

An Enterprise Approach to Endpoint Data Protection

Are you the next headline? The barrage of high-profile news regarding loss or theft of sensitive information has raised awareness of the risks faced by all organizations. The consequences of these breaches have made securing data a top priority for the enterprise. Simply disclosing a leak of customer information can entail huge costs for everything from communicating with affected individuals, to staffing up a hotline, to provisioning free credit reports, to legal expenditures and more. In addition, the resulting loss of goodwill and trust can have a much broader impact, including damage to brand equity, declining stock price, and the opportunity costs of distracting the organization from its core business.

The Unacceptable Risks of Unprotected Data

Additionally, along with the privacy protection measures included in the Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability & Accountability Act (HIPAA), and Federal Information Security Act (FISMA), many states as well as foreign governments — are adopting tough disclosure laws similar to California's SB1386. Companies that compromise the security of consumer information or fail to disclose such breaches also face vigorous prosecution and enforcement actions by national government agencies, such as the US Federal Trade Commission and the UK's Financial Services Authority. These actions can lead to crippling fines and loss of customer confidence, as well as forced settlements with affected individuals.

Given the high stakes involved with the compromise of sensitive information, no one can afford to gamble by failing to adopt anything but mature and proven data protection measures. Organizations need to reduce or eliminate the risks associated with data breaches by securing data no matter where it is at all stages of its lifecycle.

The Benefits of Evolving from Compliance to Governance

Organizations of all types now find their operations facing an unprecedented level of scrutiny and oversight through the many legislative initiatives that have become part of the business landscape. The initial response of most IT organizations to implementing the many varied controls required to meet these requirements was to adopt a reactive posture, driven to a large extent by near-term audit scrutiny. Today, however, this stance has evolved to a much more strategic approach. Organizations have found that the practices and protections demanded by the various regulatory tracts which are founded in established control frameworks such as COBIT and ISO17799 represent a best practices approach to managing the security environment.

Organizations need to reduce or eliminate the risks associated with data breaches by securing data — no matter where it is at all stages of its lifecycle.

As a result, enterprises have now begun adopting these measures and practices pro-actively with the goal of establishing a governance posture one that not only satisfies immediate obligations but also stands as clear and demonstrable evidence of the organizations commitment to its customers, partners and employees.

A Unified Approach to Data Protection

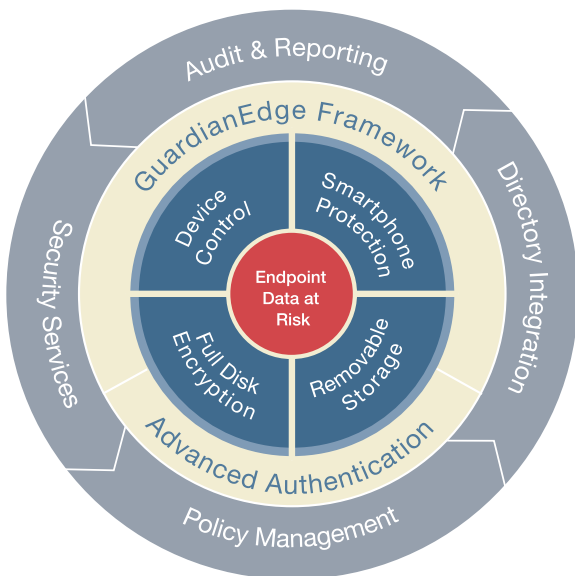
This emerging focus on governance brings with it significant challenges. In the past, many of the required controls and processes were adopted on a project basis. However, enterprises have discovered that the resulting inefficiency led to redundancies in terms of people and processes, and unnecessary costs. Additionally, the absence of system-level correlation across the components of the security ecosystem creates the potential for misalignment, which can lead to security exposures. It also adds the cost and complexity of manually correlating the output of multiple control systems in order to satisfy internal and external audits.

In response, enterprises are looking for solutions that provide a much higher degree of unification, typically through a centrally managed and monitored policy infrastructure. This type of unified approach enables organizations to leverage their resources more efficiently, and minimizes the potential for material errors or omissions.

As the adoption of data protection controls accelerates, organizations are learning that the full scope of data protection measures must effectively address the encryption of hard disks, strong authentication of users, protection for data on removable media, and policy-based access controls for I/O ports and their associated devices. A unified approach is required to closely integrate these capabilities. This lowers the cost of ownership by eliminating redundancy, and ensures that misalignment of policies and their administration do not create hidden exposures.

The GuardianEdge Data Protection Platform

GuardianEdge provides a unified data protection platform that tightly integrates data protection controls. The core security and management services required to implement these controls including policy management, user authentication, key management, provisioning, backup, recovery, monitoring, and reporting are all enabled through the centrally managed GuardianEdge Data Protection Framework. This unified foundation leverages the efficiency of shared services to power a suite of data protection applications that include hard disk encryption, removable storage encryption, and external device access control.



Platform Benefits

- Achieve safe harbor from mandatory disclosure laws
- Prevent loss of consumer and employee data
- Demonstrate compliance with privacy regulations
- Protect intellectual property against theft or loss
- Securely transfer or dispose of old PC's
- Centrally manage unified data protection policies

"The GuardianEdge solution provides a complete framework to protect data on endpoints from theft or loss — inside or outside the perimeter." *Alan Fudge - CEO, GuardianEdge Technologies*

This approach to data protection gives organizations the ability to define and implement the full suite of policies required to protect their data with a single product solution. These policies are delivered to the GuardianEdge security modules on the endpoints through the framework infrastructure, which leverages industry-leading integration with Microsoft's Active Directory that provides the out-of-the-box scalability, robustness, and availability demanded by enterprise IT environments. Additionally, by coupling the implementation of data protection policies with existing domain management tools, privileges and

practices, enterprises can easily map data policies to their organizational structure, business processes and user and machine roles.

The audit and reporting capabilities of the GuardianEdge Data Protection Framework enable administrators to demonstrate that the required policies are in place, and that users and machines are in compliance with their security requirements. This centralized visibility streamlines audit processes, and ensures that the intellectual capital of the business is safeguarded at all times.

Meeting the Solution Challenges of the Enterprise

GuardianEdge provides an integrated set of solutions that protect data at rest on or ported across endpoint devices. These include:

Using Encryption to Avoid the Costs of Data Breach Notification

Disclosure of data security breaches stemming from the theft or loss of laptops containing personal information can cost millions of dollars but is required by laws like California's SB1386. The GuardianEdge Data Protection Platform can eliminate this need for disclosure by not only assuring this data is always protected but also providing the ability to prove data was protected at the time of loss. It provides a unified approach to protecting endpoint data by combining robust, easy-to-use encryption and access control applications under a single powerful management framework.

Leveraging Managed Data Protection to Safeguard Intellectual Property

Laptop PCs and other endpoint devices make it more difficult to maintain control over intellectual property and other valuable information assets. As an integrated component of a comprehensive risk management strategy, GuardianEdge endpoint data protection solutions let organizations take control of their electronic information assets and prevent the exposure of intellectual property and other confidential business data.

Satisfying Global Privacy Initiatives with Endpoint Data Protection

The globalization of data protection legislation presents new challenges for regulatory compliance management. The GuardianEdge Data Protection Platform can help organizations reduce the cost and complexity of meeting global compliance requirements by securing information stored on endpoints across the enterprise.

Ensuring Data Is Secured When Retiring PCs

Disposing of PCs without a process for sanitizing sensitive data can expose organizations to security breaches and financial risks. The GuardianEdge solution overcomes the limitations of most conventional data sanitation techniques to protect sensitive information during use and disposal of PCs.

“Companies should act now and protect all data before they themselves are faced with the costs of a data breach. There is a very real risk that long-lasting damage could be done to a company’s reputation and brand image.”

—*Alex Kwiatkowski, lead analyst at Datamonitor.*

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.