Making the Case For

Enterprise Security

AT&T's Defense In-Depth Approach

Executive Summary

It should be no surprise that AT&T, one of the world's leading networking providers, turned to the network to ensure its own security. In the late 1990s, confronting serious and continuing threats to the security of its internal communications, AT&T at first deployed the same weapons customarily used by enterprises. This line of defense included firewalls, intrusion detection systems, antivirus programs, spam filters and Web surfing controls, duplicated multiple times across the company's global locations.

The resulting security came at a high cost in those days. These protections required continuous management, frequent software updates and regular replacement of hardware platforms. The work required many hours, invested by highly trained security staff.

Facing continuing pressure to cut costs and deploy resources to the most productive projects, the company's security and IT managers sought a simpler and more efficient way to provide security. All information that moves across LANs or WANs must cross the network, they reasoned, so why not centralize security there? That way an enterprise-wide security infrastructure, managed centrally, could deliver the efficiency and effectiveness that AT&T required.

Today the company's firewalls, virus and spam filters, intrusion detection systems and other major security systems are located in the network. Coupled with premises-based security elements that protect the PCs of its employees, AT&T has an end-to-end approach for security across its global enterprise that is cost-effective, easier to manage and provides for enhanced security over traditional premises-based methods.

Specifically, this network-centered security solution has enabled AT&T to reduce licensing costs, choke off the torrent of spam that once burdened the internal network and redirect highly skilled security resources to serve customers. The network-based defenses are backed by a powerful threat analysis system that scans network activity to detect subtle changes that could signal a developing attack, and alert network security specialists.

Most importantly, AT&T's comprehensive security approach has drastically reduced the number and frequency of business disruptions caused by security problems.

The Challenge

Seeking Higher Ground Against a Rising Tide of Threats

Like every enterprise, AT&T faces multiple and growing threats to information security.

Software viruses, Internet worms and denial of service attacks have become common. "Phishing" schemes aimed at extracting personal information from unsuspecting users appear every day. Much of what attempts to enter the corporate intranet is made up of unsolicited commercial messages, or spam. According to AT&T security experts, more than 75 percent of the e-mail messages aimed at the att.com portal daily are spam.

By 2003, increasing security threats were starting to impact AT&T's operations. In August 2003 security managers had to block ports in an emergency response to stop an attack by email attempting to deliver a dangerous new worm. Then, a few months later, a massive onslaught of spam started arriving at the att.com site. The company had to suspend the flow of e-mail until the problem was brought under control.

Today's security problems stem from three developing trends. First is faulty software, which leaves security vulnerabilities that troublemakers can exploit. If managers fail to patch those problems, they leave the doors open to intruders. A second problem starts with 'zombie' personal computers that spammers can control from afar and use to mount spam and denial of service (DOS) attacks. The third challenge arises from networks and systems that are increasingly interconnected and integrated. As AT&T Chief Security Officer Edward Amoroso put it, "Once it was hard for corporations to connect two networks. Now it's almost impossible to separate them."[1]

In such an environment, close attention to security is vital. But maintaining security poses significant business challenges:

- Network convergence. Increasing interconnection and interlocking dependencies across the many applications makes security management intricate, sensitive and difficult.
- Disparate security solutions. Multiple security solutions may be available for each area of jeopardy, which raises the question of how these solutions can be integrated most effectively.
- Increasing risks. Rapid change makes security problems a moving target. According to a September 2005 report in the Wall Street Journal, almost 11,000 new viruses and worms attacking Microsoft Windows appeared in the first half of 2005. The newspaper reported that nearly three quarters of the top 50 malicious programs were designed to expose confidential information.[2]
- High cost. For corporations trying to manage these concerns, security raises significant issues of resource allocation. The increasing number of applications running across the network drives cost, and security personnel require a high level of expertise and ongoing training.

at&t

Like most enterprises, AT&T first attempted to solve its security problems by setting up a defensive "DMZ" on its premises, armed with an arsenal that included firewalls, an intrusion detection system (IDS), anti-virus, anti-spam and worm detection capabilities, packet filtering, LAN filtering, security patching, policy enforcement and incident response. This security stockade required continuing professional maintenance, including regular investment in software and hardware upgrades to keep pace with changing threats.

Key Areas for a Network-Based Security Solution

- **Firewall enforcement**
- **Intrusion detection**
- **Email filtering**
- **URL filtering**
- **DOS filtering**
- **Threat management**

Response

Consolidating Security in a Unified Network

In early 2004, AT&T security planners stepped back from these daily battles to take a more comprehensive and systematic approach to security planning and implementation. How do we utilize the inherent strength of AT&T's network, they asked, to create security solutions that meet our internal needs and also meet the needs of our customers? Why not move many security defenses out of company offices and into one network that ties all those sites together?

Like most large enterprises, AT&T was using a system of premises-based security firewalls distributed across the company's many locations. The attacks experienced in 2003 made it imperative to find a better security solution. The company reviewed several options. As discussions continued, the most effective and efficient solution emerged: a solution based not solely on the company premises, but a layered approach with an emphasis on leveraging the network.

AT&T's Concept of One[SM] set forth the vision of a network in which security and ease of management would be built in. The consolidation of disparate security systems onto the network platform had the potential to dramatically reduce the redundant work required to maintain multiple systems.

The network-based security solution would have to deliver protection in six key areas:

1. Firewall policy enforcement. Firewall functionality was embedded in the network, using the same technology as a premises-based system. Using that technology in the network to stop threats before they ever reach the company premises made the network-based firewall highly effective.
2. Intrusion detection. Alarms from the intrusion-detection system were easily incorporated with network-based firewall activity logs.
3. E-mail filtering. Cleaning viruses and spam from incoming e-mail was addressed by automatically examining the content of data packets and placing those containing virus or spam in quarantine.
4. URL filtering. To help control network usage and prevent employees from spending time on unauthorized Web surfing URL filtering was established.
5. Distributed Denial of Service (DOS) attacks. A DOS attack is likely to be initiated by gaining control over thousands of PCs and aiming their energy at a destination IP address. Those streams of data combine to form a torrent of data. The best place to stop that flood is not on the premises but far upstream in the network, before the flow gains strength.
6. Threat Management. By analyzing network activity in fine detail, identifying subtle changes from normal traffic patterns and acting early, AT&T could see the very beginnings of a developing DOS or spam attack and cut it off before it caused problems.

The solution the AT&T team put in place includes two primary components. A layered security platform that applies network-based security, including network-based firewalls, virus and spam filters, operates to stop security problems before they ever reach the company's offices. These measures operate in tandem with a second key component, a powerful threat management system that continuously scans traffic and enables AT&T security managers to identify emerging problems, see their sources, and take preventative action before they affect operations.

Planning and Implementation

Parallel Paths to Enterprise Security

In order to quickly address the growing risks, the security initiatives moved ahead not step by step, but on parallel paths. The first path the company took moved its internal security operations onto network-based firewalls, which is a service now available to AT&T customers.

Over roughly the same period, AT&T developed a robust traffic monitoring and threat management system, internally referred to as Aurora. Because no commercial database can handle the 20 terabytes of IP metadata that AT&T monitors on its network everyday (just building the database for a day's traffic would take more than 24 hours), AT&T Labs built a threat management system to handle the vast traffic and complex relationships that characterize the network.

Security analysts at the AT&T Global Network Operations Center in Bedminster, N.J. are able to collect and process network information from across the globe. Applying different diagnostic algorithms, they uncover and resolve an average of 40 security cases each day.[3]

You start to see little things develop and you stop them before they can build into anything. That's what carriers can do with network-based denial of service. I think it has the potential to render the distributed denial of service problem moot

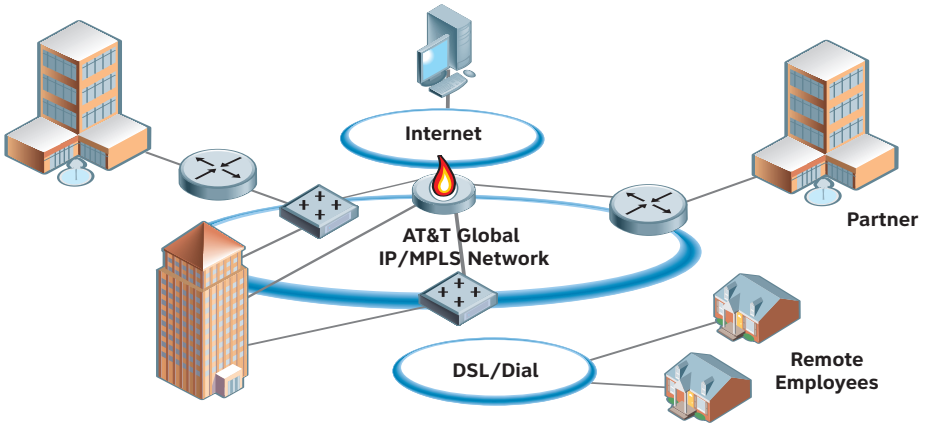
Edward Amoroso, AT&T Chief Executive Officer

Results – Simplicity Produces Security and Savings

Simplicity

AT&T's revised security approach is clearly less complex. And less complexity means fewer elements to buy, secure, maintain and upgrade; fewer interfaces to rely on; and fewer facilities and less physical geography to cover.

AT&T Network-Based Security



Moving to the network-based firewall has eliminated 80 dedicated premises-based firewalls.[4] Instead of three e-mail gateways, AT&T now needs only one, because network-based protection is stopping a vast amount of spam, viruses and other suspect traffic – once 75 percent of the total – before it reaches the gateway.

Improved Security

In 2002, viruses, worms and spam problems were causing outages and extremely slow e-mail performance for AT&T's internal users. Today there is a qualitative difference due to the security approach that the company implemented to solve its own problems and now offers as a service to its customers.

Out of 2.5 million daily inbound e-mail messages, 2.1 million are now blocked in the network based on security parameters. This e-mail filtering frees up network resources for legitimate traffic, more than doubling the bandwidth effectively available.[5]

AT&T has also improved its system for patching software bugs and upgrading virus protection in the thousands of PCs used by employees. Early on, the security team discovered that there were PCs in use throughout the company for which they had no virus protection information. So the team implemented a method for security patch downloads that cover 90 percent of PCs in use. Now patches are delivered automatically, without assistance from IT staff, when users log onto the network.[6]

In addition to fending off attacks and providing more consistent software patching, AT&T's security approach is designed to assure business continuity. Security infrastructure equipment is housed in hardened AT&T data centers, disaster-ready buildings equipped with robust backup systems, instead of being dispersed at potentially more vulnerable enterprise sites.

Since backbone providers see DDoS attacks every day, they can mitigate them much more cost-effectively than a company investing in the technology itself.

***"Security in the cloud; Telcos Reclaim Network Intelligence Through Security"* Forrester Research, Inc. March 1, 2005**

AT&T also simplified the job of managing security policies across a complex, multi-site organization. AT&T's security team set inbound and outbound policies through an Internet portal, and have the option to apply policies uniformly across the enterprise, or to adjust policies to fit the differing needs of facilities and business operations.

Savings and Reduced TCO

Removing the burden of managing an infrastructure that is deployed at multiple sites across a broad geographic footprint has also enhanced efficiency. Network-based spam filtering uses the same filtering technology as premises-based filtering, but it is far less costly and more efficient because it consolidates the number of systems that must be deployed, managed and maintained.

System upgrades are vastly simplified because they are centralized, not repeated multiple times across a distributed system of security DMZs. And the work required to keep systems up to date can be significant: Network based e-mail security defenses may be upgraded in response to a new virus signature or new e-mail threat as often as every ten minutes.[7]

Lessons Learned

Software, System Management and Simplicity

AT&T's experience in migrating to a comprehensive security solution has taught the company several key lessons that it shares with customers to help alleviate their security challenges.

Fix the Software Now

Software still continues to be a key source of vulnerability, due to broken code – a problem that is not likely to change for a long time according to Amoroso. So rather than wait until a comprehensive service pack is available to remedy software problems – an approach that Amoroso calls "patch roulette" – AT&T's security team updates PC software as soon as patches are available. For nine out of ten AT&T employees who are connected to the corporate network, downloads are automatic. Other employees receive notices that action is required. Enterprises should have a plan in place to quickly deploy patches as soon as they are available to avoid risk.

Eliminating premises-based antispam systems has saved approximately $400,000 a year. And AT&T has been able to reduce the number of engineers devoted to internal WAN and security management by 50 percent.

"The network-based services wil augment, rather than replace internal security controls. Existing people and technology will deal with fewer security incidents, rather than just dealing with noise."

***"Security in the cloud; Telcos Reclaim Network Intelligence Through Security"* Forrester Research, Inc. March 1, 2005**

Unify Leadership and Vision

"All the things that we have done would not have been possible if organizational changes were not made," says AT&T security manager Sanjay Macwan. "Many security groups are very product-specific, dispersed across corporations in a variety of different organizations. The synergies just don't exist for everybody to come together under a single direction from a single leader."[8] By consolidating security management, AT&T has conquered those organizational issues. Enterprises should create a vision and align key resources in order to gain productivity and strengthen overall security.

Watch the Indicators

"The AT&T security team pays a lot of attention to indicators," Amoroso notes. "If you talk to information security teams from the enterprises around the globe, most of them will tell you that when they are doing incident responses, it is because the LAN is down, people are complaining, e-mail is not working, and applications are broken. AT&T does not wait until something is broken. In fact, the security team is rewarded for handling security incidents in a proactive way."[9] Enterprises should have a proactive security program in place that addresses security risks as early as possible.

Conclusion

Redefining the Industry with a Security Revolution

Beyond creating a significant improvement in AT&T's internal security – and at the same time helping cut costs – AT&T's experience with network-based security and threat management is pointing the way for the company's customers.

AT&T has a portfolio of security services that protects customer's vital data and secures their enterprise networking environment. AT&T delivers a suite of offers that assess vulnerabilities, protect customer's infrastructure, detect attacks and respond to suspicious activities and events.

A leading innovation that came from the company's own learnings is AT&T's service called Internet Protect℠ Service. This security alerting and notification service offers advanced information regarding potential real-time attacks including viruses, worms and DDOS attacks that are in the early formulation stages.

"We think that what we are doing to protect the AT&T enterprise is revolutionary," Amoroso says. "It saves an awful lot of money, it's more effective and it's allowed us to help customers address their security challenges. We believe that we are helping to redefine the industry."

References

1. Amoroso interview Sept. 23, 2005
2. "Huge Numbers of Spammers Hack Away at PCs," Sept. 19, 2005, The Wall Street Journal
3. Amoroso interview Sept. 23, 2005
4. Daudelin presentation April 6, 2005
5. (Morris notes)
6. (Morris notes)
7. Amoroso interview Sept. 23, 2005
8. Security staff interview July 20, 2005
9. Amoroso interview Sept. 23, 2005

For more information, contact your AT&T Representative, or visit www.att.com/business.

About the Series

This is one in a series of case studies aimed at sharing the lessons AT&T has learned within its own business about how next-generation networking solutions can pay off: enhancing productivity and reducing total cost of ownership (TCO). Our goal is to provide real world answers, based on real life experience, that help executives deal effectively with today's business issues.

Our own approach to enterprise networking is built on the principle that solutions must deliver value and enhance the performance of business applications. We begin with a vision to consolidate our network into a single, global, MPLS-enabled IP network with consolidated operating support systems.

We hope that these papers will serve our customers as a practical networking roadmap. We have put this roadmap to the test inside our own business. AT&T faces the same business challenges as other enterprises, and we believe strongly that the solutions we provide our customers should be the same that we use across our own company. If a solution creates value for AT&T, it will for customers, as well.

at&t Your world. Delivered.