



A Trusted Security Expert HAS THE PERFECT PRESCRIPTION FOR INTERNET SAFETY

Managed Security Services from Internet Security Systems are the University of Colorado Hospital's antidote to hacker attacks

∴ Organization Profile

Top medical professionals, superior medicine and progressive change make the University of Colorado Hospital one of the leading hospitals in the nation. Ranked among the top 10 hospitals in the country by *U.S. News & World Report's* annual survey of "America's Best Hospitals," the hospital is internationally respected for its exceptional teams of medical specialists. With campuses in Denver and Aurora, Colo., the hospital has the Rocky Mountain region's only academic medical center. The Aurora campus is home to the prestigious Anschutz Centers for Advanced Medicine and the Rocky Mountain Lions Eye Institute. Recognized as the region's leading specialty care and referral center, the Denver campus is part of the University of Colorado Health Sciences Center campus, one of four campuses in the University of Colorado system.

∴ Increased Accountability

Entrusted with highly confidential patient data, the hospital is governed by the stringent regulations that were issued by the U.S. Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which became effective in April 2003. The HIPAA Privacy Rules require specific methods of handling protected health information. Fines, penalties and even jail time can be imposed for non-compliance. While protecting patient confidentiality and increasing network uptime have always been priorities for the hospital's IT department, the current regulatory environment, combined with an exponential increase in the frequency and virulence of hacker attacks, prompted Joe Bajek, University of Colorado Hospital's director of IT, and his team to ensure that the hospital's Internet security measures were up-to-date and state-of-the-art.

Customer

The University of Colorado Hospital

Profile

Health care organization

Location

United States

Situation

The University of Colorado Hospital needed to protect highly confidential patient information and mission-critical operations data from escalating Internet security threats.

Solution

Internet Security Systems provides the hospital with its Managed Security Services for reliable, cost-effective, 24/7 online security.

Benefits

ISS' Managed Security Services keep highly sensitive information secure and improve network uptime by protecting against internal and external threats, while allowing limited internal IT resources to focus on business-critical and strategic initiatives.

INTERNET | SECURITY | SYSTEMS®

Ahead of the threat.

∴ Gaining an Excellent Return on Investment with Managed Security Services

Working with Internet Security Systems (ISS) to upgrade the hospital's network security was one of Bajek's first responsibilities when he joined the IT department about five years ago. New on the job, but a seasoned veteran in enterprise security, Bajek was pleased to learn that the hospital was already working with a trusted partner for the hospital's Internet security strategy. While the firewall was an important building block for this strategy, Bajek quickly realized that defending against external threats 24/7 required resources and manpower that the hospital simply did not have. Explains Bajek, "When ISS offered to manage the firewall around the clock, we jumped at the opportunity to outsource this function because we simply lacked the expertise and time to handle it effectively in-house."

Defending the hospital's network security is an integral part of protecting patient information, employee data, internal communications and other business applications. But as Bajek observes, "You really need 24/7 protection by an army of highly trained engineers with expertise in network security." For most organizations, the cost of acquiring, training and retaining this level of talent is prohibitive, as is the expense to watch the Internet around the clock.

Today, enterprises in the public and private sector alike are locked in a continuing battle with smart and destructive online enemies that can strike at any moment. To address this challenge, organizations are increasingly outsourcing security operations to managed security service providers (MSSPs). For a fixed monthly fee, an organization can purchase the infrastructure, knowledge, resources and on-demand expertise needed to protect its systems from Internet attacks around the clock — all at a fraction of the cost and complexity to build and maintain an in-house capability. As a result, an MSSP consistently and reliably protects enterprise information, while reducing the total cost of ownership and delivering an excellent return on investment (ROI).

"Outsourcing network security monitoring and management to ISS just makes good fiscal sense," says Bajek. "We are saving more than \$100,000 annually just on the costs to hire and train additional people to ensure proper network protection...and those figures don't include the ROI that comes with increased staff productivity. Our ROI would increase dramatically if we could also measure the value of freeing up staff to focus on strategic business initiatives that make our hospital run more efficiently."

Bajek also points out other benefits that are difficult to quantify. "We don't have to devote precious IT resources to reviewing and testing network security configurations, upgrading test environments and hiring and training staff to do all that additional work. I know that saves us time and money." Another benefit of working with ISS that can not be quantified is the peace of mind that Bajek and his team enjoy with a reliable Internet security partner.

KEY ISS BENEFITS:

ISS Managed Security Services provide organizations with an around-the-clock guaranteed level of protection, giving organizations the ability to improve their security posture while allowing them to focus on their core business operations. Benefits include:

- Protection for company assets and business continuity with 24/7 monitoring, management and reliability
- Reduction of in-house security costs by up to 55 percent
- Enhancement of security compliance with industry and governmental regulations
- Solid return on security investments
- Improved productivity by freeing IT resources to focus on strategic initiatives
- Customers, partners and shareholders reassured that critical data is protected by trusted resources
- Peace of mind, with guaranteed protection

"With some companies, the size of the check you write corresponds to the level of service you receive. Here's one that offers a money-back guarantee. We may not be their largest customer, but ISS makes us feel like their most important one."

Joe Bajek
University of Colorado Hospital
Director of IT

 **INTERNET | SECURITY | SYSTEMS®**
Ahead of the threat.

∴ Securing the Gateway and the Network with Managed Security Services

In addition to outstanding customer service and measurable savings, the hospital derives additional added value from its partnership with ISS by providing Bajek and his team early access to new technologies, such as the advanced Proventia™ intrusion prevention appliances.

Proventia is founded on proactive research from the X-Force® security intelligence team. For new hybrid threats like Sasser, MS Blaster and SQL Slammer, firewalls and antivirus are no longer enough to protect the gateway or network. Proventia appliances are designed to combat the wave of hybrid threats on the Internet by offering protection at the gateway, including Internet, branch locations, remote offices, customers, vendors and partners, and within the network, covering servers, users and other networks.

The hospital will soon be implementing the Proventia integrated security appliance, which provides protection at the gateway and at the network level without jeopardizing bandwidth or availability of server resources. Proventia integrated security appliances unify antivirus, firewall, virtual private network (VPN), intrusion detection and prevention, antispam, and Web filtering technologies in a single device. “We couldn't possibly stay on top of the latest developments in Internet security,” says Bajek, “but we know that ISS has the expertise and resources to keep our network protection up to date no matter what new worm or virus is out there.” This exceptional level of service and reliability illustrates how ISS continues to earn the hospital's trust — long after the initial contract with its unique service agreement was inked.

∴ Gaining Peace of Mind Through a Stellar Track Record

With Internet access for approximately 3,500 employees who might unwittingly spread the latest virus or worm and thousands of hackers around the world thinking up new ways to breach security, Joe Bajek could stay awake at night worrying about the safety of his hospital's enterprise information. “What I value most about ISS is that I never worry about my network security and who's monitoring it when I go home at night,” he explained. “That confidence frees me up to focus on the hospital's overall IT risk management strategy and other critically important business initiatives. It also helps me sleep a little more soundly.”

“What I value most about ISS is that I never worry about my network security and who's monitoring it when I go home at night. That confidence frees me up to focus on the hospital's overall IT risk management strategy and other critically important business initiatives. It also helps me sleep a little more soundly.”

Joe Bajek
University of Colorado Hospital
Director of IT