

Leading British Hospital Chooses Promisec to Secure Internal Network

About King's College Hospital

King's College Hospital NHS Foundation Trust is one of London's largest and busiest teaching hospitals, with a unique profile of strong local services and a focused set of tertiary specialties. King's provides a full range of local hospital services for over 700,000 people in the London boroughs of Lambeth and Southwark, and plays a key role in the training and education of medical, nursing and dental students.

Security Issues in the Healthcare Industry

The widespread adoption of electronic patient records and the increased use of mobile devices have revolutionized health services, but also created multiple security risks. According to the Winter 2006 US Healthcare Industry HIPAA Compliance Survey, Healthcare providers that are privacy-compliant have experienced numerous incidents of patient privacy breaches since July 2005. Sixty percent (60%) of compliant healthcare providers indicated that they had experienced privacy breaches between July 2005 and January 2006. Overall data security incidents continue to plague at least one-third of Healthcare providers. It is estimated that for every 1,000 consumer records, a breach of PHI could cost Healthcare providers between \$500,000 and \$1.5 million in notification costs, credit monitoring for breached consumers, fines and penalties, lost consumer confidence and remediation.

The most effective method for organizations to protect themselves from this risk is through the use of agentless technology in conjunction with their existing endpoint security management tools. Promisec's solution provides a set of tools that allows full control of all endpoints within an organization by identifying all of the installed applications, processes, services and devices per workstation and offering remote remediation where necessary. This includes a level of endpoint protection such as prevention of any device that has a memory capacity behind it.

Promisec's solution, provides near real-time, agentless endpoint security monitoring, remediation and management of third-party security applications on internal networks to ensure business continuity, corporate policy compliance and data integrity. The software installs on a single server or workstation for centralized monitoring and management of the entire corporate internal network to ensure enterprise-wide adherence to corporate security policies. Promisec also identifies malware, spyware and

other attacks and intrusions by eliminating snapshot deviations across all endpoint connected systems.

The Challenge

King's College Hospital is one of Britain's largest and busiest teaching hospitals. The hospital needed a solution to secure its internal network of over 3,000 endpoints. The solution needed to be able to identify and fix deviations from its security and usage policy without adversely affecting its network performance. Due to the large number of people using the network, it was difficult to keep track of users' activity and the software and hardware used on their workstations. The solution had to complement the hospital's existing IT infrastructure without involving any major changes to the status quo due to the limited resources available.



The Solution

After reviewing several other endpoint security solutions, King's College Hospital chose Promisec to manage more than 3,000 network endpoints and ensure that internal network compliance initiatives were satisfied.

The hospital chose Promisec due to its agentless approach to detecting potential endpoint weaknesses and ability to remediate identified threats. Promisec's solution is installed on a single server and provides an agentless single point of management for the organization's extensive network of Windows-based computer systems. Promisec's agentless solution helps the hospital to significantly reduce endpoint administrative and security tasks and increase the productivity of IT staff as well as that of its users, while decreasing its exposure to internal threats, both malicious and accidental.

Promisec also enabled a layered approach to internal network security through its centralized third-party management platform to ensure compliance with security policies and software licensing.

The Promisec solution was the ideal choice because of the complete range of threats it addressed, its ease of deployment and simple yet powerful operation.

King's College Hospital has expressed great satisfaction with its new security system.

"Promisec gives us comprehensive visibility into endpoint activity and greater control over our network," said Derek Farlow, ICT Security Manager at King's College Hospital. "Its agentless approach makes deployment quick and easy, and the software's versatility enables us to secure our endpoints simply while enforcing that security across the entire organization from a single point in our network."

Promisec's all-inclusive security solution for the Healthcare industry has become a source of pride for Promisec.

"We are very pleased to be the endpoint security product of choice for King's College Hospital and safeguarding its network with Promisec's highly effective approach to endpoint security management," said Amir Kotler, CEO and Co-founder of Promisec. "By meeting critical requirements with our simple yet powerful solution, Promisec provides institutions such as King's College Hospital with assurance that their IT operations will remain secure under their watch."

Benefits of the Solution

- Detects hidden threats. Promisec identifies threats that have bypassed gateway security systems and embedded themselves in the network - rogue access points, modems or any other peripheral device added to any network endpoint or server, and unauthorized processes or applications. Especially problematic here was the unauthorized use of Instant Messengers.
- Eliminates potential threats. Using remote remediation technology from a centralized management console, Promisec enables administrators in the hospital to automatically kill harmful processes and reverse dangerous registry changes, directly from their own workstation.
- Prevents leaking of confidential information. Promisec prevents the use of mass storage devices or any peripheral I/O device on any endpoint or group of endpoints as well as other mechanisms used to port information out of a network. This effectively stops individuals from illegally copying sensitive company information onto portable devices.
- Monitors for compliance. In today's environment of ever-evolving regulatory standards, Promisec enables organizations to ensure constant compliance according to company policy. If for any reason an endpoint becomes non-compliant, Promisec's solution can return it to a state of compliance using the built in Repair module.

For More Information:

Tel: +1-800-780-0636

Email: inquiry@promisec.com

Internet: www.promisec.com

About Promisec®

By providing unique agentless solutions that deliver unprecedented visibility, Promisec guarantees 100% accuracy for the IT business deliverables of service management, compliance, and power management. Using patented agentless technology, Promisec does more than monitor and manage endpoints. Promisec proactively analyzes and fixes IT endpoint issues, particularly those associated with Microsoft infrastructure. Promisec resolves endpoint problems with fast, right-click or self-healing remediation in a matter of minutes with minimal, if any impact on the network or endpoints.

Promisec optimizes IT operational efficiency by lowering cost and increasing accountability. By proactively overseeing everything installed and not installed on the endpoints, Promisec empowers a higher level of accountability by enabling existing IT management and security solutions to actually work as promised. Promisec is a privately held company with headquarters in Israel and offices in New York, India, and Paris. Our customers include Forbes Global 2000 companies and other organizations in the manufacturing and service industries as well as government and health care institutions.