



BackStopp

Backstopp is a simple but effective tool to help an organisation protect its mobile data in the event of the loss or theft of a laptop, PDA or other mobile computer.

Developed by Virtuuity Ltd



BACKGROUND

The series of recent stories in the media regarding the loss or theft of laptops from prominent organisations, both public and private has highlighted the growing understanding of the value of data and the dangers of it falling into the wrong hands.

Following the theft of a laptop from the home of an employee of the Nationwide Building Society in 2007 the FSA issued a fine of nearly £1m. The CEO at the time was forced to issue a statement of ignorance and the negative publicity resulted in a rash of closed accounts.

This ignorance inspired Virtuuity to develop Backstopp. Backstopp uses the fastest methods available to pinpoint a lost or stolen laptop and securely delete the data before it has been compromised.

Using similar principles to Vehicle Telematics it allows an operator to receive information about the lost or stolen device and report on its status accurately, removing ignorance from a critical situation and ensuring the losing organisation appears to have covered all eventualities and to be strong in difficult circumstances.

INTRODUCTION

For the first time laptop sales outstripped those of desktops in 2007 and the trend seems likely to continue as the size, weight and most importantly the price of laptops fall while their power increases.

Mobile phone companies are spearheading a mobile broadband revolution with cheap data packages allowing access to the web almost anywhere on Earth. Fierce competition has led to some subsidising the value of the laptop.

Organisations are increasingly aware of the importance of data and the damage it can cause when in the wrong hands. They are also accepting that what might previously have been considered unimportant could well be interesting to competitors and data thieves alike. Now ALL data are potentially sensitive and worth protecting. Government organisations are becoming increasingly punitive towards organisations that are not seen to have done enough to protect their data.

As such they are adopting new and ever more sophisticated methods of securing data on mobile devices, such as data encryption and biometrics as well as firming up internal data security policies. All of these have their merits but often fail because of the need for human intervention and, however hard they claim it to be to access protected data the reality remains that the device still has data on board.

BackStopp's philosophy is that protected data is good, NO data is better and the ability to be able to prove it is best. In that, speed is all important. BackStopp quickly locates the device and securely deletes the data.

It then provides a comprehensive report that allows an organisation to effectively manage a critical situation internally and externally.



SENSITIVE DATA

Data Security Framework guidelines recommend that all data be held on a secured central server. These data are then accessed and manipulated locally or remotely using the particular communications mechanisms favoured by individual organisations. However, for any number of reasons data are stored on mobile devices.

Mobile workers create and receive information whilst away from the office and much of this is stored either deliberately or automatically on the disk. If the device is lost or stolen it raises a host of potential issues from embarrassment to the organisation, negative publicity and even official censure.

Even using web based applications is not failsafe. Tools such as online CRMs and e-mail remove the need for data to be stored on a local disk but cookies, which most users keep for convenience, could easily provide a route to customer/prospect details which could be very useful to a competitor.

Backstopp assumes that all data could be deemed to be sensitive so leaves nothing to chance.

SENSITIVE DEVICES

Many organisations feel that data on certain devices warrant additional protection due to the seniority of the user and therefore the sensitivity or value of the data. BackStopp provides functionality that allows an organisation to quickly and efficiently identify and protect the relevant individual's device.

It does this using vITILhub, a flexible Management Information Tool developed by Virtuity using predominantly visual Key Performance Indicators to deliver the information. These KPIs allow an organisation to make reasoned decisions on the structure of the roll out to the user community.

The screenshot displays the BackStopp web interface. On the left, there is a 'Device Details' form for a device named 'PIKEVIRTU'. The form includes fields for Device Tag, Owner (Kevin Pike), Owner Email (kevin.pike@virtuity.co.uk), Department (Design), GSM Number (004479123456789), Device type (Windows Laptop / Desktop), Asset Number (D8301840869), Data Severity (High), and Location (SW1 London). At the bottom of the form are 'Cancel', 'Delete', and 'Save' buttons. On the right, a pie chart titled 'Device data severity' shows a red slice representing 'High' severity at 14.3% (2 devices). A tooltip points to this slice with the text 'Data severity'. The interface also shows navigation links like 'Event Log / Client Kit / Settings / Logout' and a '+]' button.



DATA DECOMMISSION

Remote Data Decommission is BackStopp’s primary function. BackStopp deletes all pre-specified data files including cookies and e-mail that are stored on a compromised device. Whether the theft of the device was opportunistic or targeted by identity theft professionals BackStopp deletes the data, encrypted or not, leaving a clean device.

BackStopp ensures that once the data has been deleted it is gone for good. It uses deletion patterns as detailed in the US Department of Defence’s *National Industrial Security Program Operating Manual* (US DoD 5220-22.M) and Peter Gutmann's paper *Secure Deletion of Data from Magnetic and Solid-State Memory*, ensuring decommission data can not be retrieved. Should an organisation wish to implement its own patterns BackStopp will endeavour to accommodate them.

NOTIFICATION

The Decommission of data on a laptop relies on the compromised device being contacted and the decommission executable triggered. This can happen automatically, according to pre-set parameters or manually.

MANUAL NOTIFICATION

In most instances the owner/user will notify a BackStopp operator, either within his/her own organisation or at a managed service provider that the device is missing. The operator will then identify the particular device from a list of protected devices and initiate the decommission. This decommission is flexible in that the operator needs only a web browser to be able to perform the decommission. This means that the operator could be anywhere in the world where a web browser can be accessed.



Site \Virtuity Demo Site [\[change\]](#)

[Event Log](#) / [Client Kit](#) / [Settings](#) / [Logout](#)

Protected Devices \ [Decommission In-progress](#) \ [Decommission Reports](#)

Owner	Name	Asset Number	Department	Data Level	
Anthony Wong	VIRTWONG	I9878811234	Design	High	Details Decommission
Dean Cundey	DEANLAPTOP	D2504198027	Design	Normal	Details Decommission
Eileen Omaye	LAPTOP8372	T6782300123	Sales	High	Details Decommission
Julie Moskowitz	NEWLAP234	A2344940241	Accounts	Normal	Details Decommission
Kate Barker	BARKER223	S2336499311	Sales	High	Details Decommission



AUTOMATIC NOTIFICATION

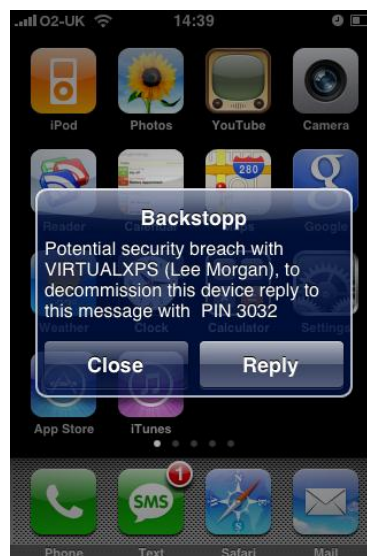
Where BackStopp forms part of a more complex data protection strategy the notification can be automated and the data deleted with no human intervention. Examples of this might be where an organisation covers its laptops with an in-premises RFID or Wireless Locator. In the event that the laptop breaches pre-defined security parameters the instruction to delete can be sent automatically.

RFID or wireless readers detect unauthorised movements



As soon as a laptop moves outside of its authorised area Backstopp takes a proactive role. It can notify security, perhaps giving them time to intercept the device before it is lost. It can also notify the official user by SMS. If he/she has the device then the SMS can be ignored and nothing will happen. If the alert brings the theft to their attention then simply replying to the SMS will trigger the decommission. Or simply if the device moves into an unauthorised area the command can be to delete the device with no alerts.

Authorised user receives a text message alerting him/her to potential device loss





Device Vacation

When a user knows of a period of time when the device will not be used, for example when he/she is to be on holiday a date and time range can be entered into the laptop. If Backstopp detects the device during this time it can work proactively as above. An alert can be sent in case whoever using it is legitimate. If the real user believes not then the same SMS reply will trigger the decommission. If the user is convinced that the device has no reason to be turned on during the device vacation then the parameter can be to simply delete the data with no alerts.

A screenshot of a software dialog box titled "Device holiday". The dialog has a blue title bar with a close button (X) in the top right corner. The main area is light beige. It contains the following elements:

- Text: "Device will be turned off from..."
- Input fields: A date field showing "15 September 2008" and a time field showing "09:00:00".
- Text: ".. to .."
- Input fields: A date field showing "15 September 2008" and a time field showing "17:30:00".
- Alert box: A rounded rectangle containing the text "Alert me if this device is turned on between 15/09/2008 09:00:00 and 15/09/2008 17:30:00".
- Text: "Call your data protection operator to cancel a device holiday."
- Button: A "Close" button in the bottom right corner.



THE VIRTUITY DATA CHAIN

BackStopp is a phenomenally powerful standalone tool that provides an unparalleled layer of security for data resident on laptops wherever they are in the world. As long as there is a mobile phone signal or an internet connection BackStopp can destroy any data on a laptop in as short a time as is physically possible, making it as difficult as possible for the data to fall into the wrong hands.

This is however just part of the data chain that is secured by Virtuuity coming in the middle of the three links that Backstopp covers.

The first link is in-premises protection, through either RFID for any device or Wireless Infrastructure for intelligent devices as described above.

The middle link is Backstopp itself.

The final link in the chain is Business Continuity. Virtuuity has linked Backstopp to best of breed products that provide bare metal rebuild in the shortest time possible and the most advanced mobile data backup and restore tool that can work through the GSM infrastructure and therefore allow a device to be backed up on a regular basis, anywhere in the world, as long as there is a mobile phone signal.

If a device is lost Backstopp deletes the data, provides the report and the reassurance that this brings and disables the Operating System. With Virtuuity's tools an organisation can then purchase and commission a new device with the corporate image and conceivably upload the exact same data that was on the lost device just before it was lost. This could take as little as a couple of hours so, with worldwide next day delivery companies of today, the user could be provided with an exact replica laptop anywhere in the world in less than 48 hours.



CULPRIT IDENTIFICATION

Many Laptop manufactures now fit a discreet button webcam to the lid of their laptops. BackStopp provides the facility to remotely enable this camera when the device has been lost or stolen. Any images taken by the camera are automatically transmitted back to the BackStopp console and included in the Decommission Report.



Images are transmitted over the GSM network but require a data contract with the network operator (certain airtime providers have zero cost contracts). A data contract isn't required to perform data decommissions or locating. A 'pay as you go' SIM card would allow the device to be identified and the data deleted. The BackStopp console provides an intuitive interface for viewing images captured on the mobile device. These images can be exported as regular image files which may be used in police investigations.

DECOMMISSION REPORT

Device Name	SAMPLE	Lost	29/01/2008 12:29:54
Data Severity	High	Sent	29/01/2008 16:32:19
Owner	Dean Bates	Completed	29/01/2008 17:35:24
Department	Sales	Submitted By	Paul Taylor
GSM Number	00447712345678	Authorised By	Mark Evans
Last known Location	Star Coffee, Albion Street, London	Asset Number	JK123456789
Decommission File Pattern	.doc; .xls; .ppt; .txt; .docx; .xlsx; .pptx; .one; .mdb; .pst;	Reason	Lost, presumed stolen, from london coffee shop

Photo captured 29/01/2008 17:35:24



Location Star Coffee, Albion Street, London

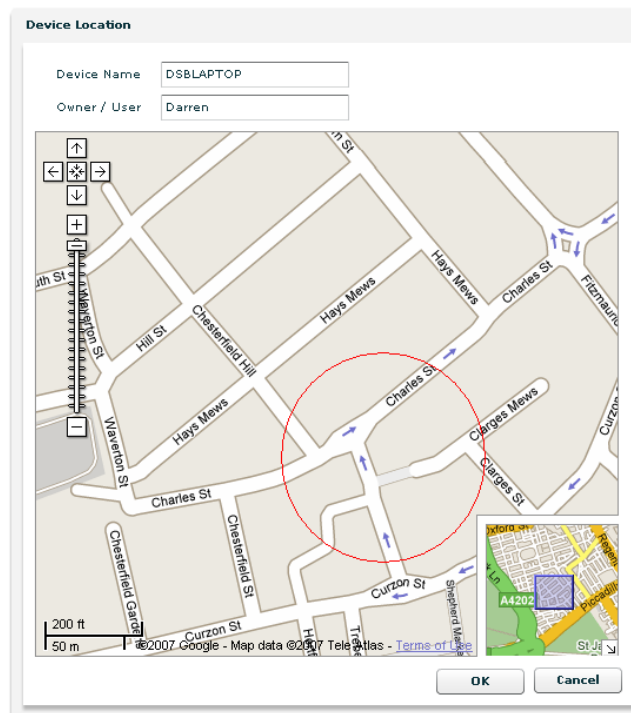




LOCATION

Devices may be located if believed to be stolen or simply for general audit. BackStopp uses data from GSM operators to locate and track the location of mobile devices.

The location accuracy is dependent on the cell mast density in the vicinity of the device. New GSM device location technology will be incorporated into Backstopp as it comes online.



GPS, IP GEOGRAPHY AND RFID

GSM locating offers the greatest overall coverage when compared to other location technologies. GPS supplies greater accuracy but requires hardware not standard in today's laptop configurations and devices often can not be located indoors. IP Geography has high availability but requires an internet/WiFi connection and lacks accuracy outside of the US. In addition, should the laptop remain unconnected to the internet for any length of time the likelihood that the data is compromised increases. BackStopp uses GSM locating as default but will integrate with GPS, IP Geography, Wireless and RFID solutions if required.

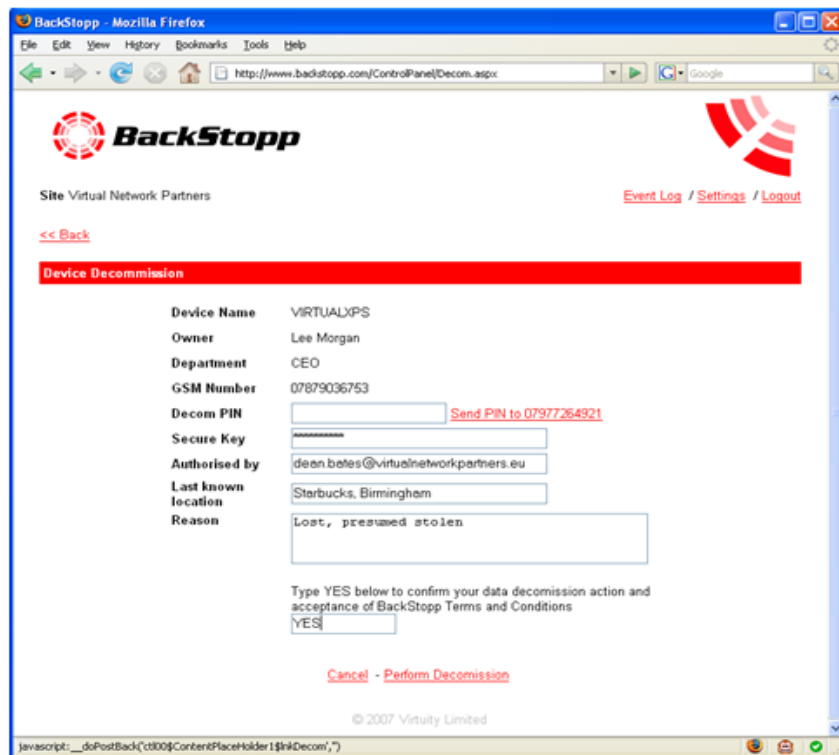


TECHNOLOGY

CORE COMPONENTS, TRANSPORT

BackStopp consists of two core components, a rich internet application console and a lightweight client. BackStopp is unique in that its primary message communications method is the GSM network. An internet/WiFi connection is NOT required.

The client runs as an operating system service and becomes active as soon as the operating system is booted. The client doesn't require the user to be logged in or connected to a LAN, internet or WiFi network. BackStopp uses the mobile GSM network which provides 99.7% coverage in the UK and similar coverage statistics in the developed world. BackStopp messages remain in the GSM cloud until an acknowledgement is received ensuring no instructions are lost if the device is out of coverage or turned off at the time of transmission. Future generations of in-built GSM laptops may provide permanent power to the GSM card so Backstopp would be able to power the device on and delete the data.



Data Decommission messages contain a secure key. The secure key is entered at the console whenever a decommission instruction is transmitted. The decommission instruction is only performed if the transmitted secure key matches a twin key embedded in the client. The security key is encrypted before transmission and at the client.



DECOMMISSION REPORT

For BackStopp the only thing as important as deleting data on a laptop before it falls into the wrong hands is the ability to reassure interested parties such as customers, stakeholders etc. that the data is safe. As soon as a decommission is completed a comprehensive report provides an organisation with the following information.

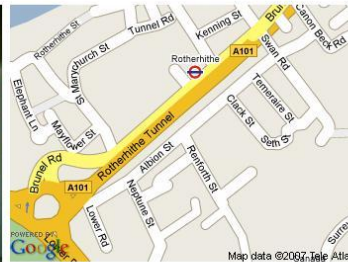
- Device Details e.g. Asset Number/Owner//User/Department/Data Severity
- Date and time of device loss and its last known location.
- Date and time of and reason for decommission
- Authorised BackStopp operator details
- Full file inventory including deletion details
- File last accessed date and time with active cross reference to date/time of loss
- List of compromised files (if any)
- Last backup date (optionally provided via integration with backup tool)
- Building exit point (optionally provided via RFID or Wi/Fi system)

DECOMMISSION REPORT

Device Name	SAMPLE	Lost	29/01/2008 12:29:54
Data Severity	High	Sent	29/01/2008 16:32:19
Owner	Dean Bates	Completed	29/01/2008 17:35:24
Department	Sales	Submitted By	Paul Taylor
GSM Number	00447712345678	Authorised By	Mark Evans
Last known Location	Star Coffee, Albion Street, London	Asset Number	JK123456789
Decommission File Pattern	.doc; .xls; .ppt; .txt; .docx; .xlsx; .pptx; .one; .mdb; .pst;	Reason	Lost, presumed stolen, from london coffee shop

Photo captured 29/01/2008 17:35:24

Location Star Coffee, Albion Street, London



File Types

File type	Number of files	Unauthorised Accesses	Total size
Microsoft Word	4	2	7.12 MB
Microsoft Outlook	1	0	431.2 MB
Microsoft Excel	4	0	7.22 MB
Internet Explorer Cookie	3	0	455 Bytes

Decommissioned Files

File	Last Accessed
C:\Documents and Settings\User\BluePrints.docx	29/01/2008 15:16:31
C:\Documents and Settings\User\MeetingActions.docx	29/01/2008 15:20:06
C:\Documents and Settings\User\CompanyBudget.xlsx	19/01/2008 04:33:12
C:\Documents and Settings\User\Cookies\user@google.co.uk.txt	12/01/2008 16:22:59

Armed with the report a CEO or other spokesman can confirm with confidence when the device was lost, when and where it was located, what data was deleted and what data was accessed if any between the time of its loss and the decommission being completed. A previously negative situation becomes positive and confidence is restored.



CONCLUSION

BackStopp is a highly sophisticated data protection application which provides remote data decommission, location and culprit identification functionality against compromised mobile devices. BackStopp is the integral part of a three link solution that covers in premises laptop protection through to Business Continuity and Productivity Enhancement, though it can be used as a stand alone tool for mobile devices only.

BENEFITS

- ✓ Uses US Department of Defence standards to destroy data
- ✓ Always on client, not just boot, so works every time
- ✓ Uses GSM network, not reliant on internet / WiFi connections
- ✓ Can be retro fitted to existing devices, so no need for early redundancy
- ✓ Culprit Identification capability
- ✓ GSM Device Location
- ✓ Comprehensive Audit Trail for real Peace of Mind
- ✓ Proactive seek and destroy functionality
- ✓ Rich Internet Application console
- ✓ Part of "best practice" Data security framework



APPENDIX

BackStopp - A highly sophisticated data protection application.

vITILhub - a Rich Internet Application that provides a **real time** set of **Key Performance Indicators** that highlight exceptions to an organisation's established rules and standards.

Unsecured Data - A data file of any type (Word, Excel, cookies etc) stored on a client device.

GSM - The Global System for Mobile communications is the most popular standard for mobile phones in the world. GSM service is used by over 2 billion people across more than 212 countries and territories.

RFID - Radio-frequency identification is an automatic identification method, relying on storing and remotely retrieving data using devices called RFID tags or transponders.

DoD 5220.22-M - The NISP Operating Manual, also called NISPOM, or DoD 5220.22-M [3]. The NISPOM establishes the standard procedures and requirements for all government contractors, with regards to classified information.