
The Leader in Endpoint Data Protection

Leveraging Managed Data Protection to Safeguard Intellectual Property

The proliferation of mobile endpoint computing devices has dramatically increased the availability and exposure of corporate information, creating new challenges for IT security. Each day, millions of laptops, portable hard drives and smart phones go into the field—outside established security perimeters where they are vulnerable to thieves, competitors, and adversaries. If lost or stolen, these endpoint devices could lead to the exposure of an organization’s intellectual property and other types of confidential business information. As a result, many organizations are increasingly focusing their information risk management strategies on protecting data stored on endpoints or portable media devices.

Portable Data is Data at Risk

Laptop PCs, flash memory cards, portable hard drives and smartphones can store massive amounts of data, and are often capable of accessing network resources from outside the corporate firewall. While many large organizations are prepared to write off the loss of hardware assets in the field as a cost of doing business, the theft of the data stored on those hardware assets can have a devastating impact.

The potential harm may include loss of proprietary company information to competitors, the compromise of national secrets, or the loss of important personal employee information that can be used to facilitate attacks on corporate networks. In some cases the loss of data could have devastating secondary consequences: critical technology data or information relating to security measures, for example, could fall into the hands of terrorists or others who would intend harm.

Many organizations have internal policies that prohibit users from accessing or storing sensitive information outside the corporate firewall, but it is very difficult to enforce these policies in a uniform manner. Security policy enforcement is also a technical challenge, given the heterogeneous nature of endpoints and the sheer number of devices in use. And, as evidenced by the growing number of data security breach disclosures resulting from the loss or theft of laptops, employees and consultants are constantly taking sensitive data on the road or to their homes, despite corporate security policies that prohibit such activities.

“GuardianEdge is committed to helping enterprise customers safeguard sensitive and proprietary information throughout their organization.”

Encryption software provides the foundation for securing data on endpoints such as desktops, laptops, or removable storage devices, but traditional data encryption software solutions are designed for individual users and do not scale well to meet the needs of corporate and governmental organizations. These organizations require a comprehensive solution for endpoint data protection that helps automate and enforce endpoint data security policies in a consistent manner across their organization.

The Solution:

A Managed Approach to Enterprise Data Protection

The most effective way to prevent the loss of sensitive data at rest on laptops and other devices is to implement endpoint data protection software from GuardianEdge. Commercial and government organizations around the world rely on GuardianEdge software solutions for hard disk encryption, removable storage media encryption, and endpoint device access and usage control to secure their critical information assets.

As a trusted and experienced provider of enterprise-grade data protection solutions, GuardianEdge is committed to helping enterprise customers safeguard sensitive and proprietary information throughout their organizations. The GuardianEdge Data Protection Platform offers comprehensive data protection capabilities that go far beyond the limitations of single-point

solutions, offering a unified approach to managing multiple data protection solutions while leveraging existing business processes and IT infrastructure.

By implementing GuardianEdge solutions as part of an integrated system for managing information security, organizations can:

- Reduce the risks and liabilities resulting from the compromise of trade secrets
- Provide auditable evidence that data on missing assets is protected
- Prevent erosion of brand equity or goodwill, and promote a stronger corporate image
- Expand revenue potential via data security as competitive advantage

The Bottom Line

Laptop PCs and other endpoint devices can greatly enhance worker productivity, but they can also make it much more difficult to maintain control over intellectual property and other valuable information assets. However, by adopting endpoint data protection solutions from GuardianEdge as an integrated component of a comprehensive risk management strategy, organizations can take control of their electronic information assets and prevent the exposure of intellectual property and other confidential business data.

Corporate Headquarters
475 Brannan St., Suite 400
San Francisco, California
94107-5421

t. +1.800.440.0419

t. +1.415.683.2200

f. +1.415.683.2349

www.GuardianEdge.com

GuardianEdge is a trademark of GuardianEdge Technologies Inc.
All other products and services mentioned are the trademarks of their respective companies.