



## Case Study American Residential Services

### MXtreme™ Mail Firewall



“Deploying MXtreme to handle all email traffic for spam has solved an enormous administrative burden and saved the IT group time and money. We spend less than 5 minutes a day administering MXtreme's anti-spam features,”

Jason Sosinski  
Information Systems Security  
Administrator  
ARS

### American Residential Services Inc.

A subsidiary of ServiceMaster, a Fortune 300 company, American Residential Services (ARS) provides heating, cooling, plumbing, drain cleaning and electrical needs, with uncompromising professional service. Headquartered in Memphis, Tennessee, ARS has served more than 1.3 million residential and commercial customers from one of 95 locations throughout the U.S.

### Eliminate a \$2million Per Year Spam Problem

Extending out from its main data center in Houston, Texas, ARS's information systems group provides services for 2500 people dispersed across the country. Email communications is a critical resource. By 2003, unsolicited bulk messages or spam, was beginning to explode across the Internet and ARS, like everyone else was becoming a victim.

According to Jason Sosinski, Information Systems Security Administrator at ARS, “we began tracking our messages and found that about 30% of all our email was unsolicited and the number was rising. Our internal audits placed the loss on user productivity at about \$2 million per year.”

To confront the flood of spam, ARS tried several anti-spam filtering solutions but found a high cost of maintenance and management in those approaches. “The problem we found with the filtering solutions we looked at is that you have to spend a lot of time examining what is coming in to develop rules that block the bad mail but let the good mail in,” said Sosinski.

### MXtreme™ Mail Firewall



Spammers use automated software tools and quickly evolve their tactics as defenses improve. They are capable of generating millions of messages per hour, with no incremental cost to create new messages. Unfortunately, once a spammer gets your email address, you can never escape. "Spammers were constantly adapting their methods of attack and as a result, bypassing our filter rules," said Sosinski. "We just couldn't keep up."

### Mxtreme Utilizes Several Automated Anti-Spam Technologies

Sosinski and his team realized they needed an automated solution that would not require much administrative attention. Sosinski decided to try the BorderWare MXtreme Mail Firewall Appliance, which delivers the most comprehensive solution for protecting email systems from all threats like spam, viruses, Trojans and worms, to malformed messages and denial of service attacks, while enabling overall email server functionality, sophisticated routing and delivery, and secure remote access.

At the heart of MXtreme is BorderWare's security technology called S-Core™, a hardened operating system that is integral to the Common Criteria EAL4+ (with EAL5 vulnerability analysis) certification achieved by BorderWare's firewall security products. The Common Criteria is a set of international standards subscribed to by 14 nations (including the U.S.) that grades products on their security and reliability, as well as the development and support processes for ensuring quick responses to problems. EAL4+ is the highest grade achieved by commercial software.

### MXtreme™ Mail Firewall

A photograph showing a person's profile from the chest up, looking intently at a computer monitor. The person is resting their chin on their hand. The background is a bright, slightly blurred office environment.

To fight spam specifically, MXtreme provides for local compilation of white and blacklists – filters that an IT administrator can set manually by source, destination, pattern and text matches to accept mail from trusted sources, like business partners or block messages from known spammers and their tactics.

Moreover, MXtreme assimilates several automated tools. The RBL (Real Time Blackhole Lists) blacklist is a source on the Internet maintained by individuals that have identified spammers. A second component is DCC (Distributed Checksum Clearinghouse), which contains lists of message signatures that sort out bulk mail. MXtreme automatically checks these databases to identify possible spam messages.

The third and most valuable spam-fighting component is a unique technology found only in MXtreme. Known as Statistical Token Analysis (STA), it performs lexical analysis on messages, and "learns" to identify mail patterns based on the customer's own usage and stream of communications, and is highly effective in differentiating between legitimate messages and actual spam.

### MXtreme Stops Spam, Administers in 5 Minutes

Although the cascade of spam now accounts for half of all email traffic at ARS, MXtreme has met the challenge. "Deploying MXtreme to handle all email traffic for spam has solved an enormous administrative burden and saved the IT group time and money. We spend less than 5 minutes a day administering MXtreme's anti-spam features," said Sosinski. "Most notably, our users are much happier."