# CASE STUDY: LEADING MNC PHYSICAL SECURITY PROVIDER

## 1 BUSINESS CHALLENGE

- Securing sensitive corporate information
- Ensure productive use of internet and computer facilities
- Monitoring mobile users having laptops

As a leading physical security provider for various banks and corporations and also dealing in moving high valued items, securing details of their clients or payloads is extremely important to their business. In order to secure their data they implemented **Bluecoat** to block majority of the internet websites and **Kaspersky antivirus** however they faced a constant threat of people finding ways to bypass them. Further they had a constant threat of leaked information via online media or via thumb drives and their tests showed Bluecoat and Kaspersky had no way of detecting this.

In order to counter this they implemented a strict routine of conducting PC audits and spot checks but unfortunately the Auditors didn't have any logs to check of what people have talked about or typed on some website or which files have been copied on the thumb drive.

## 2 E-SAFE COMPLIANCE SOLUTION

The company evaluated e-Safe Compliance and found it to be best fit for their varying range of requirements. e-Safe Compliance helped to solve their issues in the following ways:

1. With e-Safe Compliance they were able to monitor communication and documents not only in desktop machines but on laptops. Hence even if the laptops were no longer in the office premises e-Safe Compliance was still able to monitor and report on any infringements.
2. e-Safe Compliance provided complete audit trail in the event unauthorized information was being discussed over any online source or copied into thumb drives
3. With e-Safe Compliance the Auditors now had an automated mechanism which performed continuous audit and reported on possible violations. The Auditors only need to verify the violation using the reports and as such eliminated the need for spot checks and routine PC audits.
4. Using application usage report the IT personal were able to detect a small proxy client being widely used by people to bypass Bluecoat blocking. This application was blocked using e-Safe Compliance. Further as e-Safe Compliance is not effected by proxy sites or clients it served as the perfect deterrent as people knew their internet usage will be tracked.

5. Using e-Safe Compliance Software Audit they were able to detect which machines were having unauthorized applications installed and could now block them from running using e-Safe Compliance's application blocking features.
6. With e-Safe Compliance's advance porn detection technology the IT personnel now had clear track of staff who were responsible for storing and accessing pornographic material whether in their machines or on the server shared drives
7. Using drive Audit the auditors were now also able to control the amount of personal videos, images and audio files being stored by people on servers and on their company PCs.
8. With e-Safe Compliance they didn't have to worry whether people connect using the corporate network or non-corporate network sources such as 3G modems, external Wifi networks etc as they were constantly being monitored
9. e-Safe Compliance provided the company an alternate approach to excessive blocking. It helped the company in analyzing their internet utilization. Majority of their internet usage was found to be unproductive in nature. Using bluecoat they could only know the number of hits however had no idea about the amount of time spent on these websites. Previously they had employed the strategy of blocking most of the unproductive sites using the internet cache, however this policy was not popular among their staff who wanted more freedom if they could get their work done. With e-Safe Compliance they now had the ability to let the users decide the appropriate usage of unproductive sites such as Facebook etc as long as their managers were happy with their performance.