



Net'Q Capability Statement

Net'Q, founded in 1995, is an international security company that provides mainframe security solutions, software, and services. The CEO and founder, Peter Hager, specializes in security, strengthening both SNA and TCP/IP networks. He speaks on network security at conferences such as SHARE and the Vanguard Security Conference. Before founding Net'Q, Mr. Hager was a network engineer and technical specialist for IBM for 15 years, where he initiated and developed the first courses in Network Security for IBM, and served as a lead instructor providing training to IBM specialists and customers. Following his work at IBM, Hager started Net-Q in 1995. Net-Q provides consulting and software to improve large-scale, complex networks. Its clients include major manufacturers, financial institutions, and government agencies in Europe and the U.S.

Net'Q partners with SDS to provide complete solutions for the network and the network security challenges our customers face today. Net'Q solutions provide the ability to analyze, assess, optimize, monitor, and secure complex mainframe network systems, with a focus on proprietary protocols used by mainframe application servers. Traditional IT security solutions leave those proprietary protocols unsecured, even though mainframe servers today store over 80% of critical information and over 90% of financial information, and are a primary server technology to support cloud computing environments.

Contents:

1. Background
2. Clients
3. Competencies
4. Products and Services
5. Past Performance and Real World Experience:

The stories of 5 large financial institutions solving severe security issues..

Background:

Security concerns are ever present in our changing world. We make huge efforts to protect ourselves from obvious physical threats. However, many cyber space challenges remain unanswered. Infiltration of critical infrastructure information systems has the power to paralyze entire cities and bring serious threats to our intelligence, financial, and economic security. Additionally, in today's environment the compromise of select systems could result in bodily and physical harm, because energy, telecommunications, and transportation systems rely heavily on large server computer systems. Cyber security is critical to ensuring economic stability and national security.

Critical information resources have seen more and more cyber threats in the past few years. Cyber fraud has nearly quadrupled over the past two years, with over 90% of data compromises occurring in the financial sector. Many of the originators have strong ties to organized crime. These threats have included malicious code, theft of personal information, financial manipulation, and loss of corporate technical trade secrets.

Several initiatives have taken place to improve the security of information. These include licensing requirements and regulatory initiatives such as those incorporated by PCI, NIST, and ISO. Additionally, recent legislative initiatives have provided added focus on the importance of cyber security. Requirements include penetration testing, and continuous monitoring and reporting.

Despite these initiatives, there has been an increase in data compromises.

Clients:

The Net'Q security suite of solutions now serves a diverse set of world-class international clients. Over 60% are large international financial institutions, including some of the world's largest banks. Other major clients are in healthcare, manufacturing, energy, telecommunications, and government.

Financial – 60%

Energy – 5%

Government – 15%

Manufacturing – 5%

Health/Medical – 10%

Telecommunications – 5%

Competencies:

Of particular importance, Net'Q secures large complex systems, bringing focused expertise in the mainframe network environment.

Analysis	Audit Support
Penetration Testing	Continuous Monitoring
Reporting	Real-time Protection
Forensic Analysis	Compliance

Products and Services:

Net'Q provides a suite of security products and services to protect critical information:

1. Net-Examine – Examines and audits networks including SNA/APPN/APPC, host definitions, and data flows on laptops or dedicated security servers. Additionally, Net-Examine can provide continual reporting of security status.
2. SNA/APPN-EE Firewall – Protects the mainframe SNA and APPN environment. Protection is performed at the lowest negotiated session level, providing real-time protection against intrusion attempts and ensuring compliance with security rules and regulatory requirements. Additional features provide automatic generation of security parameters and performance optimization of networks.
3. Sarbanes-Oxley / NIST / Corporate Compliance – Net'Q Security suites include compliance modules that provide validation checking of SNA definitions. These validations can be customized based on the customer's needs. They also identify potential security gaps and provide system-generated validation reports.
4. Penetration Test Services – Provides detailed penetration analysis and prevention strategies using our proprietary SNA/APPN penetration test software. Provides vulnerability health reports.
5. Security Audit Analysis – Net'Q, with its proprietary Net-Examine technology, can conduct or assist in security audit analysis. We can provide independent support and consulting or train organizations to use our suite of tools.
6. Forensic Analysis – Net'Q provides analysis of mainframe system / network compromises. In addition to separate analysis, the “visitor report” log generated by the Net'Q security suite provides unique insight into both successful and unsuccessful connection attempts as well as pass-through-traffic information to further support forensic analysis and potential security compromises.

Past Performance and Real World Experience:

Financial Institution 1 – Analysis and Audit Support

Net'Q conducted an analysis at one of the world's top banks. The bank had just recently undergone a security audit using one of the major firms with no serious findings. The security in place, as at most of financial organizations, included IP firewalls, RACF implementation, and encryption. Our analysis included the use of Net'Q's proprietary analysis tool, Net-Examine. That analysis essentially took a snapshot of the system parameters and network sessions. Over 210,000 sessions were analyzed across networks and all connection types. The findings categorized all sessions in the four least secure and dangerous security categories, with major security flaws and gaps. Additional analysis revealed that the branch offices had non-authenticated open access to the core systems.

Financial Institution 2 – Forensic Analysis – Session Hijacking / Man in the Middle:

A large international financial institution discovered unusual transactions occurring during a maintenance shutdown. The organization had in place state-of-the-art and up-to-date IP firewalls, had implemented network encryption protocols, and had implemented secure ID cards. The transactions were traced to an authorized user/administrator. The user was contacted. He was neither in the data center nor working remotely. Net'Q was contacted to investigate the situation. We examined the system and identified rogue intermediate software (man-in-the-middle) that was tracking users and performing switching functions to enable an outside party to execute transactions that appeared completely authorized. Further analysis discovered that the infiltration had been going on for over eight months completely undetected. The system was accessed using SNA/APPN/APPC based protocols from outside the financial organization's network.

Financial Institution 3 – Penetration Testing – Forensic Analysis – Malicious Software:

A large financial institution found suspicious files stored on its system. Those files independently started sessions to other applications, similar to what was recently discovered on the Cleveland Federal Reserve system.

The organization was protected with an IP Firewall, encryption, and secure ID cards, plus single sign-on. After the suspicious files were discovered, Net'Q was contacted to analyze the system and determine the cause. Detailed analysis discovered that the suspicious files were all replications of the same type of file. The initial file was created during a hijacked session by what was believed to have been an authorized user. Hence the organization was concerned that the files had replicated and inquired if replication was possible.

“Is this possible?” Our answer: “Yes!” At the request of the financial organization we developed a software module that could be stored on the organization's system. With the organization's approval we infiltrated the bank's network from outside the network and stored a file that would

replicate itself automatically. Over a single weekend the file replicated itself 500 times across 20 different networks. The infiltration of the network and the replication of the malicious software all appeared as if the operations were performed by an authorized user.

It should be noted that while we programmed the module to be harmless and only replicate itself, it could be developed to initiate any type of transaction in the name of an authorized user or application. Moreover, it could have been developed to mutate during replication, taking on different functionalities or varying its execution based on the target systems or applications.

Financial Institution 4 – Rogue Intermediate Network – Forensic Analysis – Network Spoofing

In this instance, Net'Q found that a large financial organization was infiltrated using an intermediate network. The intermediate network provided the means to spoof the target system. The target believed that it was interfacing with an authorized user/application and with a trusted partner network, when in fact the session was routed through a rogue third-party network, which could then route the session to a rogue third-party user or application. In this case, all sessions sending searches/locates through the intermediate network, regardless of entry network and LU type, were subject to compromise.

The financial organization was checking session history in the attacked destination network when it discovered a session between an internal user and a LUCICS application in the intermediate network (LUCICS in NETI).

After contacting the administrators for the intermediate network, the organization realized there was indeed a LUCICS application started periodically at one of their Cisco SNA switched-entry nodes (EN).

In addition, they found sessions coming in from a remote, nonadjacent entry network (NETE), rather than their adjacent NETE.

After checking the LUCICS, the organization realized that the logic was initiating sessions to rogue networks NETR and NETE, and actually residing again at a different location.

Such an infiltration from an intermediate network can result in vulnerabilities and potential fraudulent activities across thousands of sessions using any application and with all network session types, in what appears as an authorized session.

Financial Institution 5 – Forensic Analysis – User Data

A financial organization discovered log-ins from outside their network. No security alert was generated. The connections were initiated using security administrator credentials. A detailed analysis by Net'Q revealed that user data was being transmitted during “search and locate requests” and “session initiation requests.” Confidential information was being transmitted insecurely, by means of broadcast “search and locate” requests. This essentially enabled external third-parties to obtain confidential information and initiate fraudulent log-ins and transactions using authorized user credentials. In this scenario, user data was transmitted without an actual session/connection being established. The data could have been log-in credentials or such data as social security numbers or financial account and credit card information.

Here is how it was done:

1. An SLU application issued a SIMLOGON request that included user data.
2. The target PLU did not reside in the SLU's local network, so the log-on request was broadcast to other networks, as a "search and locate request."
3. The cross-network, broadcast search for the PLU carried unsecured user data along CP-CP connections to all the available VTAMs.
4. Somewhere in the process, unauthorized listeners acquired private user data.

And because the log-on request was ultimately denied at the target PLU, that private data was released without any session/connection having been established.

Thus, without even starting an actual session/connection:

1. The content of files can be provided.
2. User IDs and passwords can be provided.
3. Social Security and ID card data can be provided.
4. Personal credit card and financial account data can be provided.

More information about Net'Q Products and Services:

To learn more about Net'Q and free product trials in North America, please contact Software Diversified Services:

763-571-9000

sales@sdsusa.com

www.sdsusa.com/netq

