



## CUSTOMER STORY

### VULNERABILITY ASSESSMENT LIMITS RISK FOR RESIDENTIAL MORTGAGE LENDER

With daily reports of companies being hacked, financial institutions are under constant pressure to identify and eliminate vulnerabilities in their IT environment. Exposures in the operating systems, routers, firewalls, web sites and applications can leave computer systems open to illegal access by unauthorized parties. The process of finding and fixing security weaknesses can be quite daunting for those companies with large, international networks.

Pressure of Federal regulatory compliance has made financial institutions even more concerned about the risk incurred by their company from a non-protected system. The importance of ensuring its customers' personal information and its financial data remained private and secure encouraged a major residential mortgage lender to look for a cost-effective and efficient way to proactively defend its network against security threats. When their search was complete, they chose NeXpose – an advanced, enterprise vulnerability assessment and risk management platform.

#### SITUATION

Prior to acquiring NeXpose, this mortgage lender had no formal process or product to find and fix vulnerabilities within their environment. With a network of over 60 thousand nodes, they experienced the usual security challenges that can result in theft, fraud, and other forms of exploitation by offenders both outside and inside an organization. Finding the right solution to mitigate security weaknesses was certainly a critical requirement.

To address this need, a team of security specialists were brought together to develop a security plan to protect their network from a malicious attack that could compromise the customer information maintained in their databases. The challenge was to find a solution that could scan a broad range of platforms including Microsoft operating systems, AS/400s, Lotus Domino, IBM DB2, and Oracle databases. Initially, they felt they needed several products because most vulnerability scanners would only handle a piece of the environment.

#### SOLUTION

The security team tested many vulnerability assessment scanners and evaluated each against a weighted matrix that included criteria such as scanning accuracy, update frequency, operating system fingerprinting, non-intrusiveness to the network, reporting, device management, customer service, ease of implementation and management, and overall cost. After this extensive evaluation, NeXpose was the leader because it had a lower overall cost of ownership, extensive customized reporting and broad platform coverage.

“NeXpose became the front runner very quickly because of its ability to scan key parts of our infrastructure such as Lotus Domino and the IBM AS400, which other scanners did not support,” said the exploit management team manager. “Finding one product that can handle our wide range of systems makes analyzing our security situation easier. NeXpose definitely gives us the best bang for the buck.”



## BENEFITS

NeXpose protects networks using techniques other products can not duplicate. Most vulnerability assessment scanners superficially scan networks against a database of vulnerabilities, comparing patch levels and looking for default passwords and other types of exposures. NeXpose uses artificial intelligence technology to probe the network using coordinated attacks. The software will not only list potential threats and fixes more accurately, but also identify which of the devices are most vulnerable to the threat before the hosts are compromised.

There were four key features that made NeXpose the leader:

- **Alerting** - NeXpose can be integrated into SNMP consoles and in-house ticketing systems, making remediation of vulnerabilities more streamlined.
- **Customized reporting** - NeXpose efficiently scans their network and delivers comprehensive information showing vulnerabilities that could be used to compromise their network. They customized this information for various entities including executive summaries for upper management and detailed audit and remediation reports for system owners.
- **Supports Linux** - NeXpose is very easy to use and runs on Linux and Windows. Most of the competitors' products only run on a Microsoft Windows platform, but many security people prefer to run security products on Linux.
- **Broad Platform Coverage** – NeXpose performs audits on operating systems, databases, applications and Web servers all from a single product, easily supporting the diverse environment of this mortgage lender.

NeXpose provides a complete solution to vulnerability management, incorporating vulnerability management, risk assessment, remediation information and ticketing functions enabling security teams to easily identify, manage and report vulnerabilities across the entire network. In addition, NeXpose provides an accurate and thorough assessment of your organization ensuring organizations maintain up-to-date insight into its vulnerabilities and exposures at the entire enterprise level.

“NeXpose helps me limit the risk vulnerable systems can have on my company,” said the exploit management team manager. “We hunt down rogue systems, take infected computers off our network, and generally make our network a safer place.”