



## **Monitoring and Enforcing Secure User Behavior with BSMS** **Sample threat scenarios countered**

**Scenario 1:** Internal and outsourced IT administrators have unlimited access to corporate data including the CEO's desktop or mailbox.

*Impact:* Access can lead to data leakage of proposal, merger information and more.

*Solution:* With BSMS agents running on the desktops and servers, audit trails of activity are available.

**Scenario 2:** An employee copies work related information to a storage devices like a USB thumbdrive and loses it on the way to lunch.

*Impact:* Unencrypted files on USB files can lead to accidental data loss. Anyone who gets hold of the USB stick can look at the files.

*Solution:* BSMS policies can be configured to restrict copying or enforce encryption while copying to USB storage devices for all or a specific group of employees.

**Scenario 3:** An employee who is about to resign backs up all his/her work to a thumb drive or portable disk drive.

*Impact:* The data could be valuable Intellectual Property which if taken to a competitor could mean loss of business for you.

*Solution:* BSMS policies can be configured to block file manipulation activity at a destination where confidential documents are stored. These documents cannot be copied, emailed, printed, uploaded or altered.

**Scenario 4:** A "half-techie" employee changes the registry or stops a service like the antivirus agent.

*Impact:* Corruption or malfunction of the computer. Support engineers could take hours or days fixing the corrupted computer thus losing productive hours for the individual.

*Solution:* BSMS can alert the admin team while the changes are being carried out by the employee. BSMS can be configured to automatically start essential services every time they are shutdown by the user.

**Scenario 5:** An employee sends an email with sensitive content. Example: A list containing customer names, phone numbers, social security numbers and credit card numbers.

*Impact:* Legal penalties, fines or payout in damages and lawsuits.

*Solution:* BSMS's advanced content analysis capabilities can detect sensitive content within the email body or attachment. BSMS's policies can be configured to warn users of violations or block emails with such content.

**Scenario 6:** An IT employee with administrative privileges downloads a pirated movie or software.

*Impact:* Legal penalties, fines and possible corporate image damage.

*Solution:* The BSMS administrator can be alerted when a download occurs and the policy can be set to prevent an installation from happening.

**Scenario 7:** An employee prints documents containing confidential information and leaves the document on the printer.

*Impact:* Prints could be viewed by anyone and compromise the confidentiality of information.

*Solution:* BSMS can alert or block printing of sensitive documents.

**Scenario 8:** An employee changes the proxy settings to bypass restrictions on browsing the internet.

*Impact:* Misuse of the internet can reduce user productivity, violate company policy, and cause bandwidth issues.

*Solution:* BSMS can lock the proxy setting screen to changes.

**Scenario 9:** Senior members of the management send emails unencrypted.

*Impact:* The emails containing sensitive content can be intercepted and read by unauthorized personnel, leading to misuse of confidential information.

*Solution:* BSMS can enforce email encryption.

**Scenario 10:** An employee plays games during business hours.

*Impact:* Company resources and productive time is wasted.

*Solution:* BSMS can block applications as well as alert an administrator when these applications are used.

**Scenario 11:** An employee violates company policy that only authorized USB devices are accessed by using an iPod or PDA.

*Impact:* Large unauthorized removable storage devices can be used to steal confidential data.

*Solution:* BSMS policies can be written to allow only authorized USB devices.

**Scenario 12:** A malicious or disgruntled employee steals corporate data like customer lists, credit card numbers or other Intellectual Property.

*Impact:* Legal penalties, fines and possible corporate image damage.

*Solution:* Using BSMS's Protected Document Path, User actions such as; copy/move, print, file upload, email, and copy & paste, can be prevented. BSMS's Spider can also scan locations for sensitive content and encrypt found sensitive data if necessary.

**Scenario 13:** While you invest heavily into securing your applications with access control or identity management software, you are concerned about ethical use of provided access or users copy/pasting sensitive data from your secure applications.

*Impact:* Employees who have access to confidential data may use it unethically leading to loss of business or legal /financial penalties.

*Solution:* BSMS policies can be configured to block unauthorized clipboard actions on a specified list of applications. BSMS's user behavior analytics can be used to notify of suspicious user activity.

**Scenario 14:** You suspect an employee of treason, but do not have enough evidence to fire the employee or even confirm the suspicion.

*Impact:* Information leaks can continue with further losses and in the absence of immediate and strict disciplinary action your corporate policy weakens.

*Solution:* BSMS's user behavior analytics can be used as forensic evidence to confirm the suspicion or legal documentation.

**Scenario 15:** An employee sends (uploads) confidential documents using his/her personal email address.

*Impact:* Violating company email policies can lead to the loss of confidential data and by-passing corporate email systems.

*Solution:* BSMS policies can be configured to track or block file uploads to personal email websites.

**Scenario 16:** A malicious laptop user saves confidential data on a laptop and transfers it to a computer at home.

*Impact:* Legal penalties, fines and possible corporate image damage.

*Solution:* BSMS agents execute in stealth mode, therefore a user cannot stop the process. The agent also enforces policies off the company network.

**Scenario 17:** A music and movie enthusiast is issued a laptop for travel. The user creates a music repository on his laptop at home. The file extensions are changed and transferred to your file server before returning the laptop. Every time the user and his friends want to play music or watch movies they connect to the central repository, (your fileserver) and change the file extensions. Ever wonder why you cannot find these files and where they came from?

*Impact:* Pirated movie, music and software can lead to legal and financial penalties. Storing these files on your file server, decrease available space, increase your backup requirements, cost and IT overheads.

*Solution:* BSMS policies are enforced even on offline laptops. Which means the users cannot copy or download music to laptops from CD or USB devices or internet. BSMS application policies can be configured to block media

players. You can further configure BSMS policies to block software installations or application runs from all forms of storage devices or internet.