



## Major Urban Utility Company

### Customer profile

Utility company in major urban city center serving ten million customers

### Industry

Power

### IT environment

Serves over 10 million customers and over 17,000 employees

### Challenges

Protect the Control Center from attacks with reliable, easy to deploy, manageable and flexible security solutions

### McAfee solution

McAfee Firewall Enterprise Edition (Sidewinder)

### Results

- Independent Systems Operator (ISO) networks can interconnect without jeopardizing the control network
- Vulnerability tests confirm that McAfee Firewall Enterprise Edition (Sidewinder) cannot be penetrated
- Patches and upgrades can be delayed without a risk to security
- Meets the company's 99.99999% standards
- Ability to add a new rule in minutes

## Major Urban Utility Selects McAfee Firewall Enterprise Edition to Protect Critical Control Systems

Utility companies in major urban centers have many competing risks to balance. In a typical corporate network, IT administrators worry about "CIA"—confidentiality, integrity, and availability—in that order. But to an IT specialist in charge of security at a utility control center in a US metropolitan area serving ten million customers, the priorities are very different. He worries about "AIC"—99.99999% availability, integrity of the data, and confidentiality ranked as a distant third.

Integrity is about making sure that critical information is communicated reliably and is unchanged. After all, the last thing a utility would want is for a sub-station to be told to shut down when in fact more power is actually required. Inaccurate information could cause damage to critical equipment, release of hazardous materials into the environment, or even a threat to national security.

Since availability is critical, normal maintenance schedules don't apply. Even installing a new signature file can actually constitute a denial of service and can disrupt the flow of power to the utility company's customers. In addition, hardware in these environments is expected to last 15-20 years and only be brought down for maintenance every 6 or 12 months. This represents a nightmare for the average security vendor who needs to apply regular security updates and patches.

In addition, much of the control system infrastructure was designed decades ago, when data centers practiced "security by obscurity." The only way to attack the control system was by physically being in the network room. Not so today; control systems are interconnected to corporate networks and to other utilities via Independent System Operators (ISO) networks for the sharing of power and information between power generators.

### Easy to manage, strong and secure

"When I went looking for a firewall 14 years ago, I knew I needed the strongest and most secure product available. But I also needed something that I could manage easily. I selected McAfee Firewall Enterprise Edition (Sidewinder) because it allowed no root access, had never been hacked, and had a reputation that was just sterling," says the IT Specialist at this utility. With his CISSP and CCNA credentials, he understood exactly what he needed to protect the control systems both then, and now. McAfee's Network Security Business Unit (*formerly* Secure Computing) has been able to satisfy the company's requirements for robust solutions that are easy to manage and reliable.

"As you can imagine, we're a highly regulated industry, but unfortunately, most of the regulations talk a lot about the 'what' and very little about the 'how.' So we're left to develop our own best practices for a security model," continues the IT Specialist.

What worked 14 years ago is still working today. This utility company still uses McAfee Firewall Enterprise Edition to protect the control network from all sides. Redundant pairs sit between the primary control center and 1) the corporate networks, 2) the QA network, 3) the backup control center, 4) the EMS network, and 5) the ISO network. McAfee Firewall Enterprise Edition makes

sure that no one can communicate with the control network without proper credentials, ensuring the integrity of all data communications. It also gives the utility the ability to connect with the ISO without risking the integrity of their systems.

And the all-important availability considerations? “In 14 years the only problem we’ve ever had with the McAfee Firewall Enterprise Edition devices was several years ago when there was a hard disk failure in one of the boxes. But since it was hardware that we supplied ourselves, I can’t complain too much.” The utility has followed the multiple generations of McAfee Firewall Enterprise Edition and recently upgraded to the latest version. All of the upgrades have been seamless and painless. He adds, “McAfee Firewall Enterprise Edition performs excellently. If there’s a problem somewhere my people all know it’s not the McAfee Firewall Enterprise Edition. We experience about 99.999% availability. McAfee Firewall Enterprise Edition has never had to issue a security patch, so we don’t have to worry about bringing down the firewalls

for maintenance more than once or twice a year. In fact, just knowing I have the firewall in place is what allows me to sleep at night.”

**A virtually impenetrable barrier**

As with all utility companies, regular vulnerability testing occurs to ensure the security of the control network. In 14 years, the vulnerability testers have never been able to penetrate the McAfee Firewall Enterprise Edition barrier. In fact, the testers can’t even see that a network exists past the firewall.

If he had to go shopping today for a firewall, this IT specialist knows what’s on his list: Strong security, availability, ease of maintenance, and the flexibility to design custom proxies rapidly for control system-specific protocols.

And his choice today? Same as 14 years ago. “From everything I know and everything I’ve read, McAfee Firewall Enterprise Edition (Sidewinder) is still best-of-breed. Add that to the great support I get from McAfee, and my decision is an easy one. ”

---

*From everything I know working with this security device for 14 years, plus everything I’ve read, McAfee Firewall Enterprise Edition is the best-of-breed. The fact that we use them in our control center is what allows me to sleep at night.*

**IT Specialist**  
**Major Urban Utility**

---

