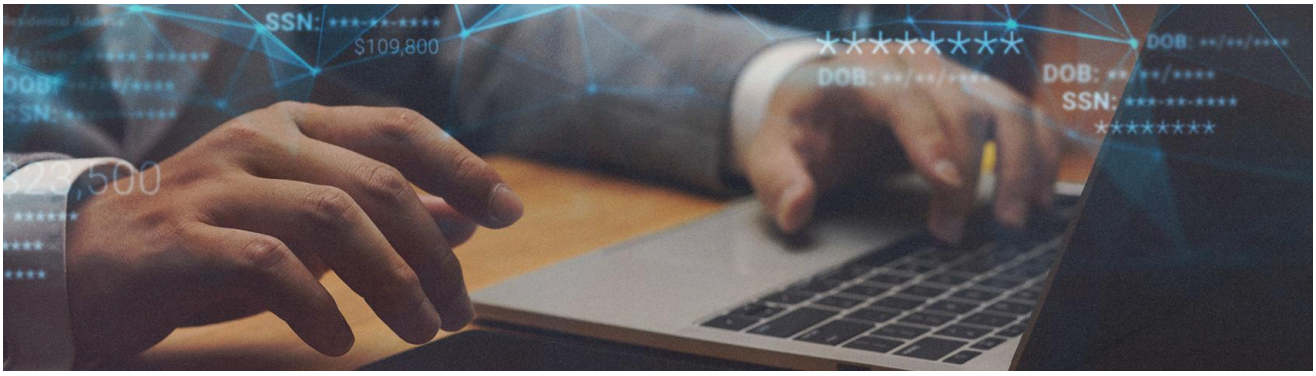
DEVICE & DATA PROTECTION



Our reliance on electronic information boosts productivity and lowers the cost of collaborating and managing quantities of information. Yet that reliance exposes costs and risks that are unacceptable in today's competitive environment. Trends in connectivity, mobility and data breach legislation demand solutions quite different from those that sufficed in the recent past. ***DriveStrike*** *provides a comprehensive data-protection solution to address these needs.*

CONTENTS

EXECUTIVE SUMMARY

For many organizations, electronic information is the single most valuable asset outside personnel. Protecting those assets from breach or compromise—the exposure of critical information to unintended parties—is paramount to protecting your business.

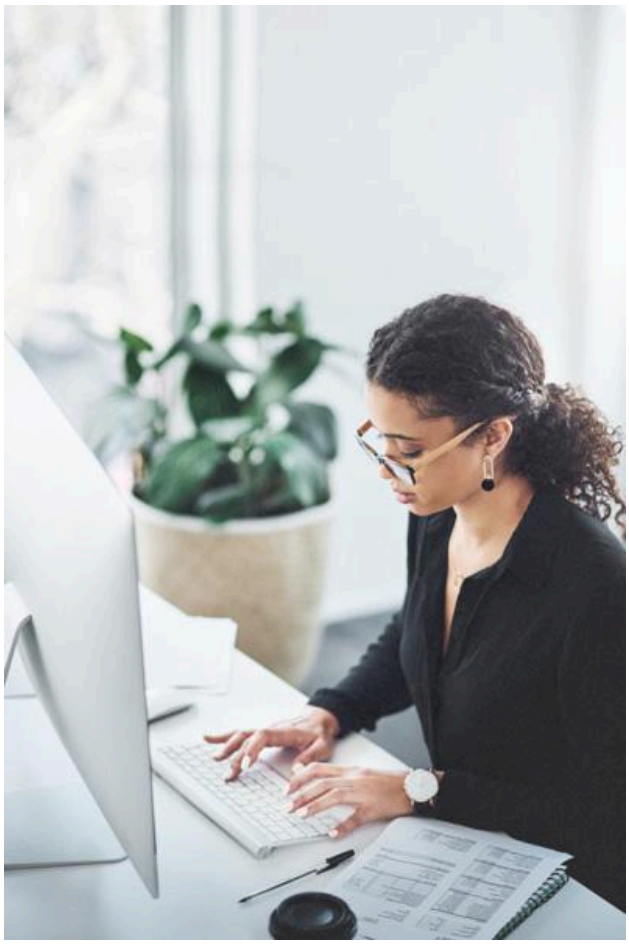
Today's data environment is no longer confined to an organization's local network, presenting new challenges and opportunities for data protection. With laptops being the most common computers sold, an organization's critical information is spread across more working locations and schedules than ever before.

Compounding the data protection challenge, smartphones and tablets increasingly carry copies of personally identifiable information (PII), protected health information (PHI), work email, contacts, sales data, financial data, insurance information, and documents. DriveStrike encrypts data in transport using TLS 1.2 with the strong cipher suite and stores data server side using AES256. All stored credentials are hashed and salted.

The global average cost of a data breach in 2023 was USD 4.45 million, *a 15% increase over 3 years.*

Source: "Cost of a Data Breach Report 2023"

According to IBM's Security analysis of research data compiled by Ponemon Institute, "this represents a 2.3% increase from the 2022 cost of USD 4.35 million. Taking a long-term view, the average cost has increased 15.3% from USD 3.86 million in the 2020 report."



DATA COMPROMISE

The persistence of data—in the wrong hands—can be as costly as its loss. How many customer records, accounts, contacts, and financial documents would you want a competitor, identity thief, or an unauthorized person to have?

The consequences are sufficiently grave that seasoned regulations such as the Data Protection Act for healthcare, PCI-DSS in financial services, GDPR, and FRCP for any company in a lawsuit specify requirements and best practices for handling data and preventing compromise. Newer legislation increases the stakes. Nearly all countries now have data breach legislation, requiring that organizations publicly disclose incident details, and inform parties whose personal information is compromised.

According to the Ponemon Institute, a typical data breach in the US costs organizations an average of $225 per compromised data record. The biggest component of that cost is lost business. A third of breach cases involve lost or stolen laptop computers or smartphones, in 2017 the average total cost of a data breach was measured in at $7.35 million.

HARDWARE LOSS

$49,246. That's the average cost of a lost laptop after accounting for replacement cost, detection, forensics, data breach, lost intellectual property costs, lost productivity and legal, consulting and regulatory expenses. Tracking and recovering lost computers and smartphones helps identify such causes, and prevent a repeat occurrence.

COMPREHENSIVE DATA & DEVICE PROTECTION

These risks highlight the need for a comprehensive data protection solution combining remote data wipes and hardware tracking.

DriveStrike addresses these needs in a manner that works the way today's organizations do, to deliver enterprise-level data protection at a fraction of its traditional cost. DriveStrike involves lightweight software installed on devices to be protected and a web-based management portal providing device and data protection across *Windows, MacOS, iOS, Linux, Android, and ChromeOS within one secure centrally managed solution.*

Administrators can balance central administration and user autonomy according to their needs. DriveStrike uses a Software-as-a-Service model, so it requires no additional IT infrastructure, is highly scalable, and can be easily and rapidly deployed.

The average cost of a lost and breached laptop is $49,246.

Source: "The Cost of a Lost Laptop"

According to Intel's sponsored research data compiled by the Ponemon Institute in 2009.

REMOTE WIPE

Almost every organization has had a smartphone or laptop lost or stolen. What's troubling is that 71% report that it resulted in a data breach.

DriveStrike provides protection from data breach by allowing users to remotely wipe sensitive data from their hard drives on-demand. From DriveStrike's secure login site, customers initiate a remote wipe. As soon as their lost or stolen machine connects to the Internet, the remote wipe begins.

Two options trade-off different qualities important to users seeking to prevent data compromise. When a user believes that time is critical in erasing his data, the DriveStrike Remote Wipe option can be employed to render the entire drive unusable in just a few seconds. The Destroy option renders a drive unbootable, and unmountable to be read as a secondary drive in another computer. This makes its data out of reach of everyone except for experts utilizing digital forensics tools to recover data. For encrypted Windows and Linux systems DriveStrike deletes and overwrites the local encryption key to prevent data access.

REMOTE LOCATION

DriveStrike *periodically records the location of every protected device* using the following location prioritization: GPS if the device supports it, WiFi triangulation, and finally recording the public and private IP addresses. DriveStrike retains 90 days for device location historical data. Administrators can request real-time location information on demand at any time for any device.

- **Geofencing:** Automatically send email alerts, lock, and or unlock on entry or exit of a defined geofence.

ENCRYPTION

DriveStrike provides **BitLocker encryption** integration empowering Administrators the ability to remotely enable, persist, and escrow encryption keys for Windows 10 Pro and Windows 10 Enterprise systems. For Windows devices with BitLocker enabled prior to DriveStrike installation – DriveStrike will obtain and escrow a Numerical and External encryption key providing Administrators the ability to remotely remove existing local encryption keys and rotating DriveStrike escrowed keys forcing a BitLocker recovery mode which prevents access to the devices data without the DriveStrike escrowed keys. Optionally, DriveStrike Admininstrators can enforce TPM+PIN as well as Non-TPM Passphrase requirements for all Windows devices at the Group level and provide for Self-Service Key recovery. For other operating systems DriveStrike reports the encryption status of data on the device.

HARDWARE RECOVERY

Ninety-two percent of IT security practitioners report that someone in their organization has had a laptop lost or stolen. And with the all-in cost of each loss ($49,264), you can't afford not to track each down. DriveStrike can track a lost computer by activating forensic data-gathering components within its software. To be activated, users must complete an electronic request and provide a copy of a police report detailing the loss. Once activated, DriveStrike works with Internet service providers and local law enforcement where your report is filed to recover your computer.

DriveStrike
SPEARSTONE

DriveStrike's security measures exceed HIPAA, SOX, PCI-DSS, and State and Federal data protection requirements

ORGANIZATIONAL DEPLOYMENT

While DriveStrike provides an easy wizard setup for user installations, it also supports enterprise deployments through a command-line based installation that can be invoked from Active Directory, LANDesk, BMC, or other enterprise software management tools Command-line installs can be tailored to optionally display the user interface during or after installation, and can be configured for a particular user, thereby prevent any device registration dialog from appearing when DriveStrike launches the first time.

MOBILE DEVICE MANAGEMENT

With DriveStrike you can centrally control the security policies as well as mobile application deployment, configuration, and setup.

Automatically install approved Android applications and restrict users from installing applications from the Google Play Store.

DriveStrike is an approved Google Enterprise Mobility Management Partner with the full suite of Android remote management features. Full Apple MDM support is planned for Q1 2022.

A PARTNERSHIP YOU CAN TRUST

DriveStrike was developed by **Spearstone**, which started in 2005 with a commitment to innovation and continuous improvement in data protection.

It drew on deep experience building solutions for *Fortune 500 teams in legal, financial, and professional services*, as well as small-office users in healthcare and related fields.

DriveStrike is the expression of its goal to deliver the protections large enterprises enjoy with the affordability that all professional organizations require. Our drive to be the best in class commits us to providing a level of service that you *will* notice.

We continuously seek and act on customer feedback, as we consider you the most qualified judge of our success.

Start your **30-Day free trial** today.

https://app.drivestrike.com/signup/