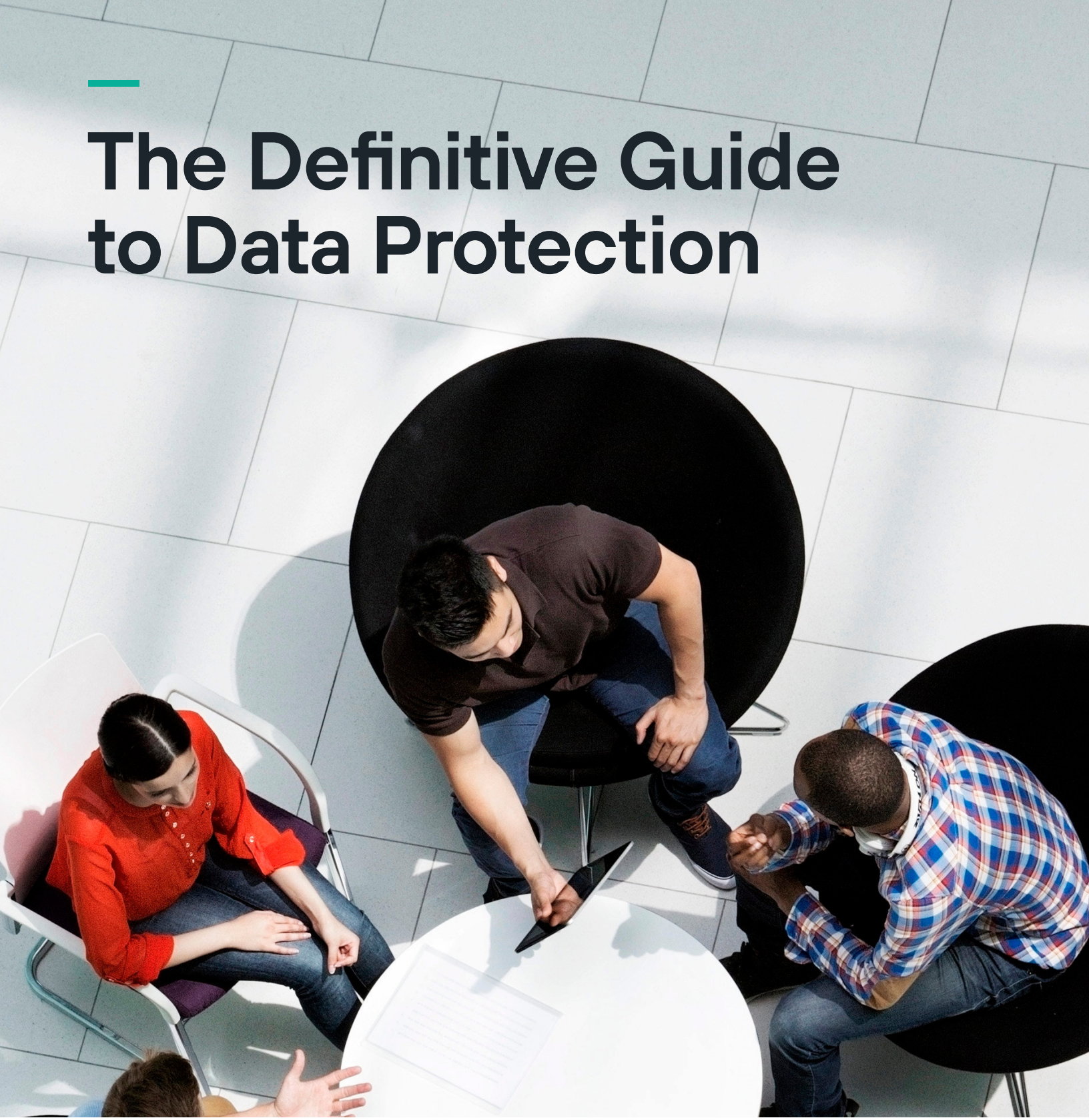
The Definitive Guide to Data Protection



Forcepoint

Brochure

Landscape Overview

In some ways, the relationship between data security and business performance is a tale as old as business itself. After all, the very simplest form of competitive edge is a business' ability to keep its "secret sauce"—be it a proprietary process, critical intellectual property, or even a literal recipe—off the streets.

But today, the issue is infinitely more complex. It's estimated that 90 percent of the world's data was created in just two years.[1] To compound that effect, the proliferation of mobile devices, far-flung client and contractor relationships, remote and roaming employees, and more means that data is stored and accessed in more places, by more people—at any time.

On the heels of this shift in data's role in the workplace, high-profile data breaches have helped make a new business case for data security. The financial impact is one factor, of course; the average cost of a data breach is $3.26M.[2] But, in less cut-and-dried terms, data security incidents can do critical damage to a company's brand and the trust of its customers.

Heavily regulated industries such as healthcare and financial services have long been under a legal mandate to secure sensitive data. More recently, however, heightened public scrutiny and awareness of data security has helped to spur new legislation targeting how businesses can collect, process, and store data. Malaysia's Personal Data Protection Act, the EU's General Data Protection Regulation, the Australian Privacy Principles, California's Consumer Privacy Act—the list goes on. And it's enough to make any organization—whether it's subject to current regulations or not—think critically about data protection.

$3.26 Million

Average cost of a data breach[2]

2,600-10,000

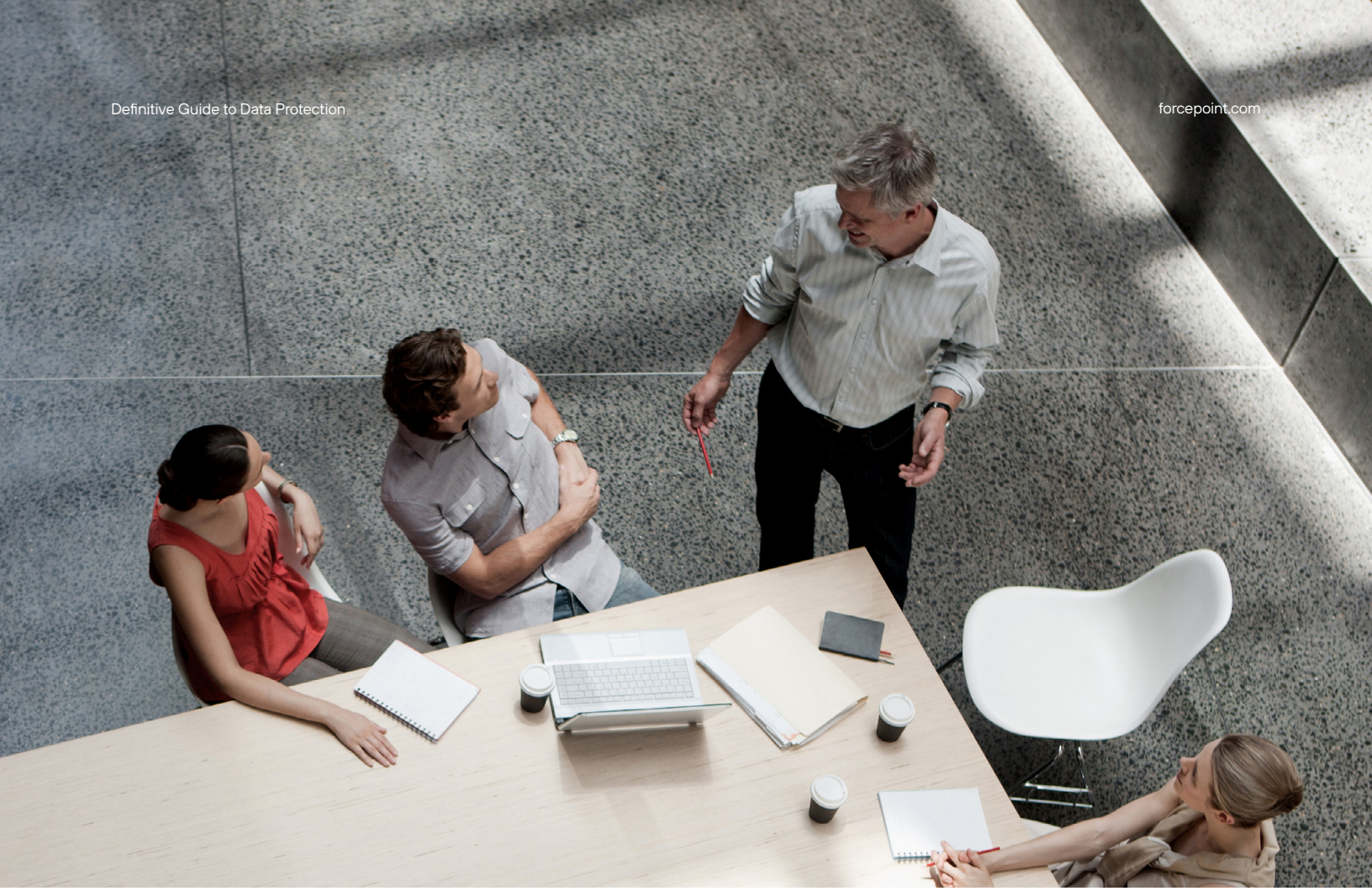
Number of sensitive records lost in an average breach[2]

68%

Percentage of data breaches that go undiscovered for months[2]

Amid all this, one thing has become clear: Empowering companies and employees to perform in today's business environment demands a shift in how we think about data security. In the constant state of change that has become our new normal, reactive policies are no longer enough to keep us safe. Let's explore how to take a proactive stance on data protection—and why it's the safe choice for businesses today.

It's estimated that 90 percent of the world's data was created in just two years.[1]



Elevating the Role of Data Security

For many data security teams, days consist of cycles of receiving an alert, investigating it, and repairing the damage. Rinse and repeat. The problem? Inflexible policies frequently flag low-risk activity, resulting in "false positive" alerts. Investigating these places an immense burden on data security teams who already have more tasks and responsibilities on their plates than they have the bandwidth to fulfil.

Data protection technology that can read into the context surrounding cyber activity can lessen this burden for data security teams, helping them to focus their investigations on incidents which are truly threatening and filter out those that don't pose a real risk to the business. And, by prioritizing their time more judiciously, this allows a security team to evolve its role within an organization from one that simply enforces rules to one that proactively leads the business forward toward a safer, more efficient future.

Empowering Professional Growth

Data security experts who are not overrun with false alerts have the ability to coach and mentor other employees, contributing to their professional development and career trajectories.

Empowering Business Growth

Security professionals who are able to find efficiencies in their own workloads can help pinpoint opportunities for the business to grow through smarter usage of data. (Or, raise flags about data behaviors that may impede business growth.)

Empowering Digital Transformation

Streamlining investigations based on contextual understanding of data incidents allows teams time to optimize their policies and procedures to suit a cloud-powered data culture—enabling faster digital transformation and competitive advantage for the business.

Protecting Data Everywhere Work Happens

Traditional data loss prevention safeguards data at three access points: on your network, at endpoints, and increasingly, in the cloud. And that might be enough—if the people accessing that data stay within those perimeters. But increasingly, they don't, and as soon as the perimeter is crossed, its data protection policies break. That means it's no longer enough to color inside the lines. Let's examine what can be done to work past this.

Implications of Cloud Transformation

Cloud migration isn't a question of "if." It's a question of "when." The demands of remote workforces, customers, and strategic partners only accelerate the timeline, pushing for more rapid cloud adoption. One example? Eighty-seven percent of companies today rely on employees accessing mobile business apps from their personal smartphones[3] —referred to as bring-your-own-device or BYOD. Additionally, nearly a quarter of Millennial workers say they have downloaded company files to those devices and installed third-party cloud applications (bring-your-own-cloud or BYOC) without notifying IT or executive leadership. These behaviors create what's known as shadow IT, and they demonstrate that a business is not always in control of when and how they move to the cloud. But whatever the pace, entrenched security policies struggle to match it as they adapt to meet new demands.

One reason is that cloud application providers tend to prioritize portability, accessibility, and ease of use—not necessarily the security of the data that's being made portable, accessible, or easy to use. They focus on a shared responsibility model in which they secure the infrastructure, but leave customers to secure data shared in the infrastructure. That means that, given the transitional, mobile nature of work today, it falls to you to build data protection that goes wherever your people do.

Humans Are the New Perimeter

How can you keep data secure when the people using it cross your lines of defense? It calls for a new perimeter: humans themselves.

Human-centric data protection allows data to be held in a secure environment which people can access from wherever they work. Plus, linking data security to a person's identity allows for policies that take personal risk level into account, providing insight into intent—for instance, an incident involving a trusted long-term employee may be much less cause for concern than one involving a shady vendor or disgruntled ex-employee. Finally, monitoring for data security at the human level provides visibility into how they use it across different devices and applications, providing context that can help security teams better identify threats and learn from them.

Making the Business Case for Data Protection

Human-centric data protection is well-suited to the dynamic reality of businesses today—but, just how much is it worth to yours? To answer this question, let's debunk the myth that plagues data security teams everywhere: that protection is the enemy of productivity. With the right tools and processes in place, each can empower the other.

Specific Responses

Traditional data loss prevention tactics may simply block risky actions—say, a sensitive company file being saved to a personal flash drive. And, if such an action were taken by a disgruntled ex-employee or a short-term contractor, that response makes sense. More often than not, however, this isn't the case; It may be a company executive simply trying to back up an important file or move it to a new computer. But traditional data security policies can't tell the difference, so they routinely blanket-block totally innocuous cyber activity—impeding company productivity in the process.

Detecting risks at the human level makes it possible to consider the context and intent behind an action, enabling specific—not blanket—security responses. Not only does this reduce interruptions to employees' workflows, but it also lessens the investigation burden on security teams, allowing them to aid progress rather than blockade it.

Reduced Vulnerability

Even an employee with no ill intent may become frustrated with blanket security policies that stand in the way of getting work done. So (still with no ill intent) they may try to find a workaround, bending the rules ever so slightly so they can get past the security blockade. In the last example, perhaps they'd break the file into smaller segments and email them to a personal computer so they can be saved to the drive after all.

This creates two problems. First, this sequence of actions may raise an even more urgent alarm than an attempt to save a file to a removable drive, because it indicates that a person is trying to circumvent security measures. It will likely need to be investigated, which takes time and resources. But perhaps more concerning is that workarounds like these, innocent though they may be, can introduce new vulnerabilities that undermine the security policies that prompted them in the first place. Human-centric data protection would allow for more flexible, appropriate policies, stopping this downward spiral before it starts.

Proactive Stance

As any teacher, pet owner, or data security professional can attest, preventing a "mess" from being made in the first place is much more efficient than clearing it up after the fact.

With the contextual clues and behavioral insights that human-centric data provides, it is possible to halt true threats before they inflict damage, while still allowing the business to perform at the highest level. Employees can go about their days without tripping over inflexible security policies. Busy data security teams can accurately triage alerts and focus on resolving incidents that pose real risk. It's data security—without compromise.

The New Standard for Data Protection

The evolving nature of security threats means we need to adjust our mindset for keeping data safe—and that includes accepting that change is, and will always be, constant. That's why our core principles for data protection are built with the needs of tomorrow in mind:

1. A preventive, not punitive, culture of data security
The role of data security teams will grow from retroactively enforcing security policies to leading their organizations and fellow employees toward safer data usage behaviors.

2. Human-centric risk assessment
Mobile and dynamic data usage demands security that accounts for the only constant: the user. This allows flexible security that adapts as a person's behavior and risk level changes.

3. Holistic view of data
Maintaining full visibility into data as it moves outside your network, across endpoints, or into the cloud gives contextual clues into intent, helping to inform fitting security responses.

4. Consistent policies regardless of environment
Establishing your security perimeter at the human level ensures that data is protected no matter where it's stored or accessed.

Are you ready for what's next on the journey to proactive data protection?

› **Check out our infographic,** 9 Steps to Success with Data Protection.

1. IBM Marketing Cloud, "10 Key Marketing Trends for 2017"
2. Ponemon Institute, "U.S. Cost of a Data Breach Study," 2017
3. Syntonic, "BYOD Usage in the Enterprise," 2016

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.