systems and procedures. And ISO 17025:2005 accredited. ISO 15408 is planned.

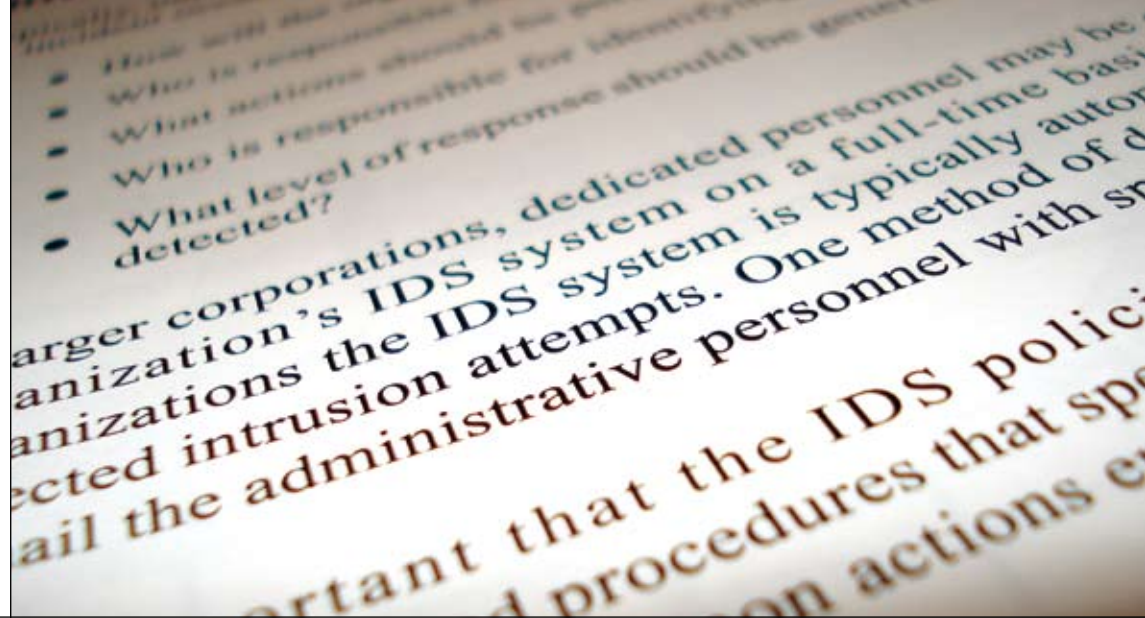
Our security testing services can be tailored to your exact requirements and business needs.

NIST special publication 800-42

Enex TestLab practically applies security technology testing to guidelines such as those found in the National Institute of Standards and Technology (NIST) special publication 800-42 and others.

800-42 addresses security testing techniques and processes such as;

- Security Testing and the Systems Development Life Cycle
- Documenting Security Testing Results
- Roles and Responsibilities for Testing
 - Network Scanning
 - Vulnerability Scanning
 - Password Cracking
 - Log Reviews
 - File Integrity Checkers
 - Virus Detectors
 - War Dialing
 - Wireless LAN Testing
 - Penetration Testing
 - Post-Testing Actions
 - General Information Security Principles
 - Comparisons of Network testing Techniques
 - Determine the Security Category of the Information System
 - Determine Cost of Performing Each Test Type per System
 - Identify Benefits of Each Test Type per System
 - Prioritising Systems for Testing



NIST SP 800-42 explains about testing:

- No matter how well a given system may have been developed, the nature of today's complex systems with large volumes of code, complex internal interactions, interoperability with uncertain external components, unknown interdependencies coupled with vendor cost and schedule pressures, means that exploitable flaws will always be present or surface over time. Accordingly, security testing must fill the gap between the state of the art in system development and actual operation of these systems.
- Security testing is important for understanding, calibrating, and documenting the operational security posture of an organisation. Aside from development of these systems, the operational and security demands must be met in a fast changing threat and vulnerability environment. Attempting to learn and repair the state of your security during a major attack is very expensive in cost and reputation, and is largely ineffective.
- Security testing is an essential component of improving the security posture of your organisation. Organisations that have an organised, systematic, comprehensive, on-going, and priority driven security testing regimen are in a much better position to make prudent investments to enhance the security posture of their systems.



ISECOM Open-Source Security Testing Methodology Manual

Another framework that is regularly used is the Institute for Security and Open Methodologies (ISECOM), Open-Source Security Testing Methodology Manual (OSTMM).

It states:

“To be most clear, any security test which does not follow a scientific methodology has little to no measurable value; therefore no clear direction can be taken through analysis and no clear result can be formed. The specific guidelines in this manual provide the basis for audits and tools towards a formal scientific method to operational security auditing, the metrics to quantify security within any channel, the rules of engagement for auditors to assure unbiased and logical analysis, and a standard for providing certified security audit reports.”



Enex TestLab is not just limited to the security testing guidelines and frameworks contained in NIST SP 800-42 and the ISECOM OSTMM. We custom tailor security systems testing to our clients requirements.

Security Test Plan and Test Script

Preparation

To ensure test coverage, test reproducibility and to provide a testing audit trail, Enex TestLab develops a specific Security Test Plan and associated Test Scripts. In accordance with your specifications and business requirements we will analyse the complete set of functions, create a test plan, test scripts, test scenarios and, if required, even test data.

Our test documentation enforces very high standards for the Test Plans to ensure that issues are reported in a structured and concise way. It maintains the best possible information for your security administrators to reproduce and fix any issues.

You are able to either use our Test Scripts to test in-house, or our experienced security engineers can continue testing for you.

Performance Testing

Performance testing determines whether the performance of your product actually meets its specifications on the range of platforms you are targeting - taking into account factors such as speed, accuracy, effectiveness.

From our tests, Enex TestLab can recommend minimum target platform specifications for your product.

Enex TestLab has also developed many of its own specialised performance tests for security systems.

Functional Testing

Security systems require thorough functional testing to ensure their services and functions are secure and reliable before they are released.

Functional specification testing ensures that all design functionality is actually in place and that a security system's operation adheres to its specification.

Enex TestLab uses a systematic approach to test coverage, including the standardised checklists and basic requirements verification techniques. Our feedback provides evidence supporting the quality of your product. It will help you make informed business decisions about your security systems.

Regression Testing

Regression testing is the process of verifying that issues reported and fixed by the security team have not compromised the existing functionality or opened further security holes. Regression testing should be undertaken whenever a functional or environmental change has been introduced to any part of your security system. It is important because new issues often are introduced when attempting to fix existing problems.

Enex TestLab checks that any code or security system changes do not introduce errors. We verify that the whole security system continues to function correctly.



Compatibility Testing

With a diverse variety of computers and technology available today you must be certain your security applications perform in every environment. Enex will test your security products on different hardware, software, web browser and operating system combinations used in your market. This includes a range of servers, network types and databases.

We test your security application under different conditions, operating systems and combinations of hardware and software, databases or servers to determine if your product is cross-platform friendly.

Compatibility testing by Enex TestLab eliminates any need for you to buy and maintain your own costly test hardware or software. Enex TestLab has all these physical and virtual resources ready.

Security Maintenance Testing

Security testing ensures that major issues are identified before attackers, and even in some cases, users/customers discovering them. However, Enex TestLab also performs regular security maintenance testing of production security systems.

Security testing on a regular, ongoing basis assists in identifying minor changes and major breakdowns before attackers discover them.

This service is particularly recommended for e-businesses as this alone can represent dramatic savings when any downtime is extremely expensive.

Attackers constantly discover new ways to compromise systems, regular security maintenance testing ensures that these risks are identified early.

Dynamic security systems require regular security maintenance testing. This ensures that any changes or updates do not introduce new issues.

During security maintenance testing Enex will also conduct performance tests to ensure that your system continues to meet its performance criteria.

Test Automation

Test automation saves time and eliminates the possibility of human error. Enex TestLab analyses the security testing requirements and develops custom of automated tests which are fast, accurate, easy to maintain and cost-effective.

Load and Stress Testing

Enex TestLab can ensure your application server or database server is able to meet its expected demand whether from day to day client transactional load or under the extreme conditions posed by distributed denial of service attacks. We perform server load and stress testing to show you exactly how your applications would perform under real-world conditions. It is better to be aware of your systems capabilities before they are tested by an attacker.

Load testing determines an application and/or application server's capacity to service an expected number of customers. Stress testing determines the server's behaviour as it operates under sustained peak load conditions.

Load and stress tests require the simulation of significant numbers of customers connecting to your site simultaneously.

Load testing will typically be performed using scripts that generate numerous requests for information. The scripts collectively measure the performance of various functional areas in your applications. Requests for static content are separated from search requests and requests that require database retrieval.

Load testing progressively increases the number of simultaneous connections while monitoring server and systems response times and CPU loads. This data is analysed and presented against your objectives. For example:

- Can the server support anticipated loads without performance degradation?
- What is the maximum number of simultaneous clients that the server can realistically support?
- How does the security system respond to these simulated attacks?

Stress testing can be performed to evaluate how your server will be able to respond to load conditions. The number of simulated customers is increased beyond the point where degradation occurs, and the server's recovery behaviour is observed. The number of simulated customers is then reduced to normal levels and its behaviour observed again. This test verifies that the systems can gracefully withstand and recover from, high load conditions such as those that may occur in an attack.



enex testing projects

Examples of common Enex security testing projects

Firewall (Hardware/Software)

Performance testing – Firewall throughput is benchmarked against the standard network connection with the firewall configured using typical enterprise security settings.

Vulnerability testing – Firewall is tested against our database of known network attacks.

Ease of use – Evaluation of ease of setup, configuration, administration, management and updates.

Anti-Spam (Software, Hardware, Appliances and Managed Services)

Performance Testing – The performance of anti-spam software/hardware tested in both a controlled lab environment and live online using Enex TestLab's custom tools.

Accuracy Testing – Accuracy of anti-spam software/hardware tested in both a controlled lab environment and live online using Enex TestLab's custom tools.

Ease of use – Enex TestLab evaluates the ease of setup, configuration, administration, definition management and signature updates.

Anti-Spyware

Performance Testing – Scan speed of anti-spyware application tested in a controlled lab environment against disk images containing spyware threats from our collection of definitions/signatures.

Accuracy/Effectiveness Testing – Accuracy in detection and effectiveness of removal of spyware tested in a controlled lab environment against disk images containing spyware threats from the Lab's collection of definitions/signatures.

Ease of use – Evaluation of ease of setup, configuration, administration, definition management and signature updates.

Anti-Virus

Performance Testing – Scan speed of anti-virus applications tested in a controlled lab environment against disk images containing virus and worm threats from the Lab's collection of viruses and signatures.

Accuracy/Effectiveness Testing – Accuracy in detection and effectiveness of removal of virus/worm tested in controlled lab environment against disk images containing virus and worm threats from the Lab's collection of viruses and signatures.

Ease of use – Evaluation of ease of setup, configuration, administration, definition management and signature updates.

Proof of Concept for Security

Technologies

Enex has been contracted to assist vendors with proof of concept and development of their security technologies using custom TestLab methodologies.

Content Filtering

Performance Testing – Server based testing of the performance of content filter with a direct comparison to the performance of the network without the filter in place.

Effectiveness in Site Blocking – Enex TestLab compares the content filters blocking ability against a database of banned sites maintained by the Lab in conjunction with the Australian Communications and Media Authority (ACMA).
Ease of use – Enex TestLab evaluates the ease of setup, configuration, administration, definition management and updates.

Wireless Security

Enex TestLab has procedures to test the security for gateways, access points, network management and monitoring software, in particular the performance impact on the network and vulnerability, along with authenticated roaming.

Penetration Testing

Enex TestLab has the ability perform penetration testing including full disclosure, stealth, social engineering and vulnerability (such as injection attacks, denial of service attacks, foot-printing, key-logging and so on).

Patch Management and Vulnerability Tool Testing

Enex Testlab can perform both Performance and functionality testing on patch management and vulnerability tools and their associated systems.

Authentication

Enex TestLab has experience in a variety of authentication testing, from biometric tools through to smart card technologies or single sign on and federated authentication technologies. Enex TestLab has developed numerous custom procedures and scripts for benchmarking and evaluating these products.

Wireless Testing

Range/Performance Testing – Enex has a range of procedures and utilities to test the throughput performance and range dependencies of wireless devices.

Mobility Testing – The TestLab is able to test the true mobility of wireless devices and infrastructures including slow and high speed roaming tests - with and without features such as authentication.

Compatibility & Connectivity – Enex TestLab has experience in wireless device compatibility testing with complex wireless infrastructure architectures designed mimic those of the client.

Network Performance

Performance Testing – Enex TestLab has tested a variety of network devices including switches, routers, thin clients, servers, workstations, NAS and SANs.

Load Testing – Enex TestLab can measure the capability of an application to function correctly under increasing loads and also determine if a business process can be carried out within the expectations documented in the SLA.

Stress Testing – Enex TestLab uses a variety of tools to determine at load/stress at which a system fails and the severity and ramifications of failure.

Summary

Your organisation's ICT systems and associated information are critical components for doing business in today's competitive arena. Whilst there are a range of security products and techniques available from many ICT vendors picking which ones are most suitable for you is not a simple task.

Involving Enex TestLab will lower your security risk through our independent testing of your systems, together with checking for known threats and vulnerabilities.

Our many years of hard won experience in working with key corporate and government organisations delivering security testing, will provide truly independent results from which you will be able to apply both preventative and remediation measures.

Our expertise is based on very relevant and current knowledge of practical systems through regular comparative and performance reviews of key security products including firewalls, anti-spam, anti-spyware, anti-virus and internet content filters.

So to ensure confidence in the security of your information and the currency of your defensive measures make use of our practical and cost effective measures.

If we prevent just one incursion by a criminally minded hacker the service would pay for itself.

Website:
www.testlab.com.au

Australia Wide
1300 662 592
enquiries@testlab.com.au

VIC
+61 3 9436 7454

ACT
+61 2 6100 8332

NSW
+61 2 8920 3882

HK/CN
+852 8125 2550

US
+1 408 512 2038

UK
+44 20 8123 2329
u

