totalsecurity™

Check Point®
SOFTWARE TECHNOLOGIES LTD.

"The granular control of Endpoint Security's port protection function enables us to keep information flow fully traceable and secure, while allowing users to work efficiently."

Adam Ataar
Network Security & Operations Consultant
NHS Blood and Transplant

CUSTOMER NAME
NHS Blood and Transplant

INDUSTRY
Healthcare

CHECK POINT PRODUCTS
- Check Point Endpoint Security™

CUSTOMER NEEDS MET
- Confidential data secured on all laptops, PCs and USB devices against malware, theft and data loss ensures compliance with latest UK Government directives
- Enables secure remote access to corporate networks for employees
- Delivers security automatically, and transparently to the end user
- Quick and easy centralized deployment, plus ease of administration and management has reduced burden on IT support staff

NHS Blood and Transplant

www.nhsbt.nhs.uk

NHS Blood and Transplant Deploys Check Point Endpoint Security for Total Protection of Sensitive Information

ABOUT NHS BLOOD AND TRANSPLANT

NHS Blood and Transplant, an integral part of the National Health Service (NHS), is an organization, which collects, processes, stores and issues approximately 2.1 million blood donations per year from its 15 blood centres in England and North Wales.

In addition to dealing with blood donations, NHS Blood and Transplant conducts new research into improving the safety of blood and blood products, and the ways they can be used to help save lives.

Storing confidential personal data as well as sensitive research data means it is imperative the organization has a fail-safe data security solution in place.

THE CHALLENGE

As an existing Check Point customer, NHS Blood and Transplant already had a robust laptop and PC security solution in place. However they needed to enhance protection for sensitive data on its PCs to comply with the latest UK Government's directives on data security in the public sector.

Adam Ataar, Network Security & Operations Consultant NHS Blood and Transplant said: "Our laptop and PC security was already strong, as we used Check Point's Integrity 6.5 solution for firewalling, intrusion prevention and endpoint policy compliance. However, we needed to deploy full disk encryption and port protection functions to further enhance security. And with 900 laptops and 500 desktop PCs across the UK, the solution had to be easy to manage, without adding complexity for users or the IT team."

THE CHECK POINT SOLUTION

Following an evaluation of solutions from several vendors, NHS Blood and Transplant chose to deploy Check Point Endpoint Security™.

Check Point Endpoint Security is the first single agent for total endpoint security that combines the highest-rated firewall, network access control, program control, antivirus, anti-spyware, data security and remote access.

Designed to protect company laptops and PCs against malware, data loss, and other threats while enabling secure remote access to the corporate network, the solution was chosen for its ability to deliver comprehensive security in a single software agent that is easily deployed and managed from a single console.

THE BENEFITS OF CHECK POINT ENDPOINT SECURITY

Check Point Endpoint Security has enabled NHS Blood and Transplant to further protect the data on its fleet of laptops, desktop PCs and USB storage devices against malware, data loss and theft.

Check Point's full-disk encryption feature means NHS Blood and Transplant employees don't have to make any decisions about what data needs protecting. Adam Ataar said: "Users shouldn't be given the responsibility for deciding what should and should not be encrypted, or to maintain security policies. These policies have to be enforced by solutions, as transparently as possible from the user's viewpoint. That's exactly what the Check Point solution does."

Endpoint Security also gives full control over data written to USB devices and removable media, as well as controlling which types of removable storage devices can be used on the organizations network.

"We use the granular control of Endpoint Security's port protection function. Each member of staff is given their own fully-encrypted 2GB USB drive, and use of all other removable media is blocked. This enables us to keep information flow fully traceable and secure, while enabling users to work efficiently," continued Ataar.

Ataar reports that both deployment and ongoing management have been seamless and easy for users and the IT team. Additionally, by reporting on the security status of each laptop and PC, Check Point Endpoint Security also allows any required upgrades or policy issues to be identified and addressed directly by administrators from the central management console.

Another key issue for NHS Blood and Transplant is to protect documents and emails that users are working on when away from the office, without compromising security or usability.

Check Point Endpoint Security is unique in that it includes both data security for preventing data loss and theft and a VPN client which provides secure remote access for employees working offsite. This delivers greater flexibility to the organization by allowing employees to work securely online when out of the office; ensuring sensitive data continues to be protected.

LOOKING TO THE FUTURE

In the future, NHS Blood and Transplant plans to migrate its secure remote access to the VPN functionality in Check Point Endpoint Security, from the Citrix Access Gateway solution it currently uses. Adam Ataar says this will further simplify security management and deliver long-term savings.

CONTACT CHECK POINT

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
800 Bridge Parkway, Redwood City, CA 94065 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com

HTNRHNNO