Foundstone®
STRATEGIC SECURITY

CASE STUDY

Security Risk Management Case Study: AT&T

Global Communications Leader Deploys Vulnerability Management Solution That Scales to Size

July 2004

*This report was prepared by **CRA Reports**, an independent reporting agency based in Washington, DC.*

Security Risk Management Case: AT&T Deploys Vulnerability Management Solution

Serving 40 million residential customers and another 4 million businesses, AT&T operates the largest telecommunications network in the world. For many consumers and businesses, AT&T is a comprehensive provider of network services that underpin the quality of their life and ensure the effective connectivity of their businesses. People and organizations around the world have come to count on the reliability, high-availability and security of the AT&T network for their voice and data communications.

AT&T's network security is overseen by its Global Network Technology Services unit, which is home to the Security Center of Excellence for the carrier. This center addresses security for all of AT&T's networks, including its circuit-switched network and high-speed packet data network—both of which are among the world's largest in those categories. The security group also addresses its U.S. IP-backbone network—one of the largest in the nation.

AT&T's security challenges are multi-dimensional—identifying and fixing software bugs, identifying and correcting network performance inhibitors, and monitoring ports to ensure they are consistent with application support and availability. These challenges underscore IT security's fundamental importance to the company.

> *"Security is part of our value proposition. It is part of the reason we are so well-accepted in the business community."*
>
> **– Ed Amoroso, AT&T's Chief Security Officer**

…Vulnerability Assessment: A Major Pillar of Security at AT&T

One of the pillars of AT&T network security operation is a system that can continuously and reliably assess its vast network assets for vulnerabilities, and then provide effective reporting to allow the security team to remediate these liabilities. Like many leading companies, AT&T has been deploying and optimizing such systems for a number of years.

In 2003, as part of its ongoing review of operations and systems, AT&T evaluated its existing vulnerability assessment systems and also scrutinized alternative assessment tools and solutions available in the marketplace. As a result of this analysis, the security team concluded that AT&T should centralize and standardize its system assessment operations and tools.

> *"We knew that, by centralizing these things, we could get commonality of security levels. Centralization also saves departments or operations the time and effort of purchasing their own assessment products, independently."* **– Eugene Kachurak, AT&T Labs**

After analyzing vulnerability assessment solutions in the market, AT&T selected the Foundstone Enterprise Risk Solutions™ system from Foundstone Inc., Mission Viejo, California.

…Lean, Highly Scalable System

The company deployed the Foundstone Enterprise™ solution across multiple locations on multiple networks and over 400,000 live devices. The AT&T security team reports that the systems are operating well.

> *"The solution is extremely lean and mean. It gets in and out very quickly."*
> **– Eugene Kachurak, AT&T Labs**

The security team determined that Foundstone Enterprise allowed analysts to quickly switch between quick "snapshots" of vulnerabilities that could then be used by analysts to conduct "full-blown, exhaustive assessments." In both types of assignments, AT&T found that the assessment accuracy was very high and produced very few false positives.

AT&T engineers also have found that the new systems make it easier to address the vulnerabilities that are identified through assessment. "Remediation is taking place smoothly," said Kachurak.

AT&T's security group reports that the Foundstone vulnerability management solution has been well-received by users throughout the company. Network administrators and operators, in particular, find that the services provided by the centralized security team have lightened their workloads. Prior to the implementation of Foundstone Enterprise, the responsibility for identifying, deploying and operating assessment tools fell on individual network operations teams spread out across the company. Now, the assessment and management responsibilities reside in one, consolidated location.

One of the most important values of the new solution for AT&T is its scalability, which was proven during the deployment throughout AT&T's networks.

> *"There are other tools on the market that are extremely well-made. But I don't think anything we reviewed other than Foundstone scaled as well to the scope of our global network."*
> **– Eugene Kachurak, AT&T Labs**

…Smooth Deployment Featured User Outreach

The deployment of the Foundstone Enterprise solution began with several months of testing different prototype configurations of the new assessment system at various AT&T locations around the world. After that, AT&T engineers rolled out the new security system at network operations centers in Schaumburg, Ill. and Tampa, Fla.

The initial rollout featured regular assessment of several thousand IP addresses, according to Kachurak. As the initial deployments proved successful, AT&T installed more engines and began assessing more addresses.

The company is now assessing approximately 400,000 IP addresses per week using 14 engines deployed in various locations around the globe. This is up from about 30,000 addresses per week that AT&T was assessing using its former systems.

A major aspect of the rollout at AT&T was a carefully orchestrated outreach and education program. This multi-part outreach featured live training sessions, conference calls and preparation and distribution of AT&T-focused documentation that presented an overview of the Foundstone solution and its mode of operation within AT&T. These initiatives helped train the local and field engineers on how the Foundstone Enterprise Web portal operates and how its functionality compared to that of other systems in use or formerly in use.

Like any deployment of a new system tool, AT&T's implementation of the new Foundstone solution required close collaboration between engineers from AT&T and Foundstone. AT&T required a vulnerability management vendor that could "partner" and support the largest network in the world with world-class security expertise and responsiveness. Foundstone is meeting the important challenges of this large enterprise customer.

Today, the Foundstone Enterprise solution has taken its place alongside other vulnerability assessment systems that AT&T has deployed to protect its networks.

"We use Foundstone Enterprise as our primary solution for vulnerability management, and also have other tools for things like patch management. Ultimately, we look at our environment from every perspective possible – internal, external, application level, and transport layer, among others. In that context, the Foundstone solution addresses one of the network's vulnerabilities, and it's been doing a good job for us."

– Ed Amoroso, AT&T's Chief Security Officer