

A NEW LEVEL OF PROTECTION

Security is not about what you can **STOP.**

It's about what you can **START.**



A THOUGHT LEADERSHIP PROFILE: NETWORK ASSOCIATES

State, local and federal government IT systems are under almost constant attack by a barrage of assailants — from mischievous hackers to malevolent cyber-terrorists.

Virus, worm and Trojan attacks are significant and growing concerns for government agencies, and IT staffs are scrambling to keep up. Today's cyber-attacks are not only extremely sophisticated, but also fast and frequent.

McAfee Security® offers an effective response to these mounting threats. As part of the McAfee Protection-In-Depth Strategy™, our McAfee Intrusion Prevention Solutions help organizations such as yours assure the availability and security of their network infrastructure everyday. In this challenging economic environment, it is essential to have tools that can help you realize your network's full performance potential.

A New Level of Proactive Threat Protection

McAfee Security enables agencies to be proactive in real time

Today, both docile and deadly cyber-diseases propagate at incredible speeds.

With the luxury of IT reaction time now gone for good, the key to total security is proactive prevention. “It used to be you would have a little bit of time when you could fix your system, patch it and protect servers,” said Chris Coyle, senior systems engineer for Network Associates®. “But that time is no longer available to an IT staff.”

Only a few years ago when the I Love You Virus burst unwelcome onto computers worldwide, it spread at a rate of about 3,000 desktops per hour. By comparison, the recent Slammer virus raced throughout the world several months ago with nearly incomprehensible speed, spreading worldwide in about 10 minutes, according to the Cooperative Association of Internet Data Analysis (CAIDA).

“Local governments are trying to protect local infrastructures, power systems, emergency systems and many kinds of records,” said Coyle. “They can’t afford to have any downtime.”

Although software patches can shore up known vulnerabilities, they present their own set of management headaches, and they can’t protect systems from the steady onslaught of new and sophisticated attacks.

As part of its “Protection-In-Depth Strategy,” McAfee products include comprehensive content protection for collaborative computing environments. Cutting-edge McAfee Enterecept and McAfee IntruShield instantly detect and actually stop harmful attacks including viruses, worms, malicious code and inappropriate content that can wreak

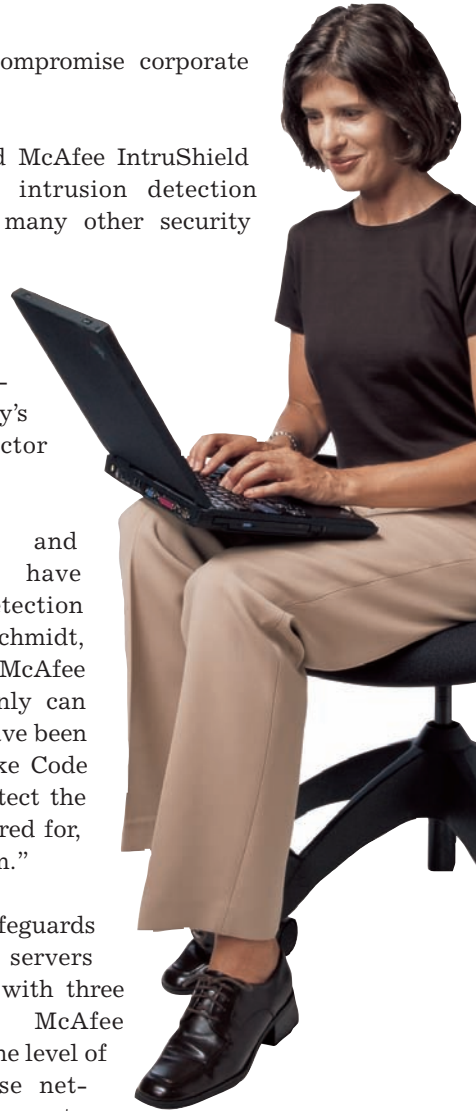
havoc on servers and compromise corporate systems and networks.

McAfee Enterecept and McAfee IntruShield go beyond the simple intrusion detection systems utilized by so many other security devices. In fact, McAfee Security solutions can stop malicious activity in real time. They deliver proactive intrusion prevention for today’s beleaguered public-sector computer systems.

“McAfee Enterecept and McAfee IntruShield have incredibly accurate detection capability,” said Rudy Schmidt, director of IPS Sales for McAfee Security. “So we not only can take on the things that have been out there for a while, like Code Red, but we can also detect the things you haven’t prepared for, block them and stop them.”

McAfee Enterecept safeguards Web servers, database servers and application servers with three layers of protection. McAfee IntruShield offers the same level of protection for enterprise networks, data centers and remote branch offices.

Government agencies demand multi-level protection to safeguard sensitive public data. But agencies previously



“It used to be you would have a **little bit of time** when you could fix your system, patch it and protect servers, but **that time is no longer available** to IT staff.” — *Chris Coyle*, senior systems engineer, Network Associates

SECURITY BLANKET

Entercept intrusion prevention solution stops attacks on Arlington County servers before they happen.

The government of Arlington County, Va., is not unlike many other local jurisdictions across the nation — providing vital services to a population of more than 200,000.

But as home to crucial federal government organizations such as the Pentagon, the Defense Intelligence Agency and Department of Defense, Arlington County officials are particularly cognizant of the need for IT security.

“We needed **real-time protection of our servers** and services so we could assure they would be up and running whenever we needed them. **We needed Entercept** to ensure we had something in place to react to vulnerabilities and threats instantaneously.”

— **Vivek Kundra**, former director of Infrastructure Technologies, Arlington County, Va.

To safeguard county servers from potentially dangerous attacks, the county recently installed McAfee® Entercept® intrusion prevention technology from McAfee Security.

“I purchased the Entercept product as a part of our post 9/11 security strategy,” said Vivek Kundra, former director of infrastructure Technologies for Arlington County. “For us, cyber-security was critical, especially given the critical national assets located here.”

Real-time Security

The county previously had invested in firewalls, virus protection and anti-spam protection, but Kundra knew exactly what his system lacked. “We needed real-time protection of our servers and services so we could assure they would be up and running whenever we needed them,” explained Kundra. “We needed McAfee Entercept to ensure we had something in place to react to vulnerabilities and threats instantaneously.”

Kundra compared products from other vendors, but chose the McAfee Security solution. “The Entercept technology is the most advanced,” he said. “It is clearly the leader in the industry.”

McAfee Entercept safeguards servers by preventing known and unknown attacks. Using a combination of behavioral rules and signatures, Entercept actually prevents attacks rather than detecting and reporting them after the fact — when damage may already have been done.

Arlington County runs McAfee Entercept on 60 of its servers. Soon, that number will rise to 75. Kundra said eventually McAfee Entercept will run on virtually every server the county operates.

Up and Running

Arlington County’s strategy is simple: Keep servers up and running 24/7 so that vital services can do the same.

“These servers are the backbone of basically all county services,” said Kundra. “They’re accessed by thousands of government employees, by the county treasurer, constituents utilizing our Web site, the Department of Human Services, our water

department, and emergency services such as fire, police and EMS. Even the library needs these servers up and running.”

The value of McAfee Entercept became obvious during the recent proliferation of the Lovsan/Blaster and Nachi viruses. Although many government agencies were stricken by the viruses and faced long clean-up and restoration procedures — with some shutting down for days — Arlington County’s systems were untouched. Efficient, secure and reliable servers clearly deliver cost savings — especially when considering the millions of dollars it can cost to clean up infected systems — but Kundra believes McAfee’s protection is worth more than money.

Trusted and Trustworthy

“Worse than losing money from downtime is losing public trust,” Kundra said. “If our job is to provide a certain service, and we can’t get our system running for three or four days, we lose public trust. And that’s something you can’t gain back.”

Just as the public can trust Arlington County services, county officials know they can trust McAfee Security, according to Kundra.

“Arlington County is a very demanding customer. We have to be,” explained Kundra. “McAfee Security has always been behind us and went out of its way to make sure our implementation was excellent. That’s why I never hesitate recommending McAfee Security. I know they look out for our interests.”

With the McAfee Entercept solution in place for more than a year, Kundra said the county plans to make the product a “base item” in its budget. “The idea is that any capital IT expenditure would mandate that McAfee

Entercept is included,” Kundra said. “In a new project, we would require that McAfee Entercept be installed on any new server. You would have to have it or the project wouldn’t go.” Kundra believes the mandate is imperative because, “security is so critical, especially in these times.”

Preventing unwanted cyber-intrusions is important to any government jurisdiction. However Arlington County officials say they must remain on the cutting edge of security technology, given the critical facilities located in their backyard. And McAfee Security allows them to do just that. “We’ve invested heavily in technology, and we are leaders in delivering

“**Worse than losing money** from downtime is losing public trust. If our job is to provide a certain service, and we can’t get our system running for three or four days, **we lose public trust**. And that’s something you can’t gain back.”

— **Vivek Kundra**, former director of Infrastructure Technologies, Arlington County, Va.

government services in an efficient, cost-effective and trusted manner,” said Kundra. “We have to be. This is a prize area. It’s Americana at its best.”



needed to combine products from several vendors to meet the requirement — raising both the initial purchase price and ongoing management costs. With McAfee Security, both solutions deliver unmatched protection against intrusion through signature and anomaly-based detection, as well as denial of service (DoS) and distributed denial of service (DdoS) detection.

The integrated design of McAfee Enterecept and McAfee IntruShield simplifies security management

Ultimately, vital government IT operations must function without the fear, lost staff productivity and unplanned budget drains caused by system attacks and security breaches. That's why today, more than 70 million users rely on McAfee Security anti-virus software to protect them from unwelcome cyber-intruders.

“With the need to protect such critical data as state and county records and emergency information, there is no room, nor can any be afforded, for

“With the need to **protect such critical data** as state and county records and emergency information, there is no room, nor can any be **afforded, for any hint of a vulnerability** that would create system downtime.”

— *Mark Small*, senior vice president of sales, government, health and education for Network Associates

and lowers operating expenses. “Because so many attacks today are blended attacks, we can significantly reduce an analyst’s time by correlating across those engines,” said Schmidt.

In addition, the McAfee Enterecept zero-day attack prevention capabilities can significantly slow — and even stop — the spread of viruses and worms. McAfee Enterecept also includes patented technology to halt “buffer overflows” — the most common new type of threat.

“This is not a silver bullet. Security is a process, not a product,” explained Schmidt. “But with these products, you can continue to do business.”

any hint of a vulnerability that would create system downtime,” said Mark Small, senior vice president of sales, government, health and education for Network Associates.

Thousands of federal, state and local agencies, including Antelope Valley Hospital, Arlington County, Va., and the U.S. Army Reserve, trust McAfee Security products to safeguard systems and networks against threats ranging from amateur hackers to sophisticated terrorists. These solutions offer more than just a way to stop attacks, they enable governments to build proactive security, enterprise productivity and most importantly, peace of mind.

Network Associates®

Corporate Headquarters:
3965 Freedom Circle
Santa Clara, CA 95054

start.mcafeesecurity.com

This *Government Technology Public CIO* Thought Leadership Profile was sponsored by Network Associates.
Copyright © 2004 *Public CIO*. All rights reserved. Printed in USA.