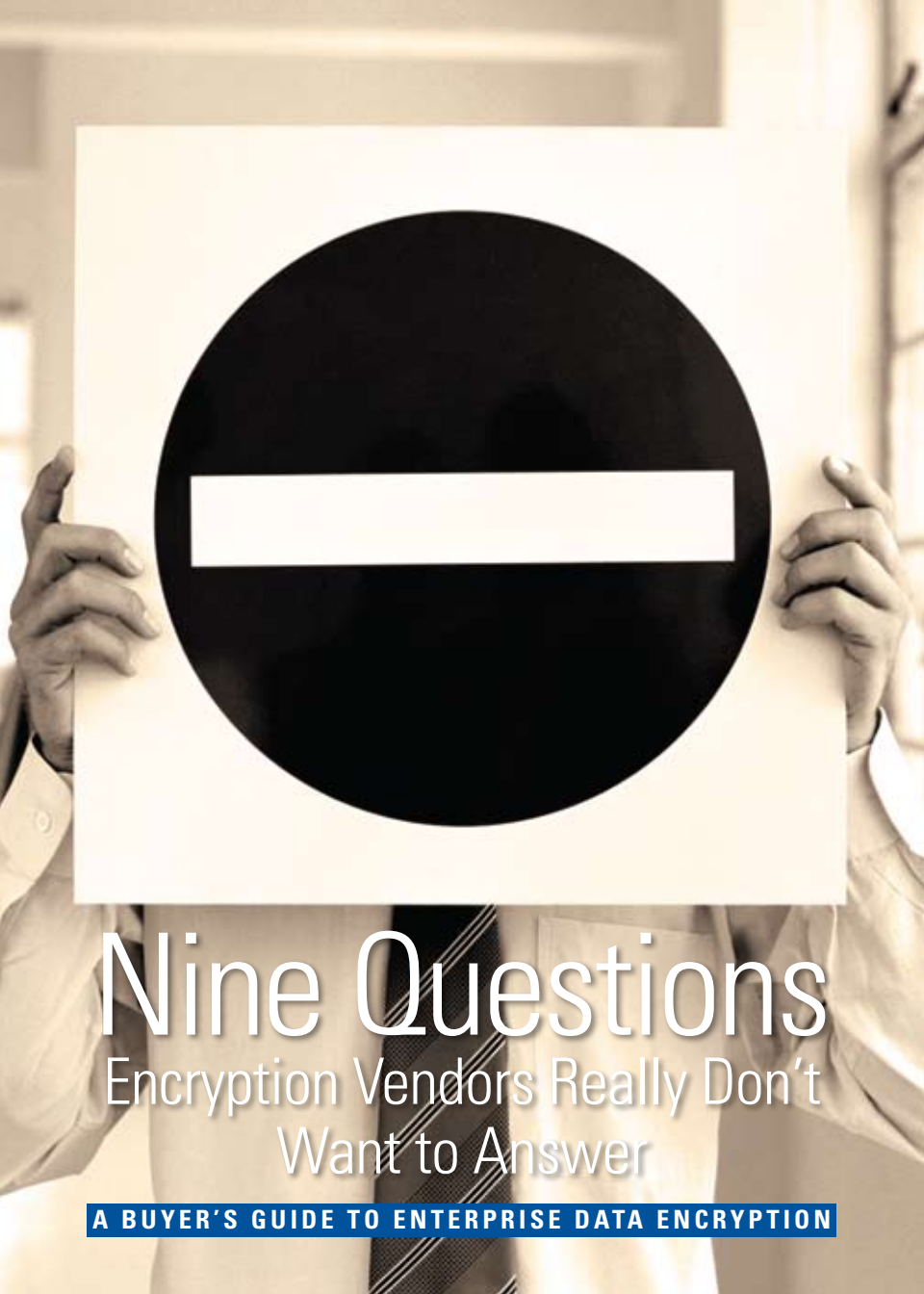


Nine Questions

Encryption Vendors Really Don't Want to Answer

A BUYER'S GUIDE TO ENTERPRISE DATA ENCRYPTION

1 Can your solution protect all of my organization's data?

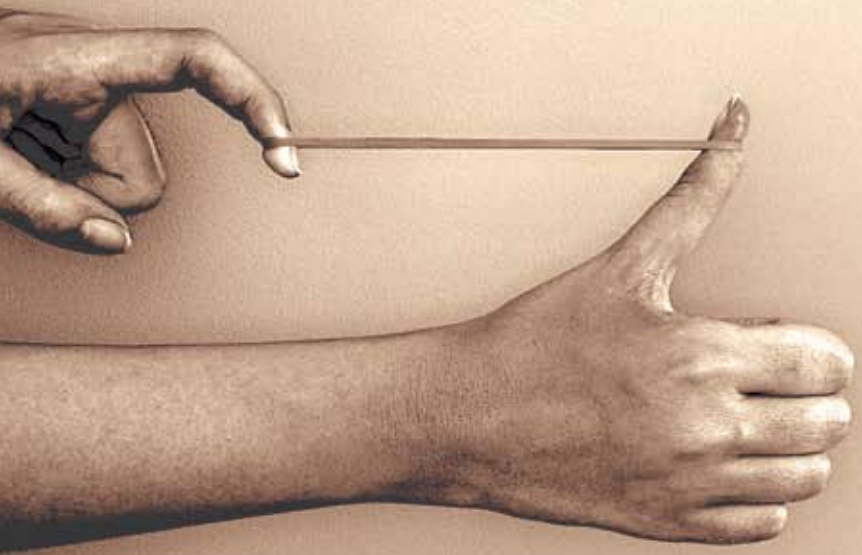
You ask vendors if they can protect all your data, and they say yes. They tell you to trust that their "full," "complete," or "comprehensive" product will make all your data secure for years to come.

What they don't tell you is that their product only protects "all the data" contained on specific devices, such as laptops, USB flash drives, or PDAs. That's a good first step, but how are you going to protect the rest of your enterprise data? The reality of point products is: you'll have to find another vendor to secure the rest of your data.

You must secure all your data, wherever it is stored and transmitted. To protect all your enterprise data, you need a truly comprehensive solution that protects individual devices and internal and external communications, servers, networked storage, data transfers, and automated backups.

By definition, point products cannot offer comprehensive enterprise data protection. That's why a business that needs to protect all it's data requires a strategic framework that supports consistent key management, user management, and policy support across multiple encryption applications — that is, you need an encryption platform.

2 Is your solution flexible enough to meet the needs of a growing business?



Vendors always say that their encryption products are scalable to meet your growing needs. But that usually means that their product can support more end users or more devices. The problem is that today's business growth is rarely so simple.

In the months and years to come, you may add partners, international offices, mobile employees, outsourced contractors, and new technologies. Each of those changes leads to growth — not just in the number of end users or devices, but in the type and amount of data that your business stores and communicates each day.

Your company's growing data protection requirements should not depend on installations of multiple encryption infrastructures or differing deployments that are costly and time-consuming. The solution: a single encryption platform that provides a unified, extensible framework that lets you easily add applications without slowing productivity, disrupting compliance, or driving up costs as your business evolves.

3 How quickly can my organization deploy encryption?

Most vendors can deploy some type of data protection quickly. Unfortunately, you'll probably need to implement another point product — and another — soon after that.

Vendors may tell you that their product deploys faster than competitors, but they won't tell you that deployment speed comes at a price.

Inevitably, you'll need to protect another device or a new source of data. When you do, you'll probably have to shop around for another vendor, and then repeat all the time-consuming and costly testing, training and implementation steps you've already gone through to deploy your first encryption solution.

It is a classic story of taking the time to do the job right the first time, or suffering unforeseen consequences at a later date. With encryption, the companies most likely to succeed make sure they cover all their data the first time. With an encryption platform approach, you deploy a solution just once to protect all your data.

4 How difficult is it to manage data encryption?

Encryption vendors often emphasize the simplicity of encryption management . The best products can be centrally managed from a single console, providing consistent policy and key management while reducing ongoing management and maintenance demands.

What they fail to mention: encryption management becomes exponentially more complicated and costly for multiple point solutions. Additional encryption products require more IT staff to handle integration, more updates and upgrades, and more maintenance.

When you deploy an encryption platform throughout an enterprise, you don't need to deploy and manage multiple point solutions. As a result, your staffing and management needs won't grow, even when your business does.

The best encryption solutions are centrally managed from a single console, providing consistent policy and key management with minimal ongoing management and maintenance. To accommodate new needs, just add new applications to the encryption platform. These applications automatically integrate with your existing key management, policies, provisioning, and other security services — minimizing your management requirements.

Recent research by The Ponemon Institute confirms the management benefits of encryption platforms. More than 60 percent of the 975 IT and business professionals surveyed indicated that an encryption platform reduces operational costs and provides the flexibility to add other encryption applications. Another 54 percent indicated that an encryption platform improves business efficiency by eliminating redundant administrative tasks.

5 How will your data encryption solution affect my organization's day-to-day productivity?

Vendors often claim that their encryption solutions will increase productivity. They say that their solution is transparent, their administration console is easy to use, and your end users won't experience delays or downtime. Yet you continue to hear stories about encryption hampering workflow and inhibiting productivity. Why is that?

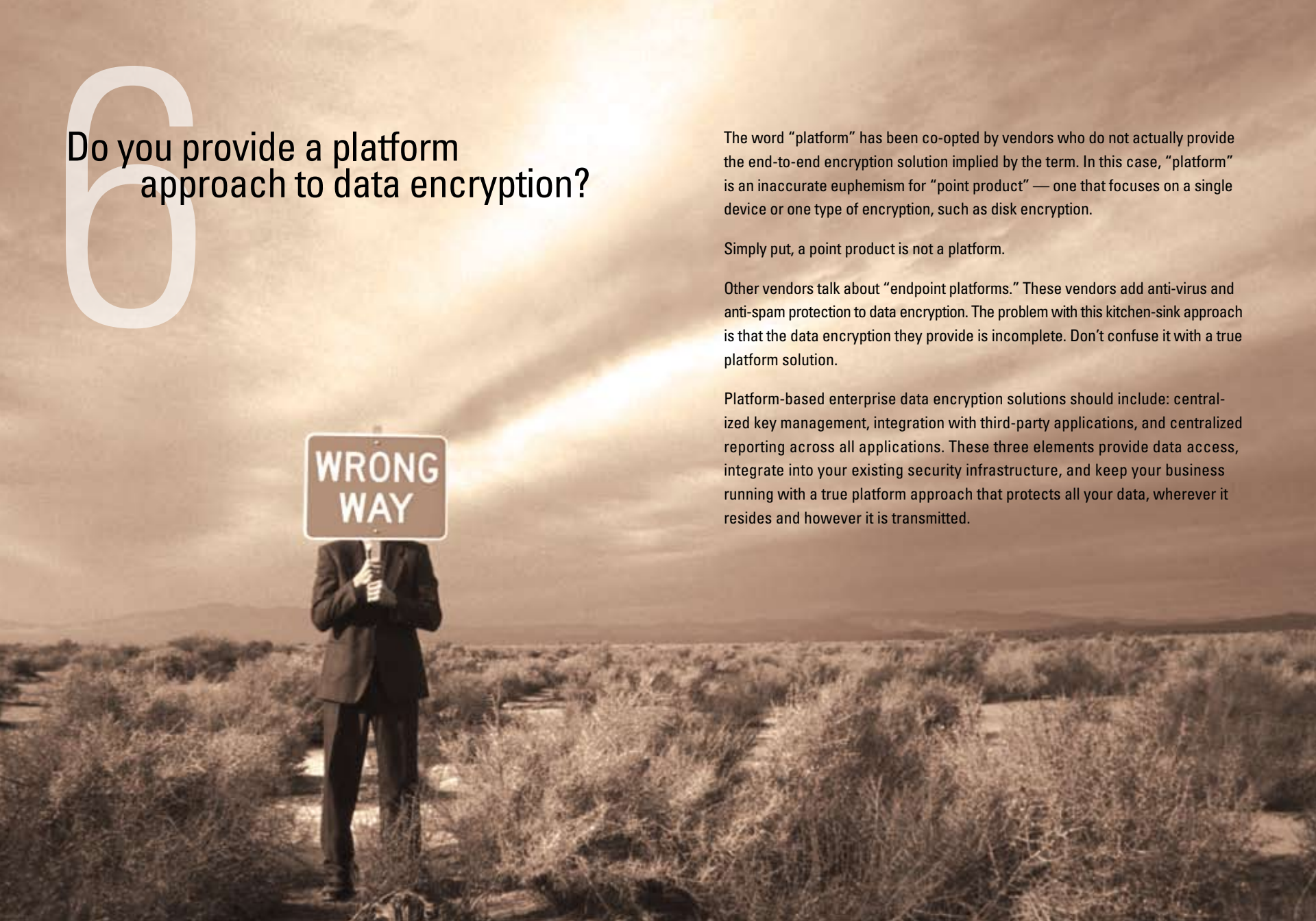
Point-solution vendors focus only on their siloed encryption product. It may be true that their single product is easy to deploy and manage. They may even have studies showing that their product enhances productivity — when compared to other point products.

What they're not telling you is that you'll require more than just their solution and that when you add additional encryption solutions, your administrators will face greater complexities, your data may not be accessible when you need it, and your end users may experience more downtime.

A recent Ponemon Institute survey reported that 75 percent of respondents viewed an enterprise-wide encryption policy and key management as "important" or "very important," largely because of productivity issues created by point encryption products.

"As expected, leading IT organizations with the most effective security programs are the ones at the forefront of strategic planning and use of encryption," says Dr. Larry Ponemon, chairman and founder of the Ponemon Institute. "Such organizations are significantly more interested in a platform approach to data encryption."

6 Do you provide a platform approach to data encryption?



The word “platform” has been co-opted by vendors who do not actually provide the end-to-end encryption solution implied by the term. In this case, “platform” is an inaccurate euphemism for “point product” — one that focuses on a single device or one type of encryption, such as disk encryption.

Simply put, a point product is not a platform.

Other vendors talk about “endpoint platforms.” These vendors add anti-virus and anti-spam protection to data encryption. The problem with this kitchen-sink approach is that the data encryption they provide is incomplete. Don’t confuse it with a true platform solution.

Platform-based enterprise data encryption solutions should include: centralized key management, integration with third-party applications, and centralized reporting across all applications. These three elements provide data access, integrate into your existing security infrastructure, and keep your business running with a true platform approach that protects all your data, wherever it resides and however it is transmitted.

7 How well does your data encryption solution integrate with my organization's existing applications?

Ask point-solution vendors if their product integrates with your existing systems and applications, and the response will probably be, "Of course."

A typical point product does integrate well enough into the infrastructure to install and run the application. But it may not integrate with additional encryption applications that you may need down the road. And it may not integrate with your existing PKI solution — meaning you may have to throw away your investment.

A platform-based encryption solution poses neither of these problems. It will coexist with your existing email and other systems including PKI, archive, data loss prevention, directory services, and strong authentication without requiring custom integration or modifications to your architecture. And when you need to add encryption applications, they will integrate smoothly into your existing encryption framework. You won't need to adjust user management or key management.

8

Will your solution help my organization comply with legal requirements?

Government laws and regulations such as the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA) require strict protection of personally identifiable information.

Unfortunately, businesses concerned about these and other privacy requirements often focus on a single data vulnerability, such as laptops. A vendor will tell you that they can protect all the data on all your laptops or other devices to ensure compliance with a particular law or regulation.

However, this thinking leads to disjointed and siloed encryption deployments that leave many companies vulnerable to data breaches and compliance violations.

An encryption platform enables compliance by reaching for the root of the problem. When you use an encryption platform to protect all the data at rest and all the data in transit to and from your company, it addresses all the threats to your data. This allows you to more easily monitor events and generate compliance reports to satisfy auditors, senior management, and other stakeholders.

Because an encryption platform protects all your data, you don't need an auditor's checklist to tell you which data or which approach devices to protect. A platform solution enhances enterprise and job security, and facilitates compliance with laws and regulations.

9 How will your solution save time and money for my organization?

Data breaches are expensive. The Ponemon Institute found the average cost of a data breach is more than $6 million per incident, or $197 per individual compromised.

By adding up the tremendously high costs of data breaches and comparing them to the relatively minor cost of a data encryption solution, encryption vendors can boast impressive figures for both TCO and ROI.

But that's not the whole story.

A single point solution may be relatively affordable, but you'll need another one soon. And then another one later. And with every additional point solution, you need to find a new vendor, test and deploy the new solution, and then maintain it.

The high ongoing costs of point solutions explain why Forrester Consulting recently found that the cost of implementing a point encryption solution is 185 percent greater than the cost of comparable functionality from a platform solution.

Forrester Consulting also found that the encryption platforms enabled an organization to avoid spending more than $2 million for implementation labor, software, professional services, and hardware required for comparable point encryption products.

The international media company studied the PGP® Encryption Platform to protect confidential data in emails, on laptops, and on file servers. According to their Chief Technology Officer Corporate Center, "The PGP Encryption Platform is a financially attractive, scalable enterprise solution that grows with our requirements and costs a tenth of a classic PKI solution."

Nine things your data encryption solution should do:

1. Protect all your data
2. Scale with your business
3. Deploy quickly
4. Be easy to manage
5. Increase productivity
6. Offer true platform functionality
7. Integrate with existing and new applications
8. Efficiently support compliance
9. Reduce costs

The PGP Encryption Platform enables solutions that meet all of these requirements.

The PGP® Encryption Platform Difference

The PGP Encryption Platform reduces the complexities of protecting business data by enabling organizations to deploy and manage multiple encryption applications cost-effectively from a single management console. Most importantly, the PGP Encryption Platform provides the automated services, centralized management, consistent policy enforcement, and extensible framework needed to develop and deliver a comprehensive, lasting enterprise data protection strategy. **www.pgp.com**

The Total Economic Impact™ of PGP Encryption Platform
Forrester Consulting Commissioned by PGP Corporation March, 2008

2007 Cost of A Data Breach
Research by The Ponemon Institute

2008 US Enterprise Encryption Trends
Research by The Ponemon Institute

PGP®
DEFENDING THE DATA

PGP Corporate Headquarters
200 Jefferson Drive
Menlo Park, CA 94025
U.S.A.
Tel: +1 650 319 9000

PGP (GB) Ltd.
Tel: +44 (0)20 8606 6000

PGP Deutschland AG
Tel: +49 69 838310 0

PGP Japan K.K.
Tel: +81 03 4360 8308