



Next Generation Security Software Limited

“NGSSoftware”

(Research, Software & Consultancy)



Introduction

- About NGSSoftware
- Research
- Software
- Consultancy



About NGSSoftware



About NGSSoftware - History

- Formerly Cerberus in 1999 before acquisition by @stake
- Present company established in September 2001
- Three main offices UK (London), US (Dallas) & Australia (Brisbane) together with several regional offices.
- Principles: develop cutting edge security assessment software, deliver the best security advice to our clients, provide deep technical understanding of security issues
- Company focus and statement:
“Intelligent Solutions for an Evolving World”



About NGSSoftware - Now

- Currently 51 UK staff
- Largest penetration testing team in Europe
- Three inter-connected areas to the business:
 - Research
 - Software
 - Consulting
- Wholly owned by the six founding directors
- Debt free – organic growth
- Trade Value 2004/05 = £2.5m
- Trade Value 2005/06 = £4.5m



Research



Research

- Acknowledged world leaders in vulnerability research
- David & Mark Litchfield voted “Best bug-hunters in the world” last year
- Discovered and responsibly disclosed more vulnerabilities than any other commercial security research group
- Trusted advisors to UK/US governments (GCHQ and NSA)
- Official Advisors to NISCC, UNIRAS, CESG and a growing number of other global agencies responsible for critical infrastructure security



Research - Highlights

- Discoverers of the Slammer vulnerability
- Breakers of “Unbreakable” Oracle
- First to fully defeat MS stack protection mechanism
- Undisputed leaders in vulnerability discovery and responsible disclosure
- Authoritative research on SQL injection attack vectors
- Cutting edge security research papers
- Globally published security articles
- Published authors of numerous authoritative security books
- Permanent speaking slots at premier conferences



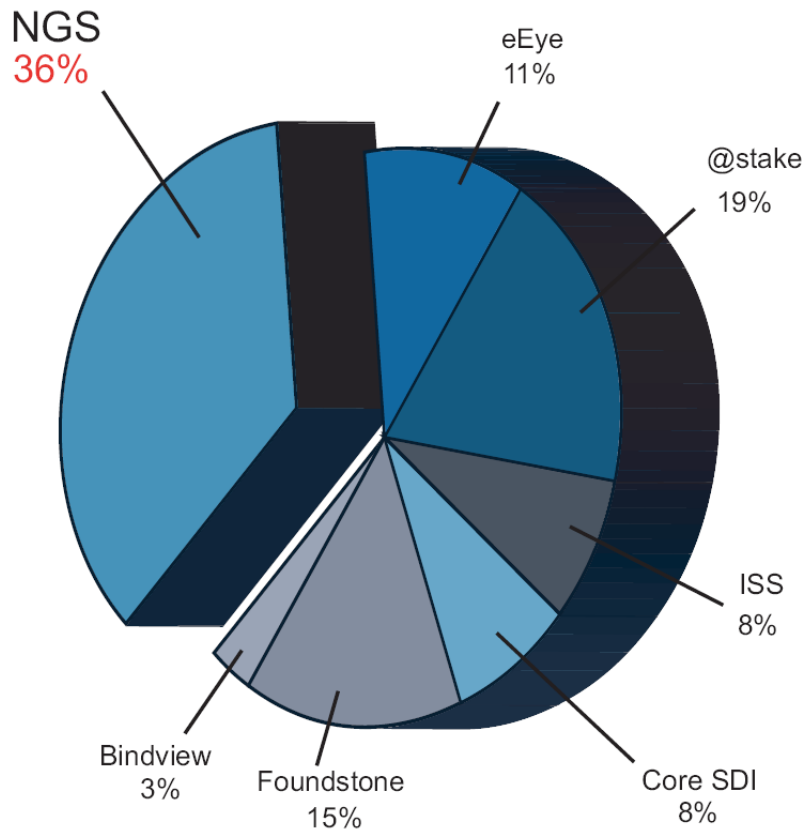
Research – Global Presentation Expertise

- CNE - Directorate of Information Assurance (NSA)
- CHECKCON (G.C.H.Q – CESG)
- Stanford University CyberSecurity Conference
- Every Blackhat Security Briefing Around The World
- Joint presentation with Microsoft at Infosec Europe
- Microsoft's Tech Ed Conference Amsterdam
- Microsoft's BlueHat Security Briefings (On SQL Server 2005)
- Various roundtables in UK

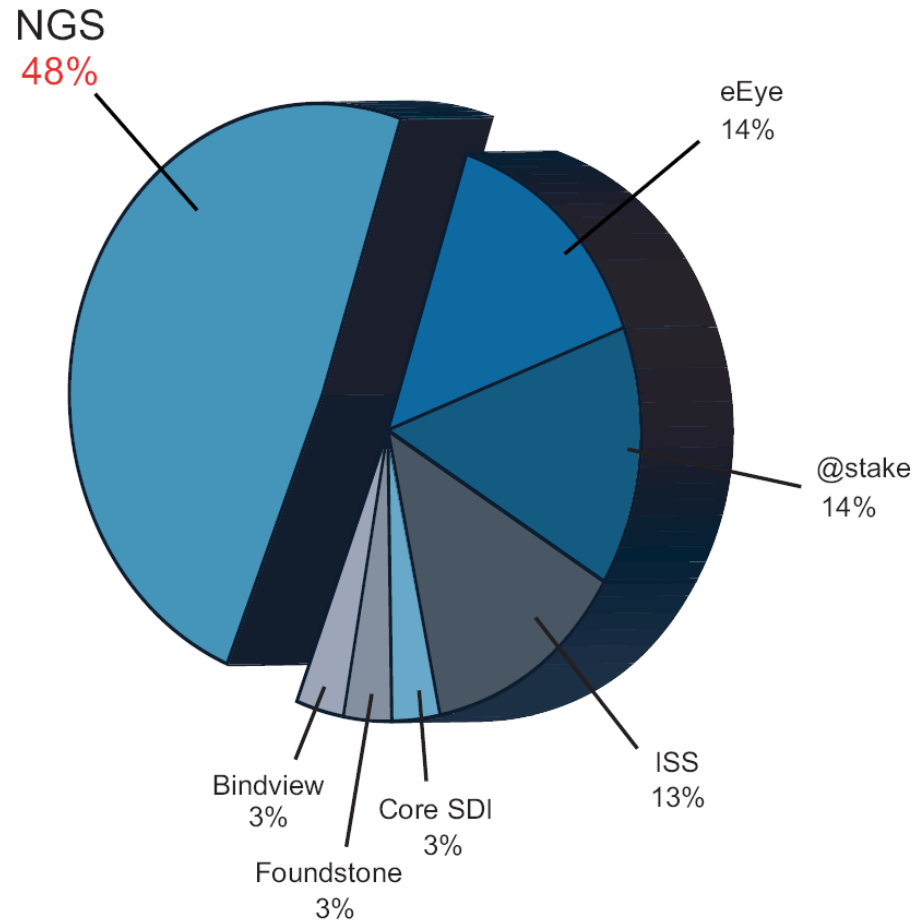


Research – Comparisons

Total advisories, 2002 - 2003



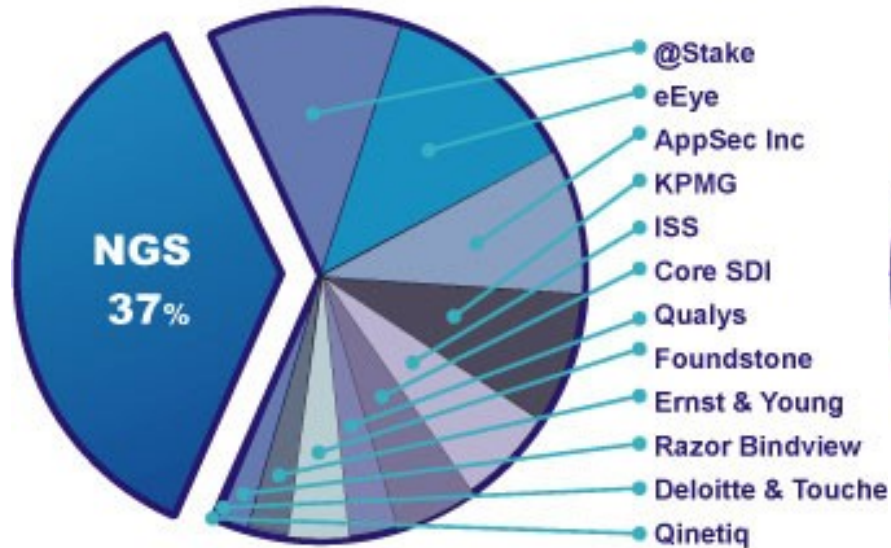
Vulnerability Research into Enterprise software, 2002 - 2003



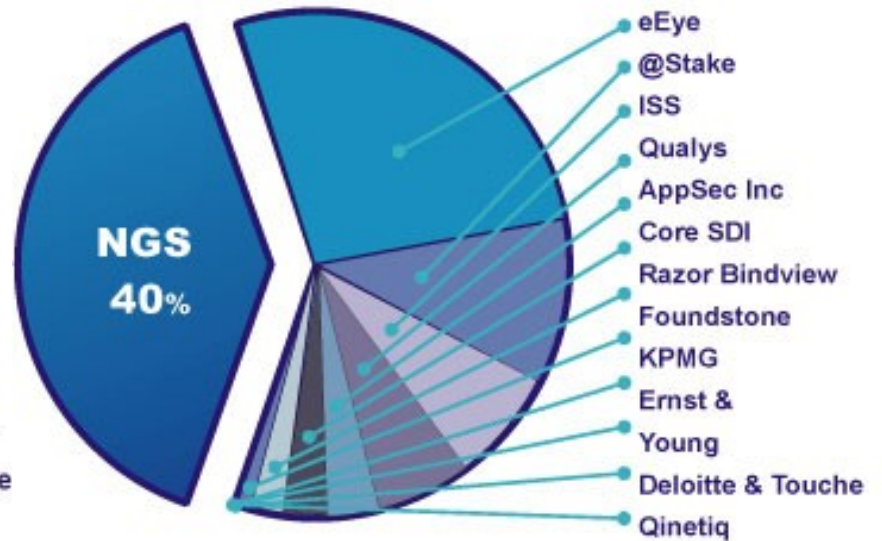


Research Comparisons 2004

Total advisories 2002-2004



Vulnerability Research Advisories 2004





Research – Recent Advisories since September 2004

- May 2006 – Multiple critical and high risk vulnerabilities in Oracle's Database Server versions 8i, 9i and 10g
- Jan 2006 – Critical Exchange/Outlook issues
 - Sun/RedHat/Novell directory server
 - Many Oracle Issues
- Dec 2005 - IBM AIX issues
 - RealPlayer overflow
- 34 critical vulnerabilities in Oracle
- 22 critical vulnerabilities in IBM DB2
- 6 vulnerabilities in Sybase ASE
- Microsoft Word Perfect Buffer Overflow
- Remote 'SYSTEM' overflow in Windows
- Kernel overflow in Windows
- 4 Critical Flaws in RealPlayer
- Other flaws in HP OpenView, L-Soft Listserv, Apple i-Tunes, Veritas Focalpoint, PHP...



Research – Current

- Numerous issues awaiting fixes in Oracle
- A dozen issues awaiting fixes in Informix
- Multiple issues in other core Databases, Operating Systems and Applications are also awaiting patching



Research – Future

“What would the criminals do?”

- Continue to examine database servers
 - Database Security is of paramount importance
- Begin active research into middleware / Message Queuing
- Go back to web servers
- Popular client apps



Software



NGSSoftware Products

- NGSSquirrel DB Assessment Suite
 - NGSSquirrel for SQL Server
 - NGSSquirrel for Oracle
 - NGSSquirrel for DB2
 - NGSSquirrel for Sybase ASE
 - NGSSquirrel for Informix

- Typhon III
 - Intelligent vulnerability assessment scanner

- Domino Scan II
 - Lotus Domino Web Application security scanner

- OraScan
 - Oracle Web Application Server security scanner



Introducing NGSSquirrelL for SQL Server

NGSSquirrelL for SQL Server allows system administrators and security professionals to quickly and easily assess SQL Servers (7 & 2000) for a variety of security vulnerabilities. This security scanner comprehensively scans SQL Servers for hundreds of possible security threats. Unlike many other scanners that only find "holes" in security infrastructures, **NGSSquirrelL for SQL Server** allows quick and accurate assessment of the level of risk that servers are exposed to.

Extended Stored Procedures

This is an **informational** issue.

These are the names and dll names of all extended stored procedures p database

This check was run at Thu Aug 21 10:51:57 2003

name	dll or comment
xp_instance_regdeletekey	xpstar.dll
xp_getprotocolldllinfo	xpstar.dll
xp_readerrorlog	xpstar.dll
xp_enumerrorlogs	xpstar.dll
xp_getfiledetails	xpstar.dll
xp_servicecontrol	xpstar.dll
xp_availablemedia	xpstar.dll
xp_dirtree	xpstar.dll
xp_eventlog	xpstar.dll
xp_fixedrives	xpstar.dll
xp_cadshell	xplog70.dll
xp_subdirs	xpstar.dll
xp_logevent	xplog70.dll
xp_getnetname	xpstar.dll
xp_sprintf	xplog70.dll
xp_IsMRCSTeadRate	xpstar.dll

Authentication Details

I have a User ID and Password

Use my current Windows Credentials

Use the following User ID and Password

User ID: _____

Password: _____

I don't have a User ID and Password

Attempt to login as these users: _____

Use the following password dictionary: _____

OK Cancel



'This is definitely a must product for large enterprises'
July 2004



Introducing NGSSquirrelL for Oracle

NGSSquirrelL for Oracle has been specifically developed to scan Oracle Database Servers allowing DBA's, system administrators and security staff to quickly and easily discover the vulnerabilities that servers are exposed to. **NGSSquirrelL for Oracle** carries out a complete scan of Oracle TNS Listener vulnerabilities including denial of service and remote server compromises. **NGSSquirrelL for Oracle's** new Security Manager has the capability to fix problems immediately and also allows management of users, roles, system privileges and object privileges.

The screenshot displays three overlapping windows from the NGSSquirrel For Oracle application:

- Server Libraries:** Shows a tree view on the left with 'Server Libraries' selected. The main pane displays a table of libraries:

OWNER	LIBRARY_NAME	FILE_SPEC
SYS	COLLECTION_LIB	
SYS	CRYPTO_TOOLKIT_LIBRARY	
SYS	DBMS_ANYDATASET_LIB	
SYS	DBMS_ANYDATA_LIB	
SYS	DBMS_ANYTYPE_LIB	
SYS	DBMS_APPCTX_LIB	
SYS	DBMS_AQADM_LIB	
SYS	DBMS_AQELM_LIB	
SYS	DBMS_AQ_LDAP_LIB	
SYS	DBMS_AQ_LIB	
SYS	DBMS_AW_LIB	
SYS	DBMS_CDCAPT_LIB	
SYS	DBMS_CDCPUB_LIB	

- Security Manager:** A dialog box with a 'Security Manager' title and a squirrel logo. It contains four buttons: 'Manage Users and Roles', 'Manage Profiles', 'Manage System Privileges', and 'Manage Object Privileges', along with an 'Exit' button.
- Password Audit:** A window showing a table of user credentials:

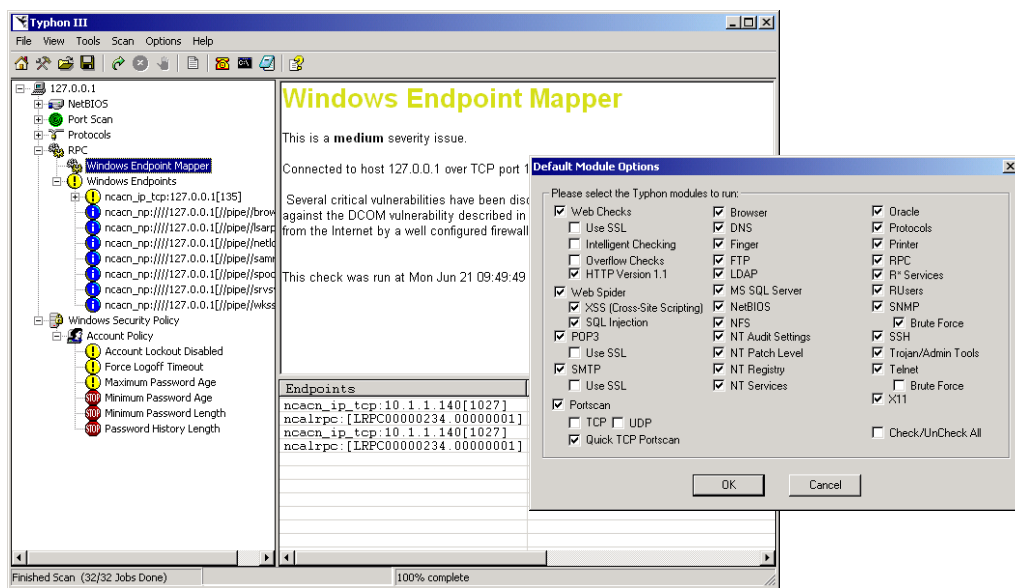
username	Hash	Password
YS	9C30855E7E0CB02D	FOO
YSTEM	ED58B07310B19002	OUTLN
UTLN	4A38A5E00595C01	DBSNMP
BSNMP	E066D214D5421CCC	DBSNMP
MSYS	7C9BA362F9314299	MSYS
ORDSYS	7EFA12C72A688F	ORDSYS
ORDEPLUGINS	88A2B2C183431F00	ORDEPLUGINS
MDSYS	72979A94BAD2AF80	MDSYS
TSYS	71E687F036AD56E5	
DB	880B44765FC66AF	
KSYS	69ED49EE1851900D	
KPROXY	B97545C4DD2ABE54	ODN
JM	C252E8FA117AF049	
ODM_MTR	A7A32CD03D3CE8D5	
OLAPSYS	3FB8EF9DB538647C	
RMAN	E7B5D92311C631E1	RHAN
HR	6399F3B38EDF3288	
OE	9C30855E7E0CB02D	
FM	72E382A52E89575A	
SH	9793B3776C3BD1A	
OS_ADM	991CDDAD5C532CA	
OS	8B09C6075BDF2DC4	
OS_US	244CF611D07D82F	
OS_ES	E5A6FA4BB042E3C2	

At the bottom of the Password Audit window, it shows '(Brute Force) 4470000 tries: Current: CVX' and '80000 passwords/sec'. There are checkboxes for 'Hide Null Passwords' and 'Beep on Hit', and a 'Quit' button.



Introducing Typhon III

In order to mitigate the digital risks facing many organisations, **Typhon III** provides a fully configurable, intuitive environment across twenty-nine application modules. **Typhon III** can be employed to quickly and accurately assess enterprise environments for security vulnerabilities. With its uniquely holistic approach to auditing, **Typhon III** is the complete security solution for the assessment and protection of your network and business critical data.



'the quality of the scans available [is] extremely high'
August 2005



'if you need a security scanner, this is a great product'
October 2004



"Our Best Buy is Typhon 3 for its no-nonsense approach and comprehensive functionality combined in a package that will be easily understood and effectively deployed within most organizations."
June 2004



Introducing Domino Scan II

Domino Scan II presents an "attacker's eye" view of the security of Lotus Domino web servers and bespoke Notes applications. Although **Domino Scan II** is stand alone software running on Microsoft Windows (NT / 2000 / XP) it can audit Lotus Domino web servers that are running on any operating system. **Domino Scan II** can enumerate and audit over one hundred sensitive and default databases, and put each of these (and the documents within) through a vigorous set of vulnerability assessment checks.

The screenshot displays the DominoScan II application window. The main pane shows a scan report for 'CGI-BIN Present' with the following text:

CGI-BIN Present

This is a **low** severity issue.

Report for host

The remote server has an executable /cgi-bin directory present.

This check was performed without using credentials.

Below the report is a table with the following content:

CGI-BIN
CGI-BIN Present

Three dialog boxes are overlaid on the application:

- Default Module Options**: A dialog box with a 'Select Modules to Run' section containing checkboxes for Web Checks, Use SSL, Spider Checks, Do DB Enumeration, Do DB Checks, POP3 Checks, Use SSL, SMTP Checks, Use SSL, and LDAP Checks. There is also a 'Check/UnCheck' checkbox.
- Web Audit Settings for Host: 127.0.0.1**: A dialog box with sections for HTTP Settings (Use HTTP Version, Base URL, Use Proxy Server, Proxy, Proxy Port, 404, Keyword), Authentication (Use Credentials, UserID, Password), Audit Single Database (Audit only this database), Default Databases (Audit Default Databases), Quick Hit (Check only to see if access can be gained to default databases), and Server-Wide Security Checks (Perform checks).



Introducing OraScan

OraScan is a detailed auditing application developed to assess the security of Oracle web applications regardless of environment. **OraScan** performs a vigorous and detailed security vulnerability audit of Oracle web applications focusing on the discovery of flaws (e.g. SQL Injection, Cross Site Scripting, Remote Command Shell execution, etc.). **OraScan** can additionally be deployed to audit the configuration of IAS web servers, ensuring that no security vulnerabilities are present within the base software architecture.

The screenshot displays the OraScan application window with the following components:

- Main Window:** Shows a tree view on the left with 'JDBCQuery.jsp' selected. The main pane displays the scan results for this file, including the HTTP response code (200 OK) and a warning: "A dangerous demo page was found. It should be removed from the server. This is a high severity issue. The requested URL was: https://.../443/demo/sql/jdbc/JDBCQuery.jsp. This check was run at Thu Jun 03 11:33:41 2004".
- Default-Settings Dialog:** A dialog box with sections for "Checks To Run" (Run Spider, Run PL-SQL Checks, Run JSP Checks, Run Oracle Default Checks, Run SQL Injection Checks, Run Cross Site Scripting Checks), "Spider Settings" (Use HTTP 1.1, Test Default Directories, Test Default Files, Test Default URIs), "Base URL", "Username", "Password", "User Agent" (Mozilla/4.0), "Default Directories" (listing _pages, bin, cgi-bin, etc.), "Default URIs" (listing /robots.txt, /%0a.pl, etc.), "Default Files" (listing test.* files), and "Extensions To Ignore".
- Add URLs to scan Dialog:** A dialog box with a text area containing "http://www.example.com:7777/index.htm" and buttons for "Add", "Remove", "OK", and "Cancel".

OraScan results can be viewed by clicking in the left-hand pane



Latest Reviews (January 2007)

Typhon III

- *"This is the best general vulnerability scanner I've found with respect to dealing with security issues for database servers..., I was impressed with how rapid it was able to perform the scans and how accurate the reports were..., The documentation is awesome, especially when it discovers a vulnerability"* – Brian Kelley, SQLServerCentral.com

- NGSSQuirreL for SQL Server

- *"Overall I found NGSSQuirreL's power, flexibility, and speed impressive,... I highly recommend these products for auditing production and development SQL Server instances on a regular basis"* – Michael Coles, SQLServerCentral.com



Software Partnerships - Preventsys



Preventsys has pioneered an award-winning enterprise vulnerability management system for large enterprises that are frustrated with the difficulty of managing multiple vulnerability assessment and configuration management tools to create risk and compliance reports. Unlike security event management (SEM) products that centralize data from security sensors for event monitoring and managed incident response, the Preventsys Enterprise Security Management system integrates best-of-breed security assessment tools into a central security dashboard, dramatically cutting costs and reducing the time it takes to create comprehensive, custom reports from weeks to seconds.



Software Partnerships - CSCI



Computer Security Consulting, Inc

CSCI was founded in 1998 in Tucson, Arizona providing the commercial and local government with security services, hardware, and software. CSCI have worked with numerous US Government agencies (including many law enforcement agencies) to provide a wide range of a security services ranging from the development of infrastructure/departmental policies and procedures through to access control and disaster recovery.



Consulting



Consulting

- Largest dedicated pentesting team in Europe
- Enterprise consultants with proven track records
- Largest number of security cleared CHECK team leaders
- List X Company, allowing NGSSoftware to work on and store Top Secret materials
- Authors of best-of-breed security analysis tools (Odysseus, Burp Proxy, web spiders, fuzzers, disassemblers)
- Frequent presenters at global conferences
- Undertake bespoke research projects (product review, network appliance testing, code review)



Consulting – Services

- Penetration testing
- Specialist database security analysis and advice
- Black-box review (custom & commercial apps.)
- Network & Web App Security assessment
- Sophisticated security code reviews
- Infrastructure & application security design and deployment
- Reactive attack response & investigation
- Bespoke “thinking outside the box” security services



Consulting – Clientele

Providing services to:

- 6 of the top 10 largest software manufacturers
 - Helping to secure Microsoft's commercial products
- 20 Leading Financial Institutions (Banks, Building Societies, Insurance Companies etc)
- Many of the UK's largest retailers
- One of the US's largest Health service providers
- The worlds largest News-feed organisations
- One of the worlds largest industrial manufacturers



Client Recommendations

Microsoft

“As part of Microsoft's Trustworthy Computing commitment, the Secure Windows Initiative Team has the responsibility for ensuring all Microsoft products are as secure for our customers as possible. As part of this effort, we seek out the world's leading vulnerability researchers to help us with our largest, most complex engagements. The NGS team is a great fit, already being trusted advisors to governments and other global corporations.

Over the last 3 years, our teams have collaborated on various product engagements requiring 3rd party involvement or leveraging NGS's unique research strengths. Our teamwork has resulted in more secure products reaching our customers. NGS have proved to be an outstanding partner and their efforts have greatly enhanced the security of Microsoft products.”



Client Recommendations (2)

ORACLE

“In the ever changing field of e-business security, NGS continues to be a leader in both quality and quantity of their research. Oracle recognizes this unique skill set and has worked with the NGS Consulting Team on high profile projects requiring third-party involvement and verification. As the world's recognized leader in information security, Oracle partners with leading security vendors to enable tight, end-to-end security for our customers. NGS fits this role perfectly and our collaboration has consistently produced outstanding and professional results.” – ***John Abel, Principal Consultant, Oracle Consulting***



Client Recommendations (3)



"The institution of security controls around our web applications is an integral part of McAfee's defence-in-depth and compliance strategies. When McAfee has a need for application security consulting, we turn to the experts at Next Generation Security Software (NGSSoftware). NGSSoftware brings a diverse background in security assessment and research that is unparalleled in the industry today. NGSSoftware offers professional, result-oriented security consulting services that makes them a vendor of choice for our business." **Charles Ross, Sr. Manager Security Assurance, McAfee, Inc.**



Client Recommendations (4)



"Huge thanks from all of us at Comic Relief for all your work and support. We received 1.1 million unique visitors during the campaign and on the night, processing over 225,000 transactions. I hope we can continue to grow the relationship with NGSSoftware and work with your extremely bright and cunning team. Thanks for keeping the door shut to inquisitive kids the world over." **Martin Gill, News Media Manager**



Thank You

<http://www.ngsssoftware.com/>