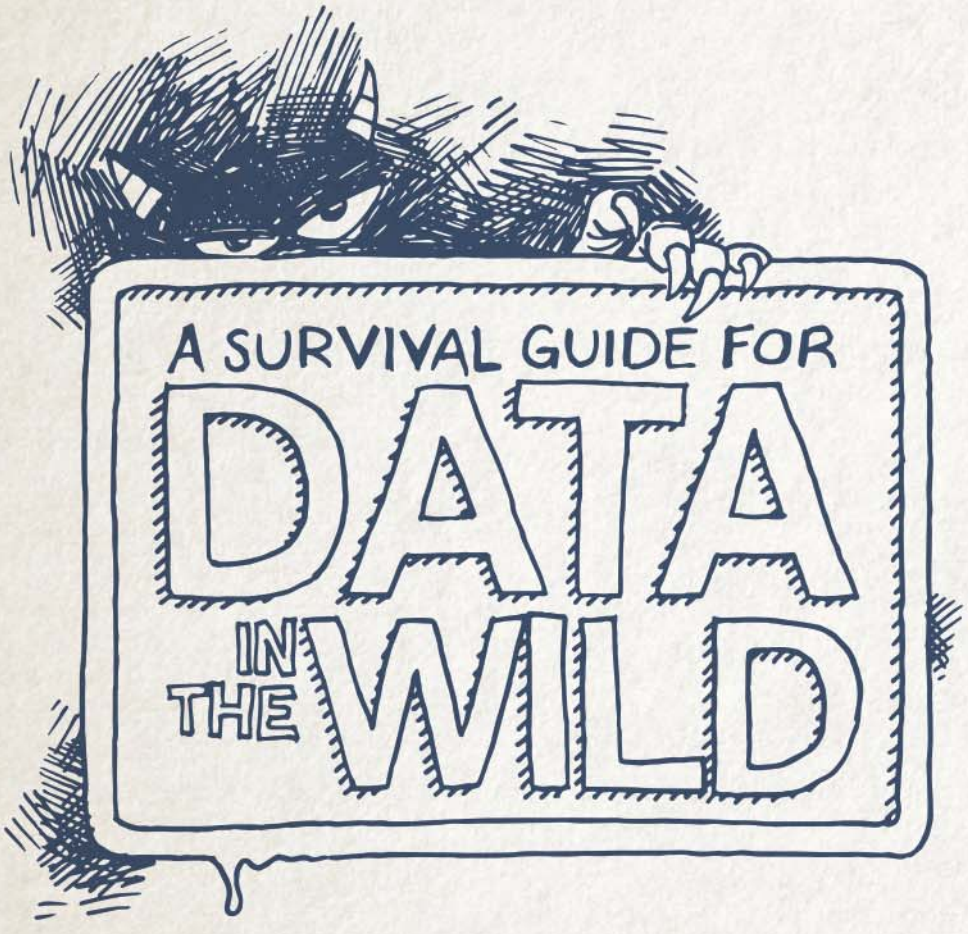
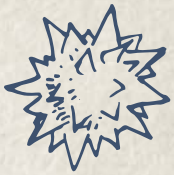


druva



What's Wild Within

A Survival Guide for Defending Data in the Wild

It's a wild world outside the corporate firewall.

Protecting data for your entire company is a heavy responsibility. There's the employee who leaves his laptop in the airport. And the former employee who still has access to corporate data from her personal device. Or the ever-present danger of litigation. You're accountable for a wide range of scenarios that put your corporate data at risk.

Fortunately, you don't have to go it alone. Learn from the experience of others to ensure that you're prepared for every threat to your corporate data in the wild. With step-by-step instructions, this Survival Guide is your most valuable tool for keeping corporate assets out of harm's way.

CHAPTER ONE

The Threat: Data Sprawl

Capturing data and maintaining visibility into how it changes

14 months from now, there will be twice as much data in your organization as there is now.

Corporate users generate more data than ever before. Emails, documents, spreadsheets, presentations and more. Each file is typically replicated countless times as users collaborate and store data on multiple devices. With an average of 3.3 connected devices per employee, data resides on laptops, smartphones, and tablets with different operating systems. Sometimes, they're users' personal devices.

Do you know, with total certainty, what data is being created, where it's located, or how it's being accessed and shared? Honestly? To gain full visibility into how endpoint corporate data is moving and being used in your enterprise, you need a way to centrally capture it. Quickly and frequently. Wherever users are working.

How to Capture Endpoint Data and Achieve Full Visibility

In addition to their company-issued laptops, your company's executives also use tablets and smartphones while on-the-go. Working from conference centers, hotels, airports, client sites, and more places in the wild, users connect to networks which are frequently weak and unpredictable. Despite all of these variables, you can defend their data with the right tool.

1 Capture data from all devices

Capture data from heterogeneous devices. To gain visibility into users' activity on all of their devices, you need to capture data from all of those devices — regardless of manufacturer or operating system.

Containerize and capture data on BYOD devices. Personal device use presents unique challenges due to the intermixing of personal and work data. By containerizing corporate data and capturing changes from personal devices, you can see what, how, and when changes happen without affecting end user privacy.

2 Frequently capture changes to data

Speed up data capture processes. To provide visibility into minute-by-minute changes, data capture must be persistent and fast. About 80% of data is duplicated. Deduplicating data globally across all enterprise devices avoids inefficient transfer of the same data over and over.

Reduce the impact of data capture on users. If frequent data capture interrupts users, they may try to disable capture processes. WAN optimization automatically detects network changes and adjusts bandwidth usage accordingly. So, data transfers happen seamlessly and without disruption.

Make sure data capture completes successfully. When users go mobile, you can't guarantee that data capture will fully complete before they disconnect from their current network. With auto-resume functionality, data capture will pick up where it left off as soon as a new connection is detected.

3 View all data activity

Gain insight into all data on endpoints. By frequently capturing data, you can see what data is created, how users are accessing it, and where it's located.

See how data is moving. Know exactly how users are duplicating, downloading, and restoring data across all their devices with minute-by-minute data capture. A detailed log of changes provides you a complete picture of data usage.

See how data is shared. By capturing how data is being shared, you can gain visibility into which files have been shared with internal and external users, who those users are, how many times the file has been downloaded, and whether external collaborators still have access. Granular visibility like this lets you control access or provide information during eDiscovery.

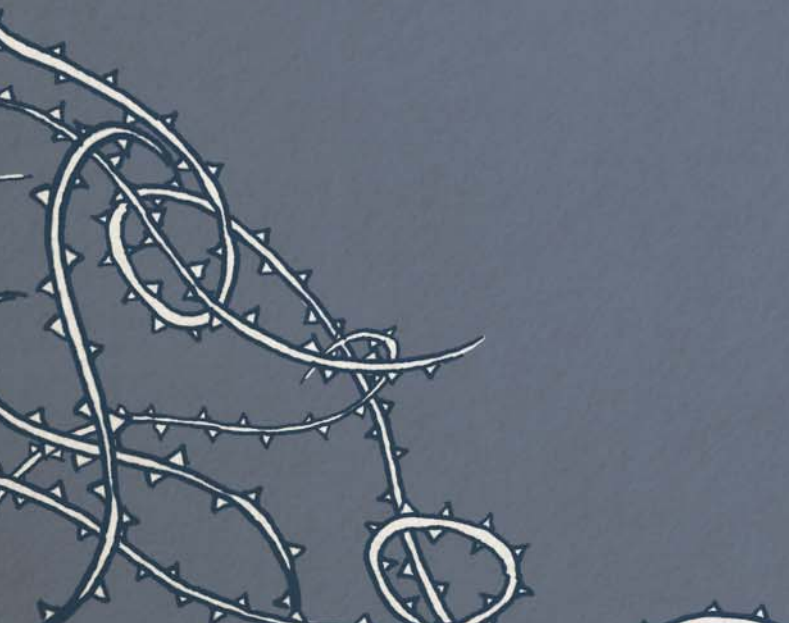
57% of the global workforce works from multiple locations in a given work week.

— Forrester Research, "Backup for Today's Mobile Enterprise," 2013

Devices Used for Work

63% MS Windows and Phone
12% Apple OS X and iOS
7% Google Android
5% RIM Blackberry
13% Other/Unknown

— Forrester Research, "Redefine Your Workforce Computing Policy To Empower Employees," 2012



CHAPTER TWO

The Threat: Wrong Data in the Wrong Hands

Controlling access and sharing

Controlling how your users create, access, and share data is essential.

With the proliferation of data and devices, it's all too easy for data to fall into the wrong hands. You need the ability to control who can do what and when.

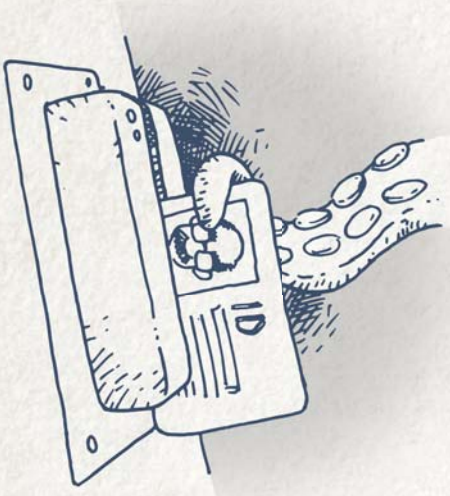
Data defense might combat malicious activity by a former employee that puts thousands of dollars' worth of research data at risk. But, 36% of data breaches are the result of inadvertent misuse. So you also need the ability to prevent damage from innocent mistakes by authorized users, such as sharing the wrong file or accidentally emailing a file to the wrong recipient.

25% of data breaches are the result of abuse by malicious insiders

— Forrester, "Understand the State of Data Security and Privacy, 2013-2014," 2014

How to Prevent Data Exposure by Controlling Activity

Today, your employees often collaborate with each other, external contractors, third-party vendors, customers, and more. So, there's a real risk that data may be shared with the wrong person—either inadvertently or deliberately. Secure collaboration is critical to productivity and innovation. With so much data, multiple versions of files, employee turnover, and the existence of personal file sharing tools, you need to be able to effectively control activity to prevent data exposure.



1 Control access and sharing with policies

Restrict data access. Establish user- and device-based policies to control mobile access, BYOD usage, and more. This will help ensure that only the right people have access to data.

Prevent unauthorized data distribution. Control permissions to mandate that only authorized individuals can share data and specify whether they can share data outside the organization. Restrict files to view-only or set automatic link expiration for files shared externally.

Revoke data access. Sometimes data is shared with the wrong person or should no longer be accessible. Being able to immediately revoke access privileges lets you prevent inappropriate access to files.

2 Restrict activity by file classification

Specify file properties. Classify files to ensure effective information rights management. Specifying file properties enables you to control and restrict how files can be viewed, edited, and distributed.

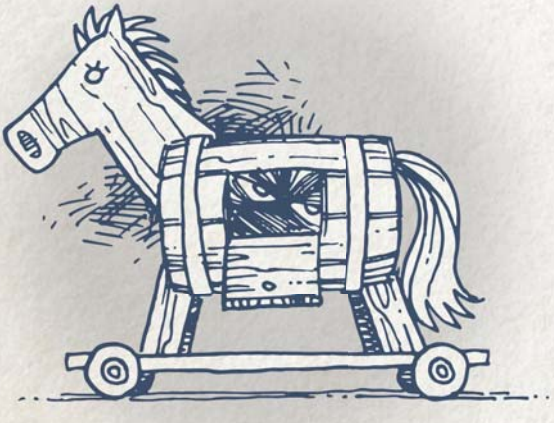
Limit activity based on file properties. Once you've specified file properties, create rules to limit data usage by properties such as geographic location, time of day, confidentiality level, version, and more. For example, if only your U.S.-based staff is supposed to have access to certain documents, you can be confident that those documents will not be available to those outside U.S. borders.

Control all aspects of data usage. Achieve granular control over all aspects of file usage, beyond whether it can be viewed or shared. Depending on your compliance requirements, you can disable copy and paste, prevent screenshots, enable offline viewing for a certain number of hours, set classified files to self-destruct after a period of time, and more.

3 Block data access by any unauthorized application

Prevent employees from sharing with personal tools. With the proliferation of personal file sharing tools, it's tempting for users to employ their own methods to share corporate data. This introduces risk to data security and protection. Blocking access to and sharing of files by any unauthorized service helps you safeguard confidential information.

Control mobile sharing. Mobile devices present unique challenges versus laptops when it comes to accessing and sharing data. You should be able to allow users to access their data on mobile devices and share it through approved channels while blocking distribution of data through unauthorized apps.



Most Common Ways Users Store and Access Files on Multiple PCs, Smartphones, or Tablets

In their quest to easily access their data from multiple devices, users resort to activities that leave data unprotected and at risk.

1. USB flash drive or CD/DVD
2. Email attachments to myself
3. Network shared drive
4. File sync, sharing, or online locker service
5. Web-based office productivity suite

— Forrester, "Understand the State of Data Security and Privacy, 2013-2014," 2014

CHAPTER THREE

The Threat: Litigation & Compliance

Maintaining litigation and compliance readiness to save future cost, time and headaches

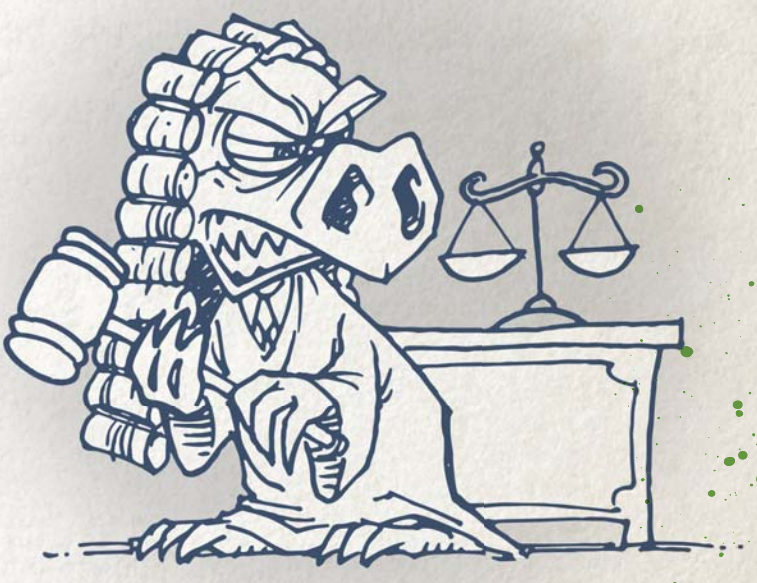
eDiscovery and compliance are scary topics.

They involve time-consuming and expensive processes. They're complicated by data dispersed across myriad endpoint devices. They are the bane of IT's existence.

Only 28% of CIOs believe their mobile security policies would satisfy an auditor[2]. Protecting data on endpoints is now about more than just back up. Capturing and tracking data on these devices to enable eDiscovery and compliance is critical. By being litigation-ready, you can save hours of IT and legal time, reduce the overall cost of gathering data for legal hold, and ensure all relevant data is effectively gathered for lawsuits and audits.

[2] Gartner, "CIO Attitudes Toward Consumerization of Mobile Devices and Applications," 2011

How to Gather and Provide Data for eDiscovery



It's happened: your company has been served legal notice. The legal department has come to you with a list of users to put on legal hold. You have to gather and provide all relevant data. It doesn't have to be a nightmare, though. With the right survival tips, you can be fully prepared when litigation and compliance issues strike.

1 Gather and provide data to your legal team

Capture endpoint data to a centralized data store. This will give you full visibility, and you'll be prepared for litigation before it happens.

Locate the data belonging to the users in question. Determine custodians whose data needs to be put on legal hold, then find these users by federated search or list import.

Place legal holds on captured data. Suspend data retention policies and preserve the content in place to ensure it remains securely stored and unchanged.

Hold data until ready for review by legal teams. Keep users on legal hold for an indefinite amount of time until legal is ready to review stored data. All past data will be preserved, and any new data created by users can also be secured.

Provide data to legal teams. Activate access for legal administration to review data that you've put on legal hold. From there, data can be transferred into an eDiscovery system, enabling the downstream legal process of review and tagging to begin.

2 Track data usage

Find out how users have been sharing and modifying data. With user audit trails, you'll have a stream of all user activity for full insight into all aspects of sharing and access.

See activity for specific files and folders. See the who, when and how of specific files or folders. Know which have been shared, downloaded, restored, accessed from a mobile device, and/or deleted.

See how users have been sharing data with external users. If your employees have been collaborating with external users, see which files have been shared and which ones have been downloaded.

Don't forget about admin activity. Users aren't the only ones you need to track for compliance purposes. Use admin audit trails for an undeletable stream of activity, including creating, modifying or deleting a profile, downloading a file, updating a user, adding or updating an admin and restoring data.

3 Locate deleted files

Keep past copies of all data. Restoring previous file versions or deleted files can be just as important as putting data on legal hold. Configure data retention policies to ensure your backup tool keeps copies of all past data, even if it's been deleted.

Locate the files in question. Use federated search to locate the files by criteria such as file name, type, user, and date.

Restore previous versions of files. By saving snapshots of files over time, you can locate and restore previous file versions to see how they have been modified. You can even restore files that belonged to employees who are no longer with the company.

IT's Worst Nightmares

5 Forgetting to wear pants to work

4 Having the CEO's computer crash in the middle of a board meeting

3 Upgrading all the company's machines to a new OS

2 Having employees fall for a phishing scam

1 **Getting a notice from legal to preserve data for litigation**

CHAPTER FOUR

The Threat: Lost, Stolen, and Damaged Devices

Escaping data breach and lost productivity when devices are lost, stolen, or damaged

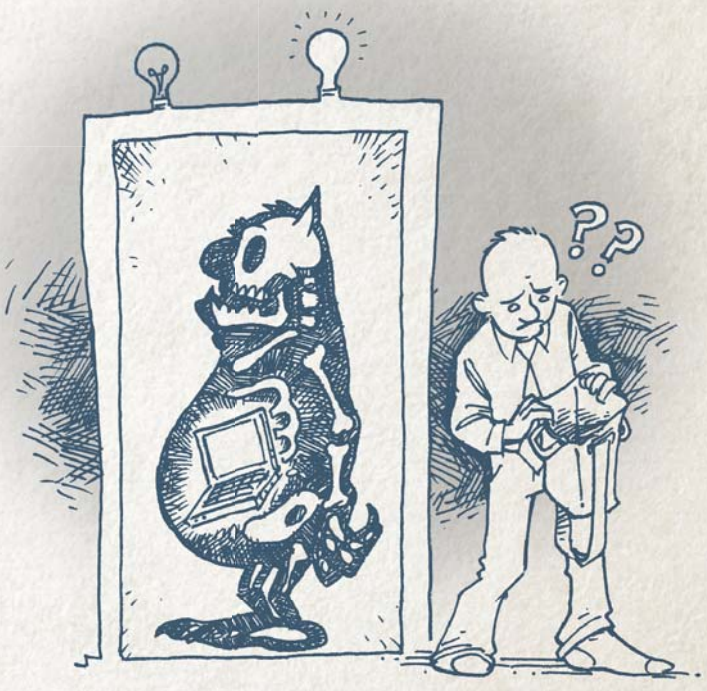
75% of today's workforce is mobile.[3]

Your corporate data is moving around like never before. Employees store all kinds of data on laptops and mobile devices because those are the devices that they primarily use. In fact, Gartner calculates that 28% of corporate data is stored exclusively on endpoint devices. However, employees don't think about what would happen if their devices were damaged or broken—and sometimes, neither does IT. In fact, only 35% of enterprise laptops are backed up[4].

Losing a laptop can result in extensive employee downtime. It can also lead to data breach if devices fall into the wrong hands. With the average cost of recovering from a single corporate data breach at $7.2 million[5], it's a risk your organization can't afford to take. The wild can be a savage, unforgiving place.

[3] IDC, "Worldwide Mobile Worker Population 2009-2013 Forecast," 2010
[4] ESG
[5] Ponemon Institute, "2010 Annual Study: U.S. Cost of a Data Breach," 2010

How to Survive the Loss or Theft of a Device



Here's a typical scenario: you get a call from one of your salespeople, saying that he's lost his laptop. He thinks he might have left it at airport security, but when he goes back to check, it's not there. The way in which you're able to respond to this situation can spell the difference between survival and extinction.

1 Locate the misplaced laptop and prevent data breach

Determine the location of the device. Use geolocation to pinpoint the exact location of a lost or stolen device. You should be able to determine the location of the device within three to six feet, so if it's still in the airport you'll be able to tell whether it's at security, in the bathroom, or in lost and found.

Retrieve the device if possible. If the device is somewhere you or the salesperson can safely retrieve it, then go and collect your property. However, if the device is sitting on the tarmac, in the garbage disposal, or in a thief's car headed away from the airport, recognize that it's out of your reach and don't attempt to reclaim it.

Remotely wipe corporate data. If you're unable to retrieve the device, initiate a remote wipe so that all corporate data will be removed the next time the device connects to the Internet.

2 Restore data and provide ongoing data access

Get the user back to work immediately. With a web client and mobile apps, the user can get back to work with a spare laptop, personal tablet, smartphone, or public computer.

Let users self-restore data and settings. Once the user has a new laptop, let them restore data and settings themselves. This reduces the time that your team has to spend getting them back up and running again.

Don't wait for data to fully restore. Enable the user to get back to work right away with a backup tool that restores the most important files first. Users can start working on their priority files while remaining files restore in the background.

Provide the user with a familiar working environment. Restore personal settings as well as data. Users can set right to work without spending time bookmarking their most-visited sites again, setting up mail preferences, or restoring their favorite screensaver.

3 Make sure your users back up their data

Recognize that you can't rely on your users to actively back up their own data. Whether it's data on a coffee-damaged laptop or files that have been accidentally deleted, the key to retrieving lost data is to ensure that the data is continuously backed up. The best solution is an automatic backup that runs invisibly in the background, without interrupting users.

Decide how frequently data should be backed up. You can control the specifics of how data is backed up, such as frequency and over what types of networks (for example, avoiding backups over cellular networks).

Select the most important folders to back up. Make sure users' most important data is backed up by selecting specific folders (such as My Documents) for backup.

Give your users the ability to back up additional data, at your discretion. You can give users as much or as little control over what they back up as company policy dictates. Let them add folders and files for backup if this is permitted. If you don't want them backing up home videos, music files and personal photos, exclude those file types from backup.

Where Laptops Are Lost

43% Off-site

33% In transit

12% Workplace

12% Unknown

— Ponemon Institute, "The Billion Dollar Lost Laptop Problem," 2010.

US Airports with Highest Weekly Frequency of Laptop Loss

1 **LAX**
Los Angeles International

2 **MIA**
Miami International

3 **JFK**
John F. Kennedy International

4 **ORD**
Chicago O'Hare International

5 **EWR**
Newark Liberty International

6 **LGA**
New York La Guardia

7 **DTW**
Detroit Metropolitan Wayne County

8 **DCA**
Ronald Reagan Washington National

9 **ATL**
Hartsfield-Jackson Atlanta International

10 **IAD**
Washington Dulles International

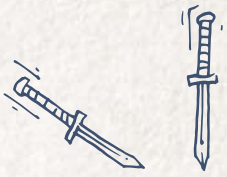
— Ponemon Institute, "Airport Insecurity: The Case of Missing & Lost Laptops," 2008

TECHNIQUES FOR BRINGING A DEVICE BACK TO LIFE

THAT YOU

SHOULDN'T TRY

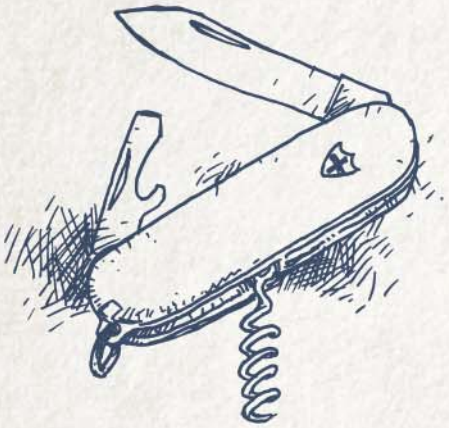
- Submerge the device in rice
- Use a vacuum cleaner to suck out the water
- Clean the inside of the device with rubbing alcohol
- Dry the device off with a hair dryer
- Microwave the device to evaporate the water



CONCLUSION

There are a lot of threats to data in the wild; make sure your data is defended.

We hope this Guide gives you a fresh perspective on the current endpoint data protection landscape. Protecting and governing corporate data requires experience, cunning and resourcefulness. You can venture into the wild alone, or trust a partner uniquely qualified to see you safely through. To learn how Druva can be your critical key to survival, visit **wild.druva.com**. To learn more about Druva inSync, **visit druva.com/insync**.



druva

CORPORATE HEADQUARTERS

United States

150 Mathilda Place, Suite 450
Sunnyvale, CA 94086
Main: +1 888-248-4976
Sales: +1 800-375-0160

WORLDWIDE LOCATIONS

Europe

1 Furzeground Way
(Stockley Park)
Uxbridge, UB11 1BD, UK
Sales: +44 (0) 20 3150 1722

India

Muttha Chambers II, Level VI
Senapati Bapat Marg
Pune, India 411016
Main: +91 (0) 20 672 63 300
Sales: +91 (0) 20 672 63 395
Fax: +91 (0) 20 672 63 321

Singapore

The Co, 75 High Street
Singapore 179435
Sales: +65 3158 5080

Australia

Sales: +1 300-361-685