Freeform Dynamics in association with CERTES

The risk mitigation imperative

Looking beyond traditional data protection to limit exposure and reduce executive liability

Time to rethink what data protection means

If your organization is like most others, you've invested heavily in securing your infrastructure. Your networks are monitored, your endpoints protected, and your cloud environments configured according to best practice. Yet when sensitive data moves between systems, cloud services and business partners, the security controls safeguarding it in one environment don't automatically transfer to the next - even though your liability does. Indeed, you remain liable wherever and however the data moves during its lifetime, including those moments when it's in transit across connections that no-one really controls.

Organizations vary wildly in the degree to which they recognize and address the challenge of protecting data as it moves around distributed systems and out into the wider world. Only you can say how confident you are in the measures you have in place to deal with the risks in this area. However, when considering this, it's worth bearing in mind that the security tools and frameworks you rely on were probably designed primarily to protect infrastructure and control access.

All of this matters because regulators don't distinguish between infrastructure breaches and data breaches - they care that you held sensitive information and lost control of it The same is true of customers, suppliers and other trading partners to whom you have a contractual obligation to protect the data they share with you, whether regulated or not.

Against this background, the paper explores a growing shift in focus from infrastructure security to data protection, and what this means in practical terms. As part of this, it examines a fundamentally different approach to protecting data as it moves across the distributed environments that define modern business operations.

Who is this paper for?

This paper is for senior professionals grappling with data protection accountability in distributed environments - whether you're responsible for regulatory compliance, security strategy, risk management, or service delivery. If you're being asked to demonstrate continuous control over data as it moves across systems you don't fully control, or if you're concerned about liability when acting as a data processor for customer information, this document addresses your challenges directly.

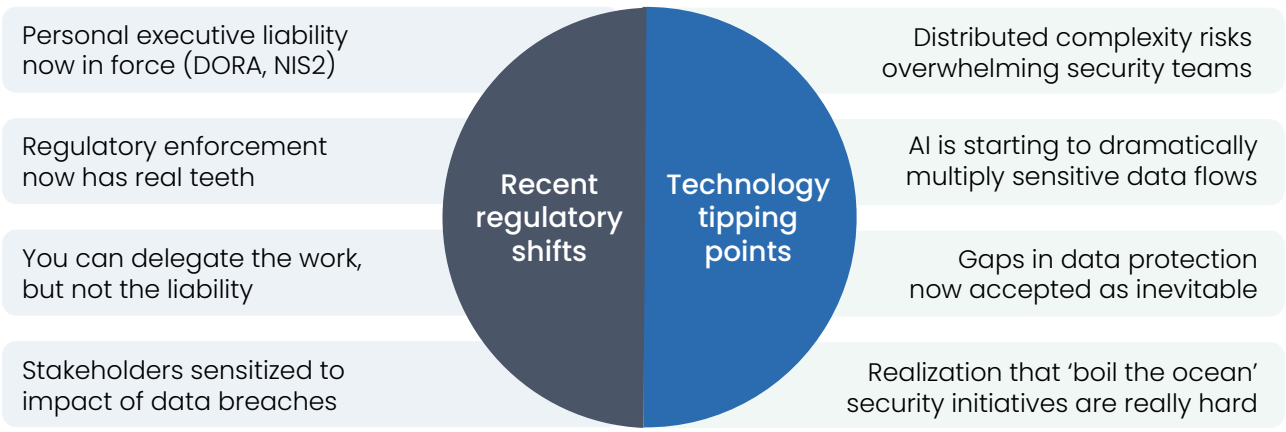
Why this conversation and why now?

Data protection isn't a new topic, but several forces have converged to make this discussion particularly pressing right now. To start with, there's the sheer scale and complexity of modern IT environments, in which data flows have multiplied in two directions. Internally, information moves constantly between applications, platforms and cloud services - crossing boundaries that may have very different security controls. Externally, data flows to and from partners, customers and service providers. The internal dimension affects every organization. The external dimension varies depending on how you operate. Both create exposure that traditional perimeter-focused security wasn't designed to address.

At the same time, the regulatory landscape has shifted decisively. Frameworks like DORA and NIS2 have extended personal liability for data protection directly to board members in some sectors. GDPR enforcement has matured from early warnings to fines measured in hundreds of millions. The direction of travel is unmistakable.

Where these two forces meet is the accountability question. Your data now moves constantly across systems and environments you don't fully control - yet regulators are making it increasingly clear that you can delegate the work, but not the liability. Wherever your data travels and however it gets there, you remain on the hook.

Events and developments conspiring to create a strategic challenge that impacts all parts of the business



What about existing investments and initiatives?

If you're thinking that network encryption, VPNs or secure tunnelling already have this covered, it's worth noting that these technologies protect connections, not the data itself. And while frameworks like SASE and zero trust offer a more comprehensive vision, they're notoriously difficult to implement at scale - which is why so many initiatives stall, get scaled back, or become quietly abandoned. The uncomfortable truth is that despite significant investment and effort, most organizations still have significant gaps in how they protect data as it moves around.

But before we get into the technology side of things, let's step back and look at who's actually on the hook when data protection falls short.

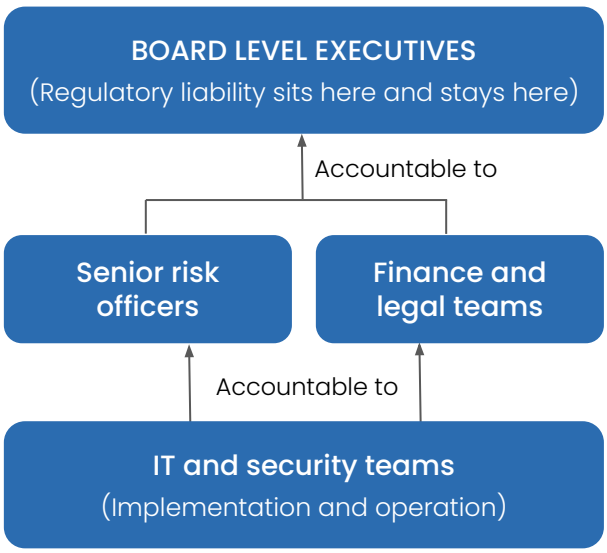
Who is on the hook for what nowadays?

It used to be the case that matters of data-related risk were routinely delegated to IT and security teams. But this is no longer sensible or practical. Most data is actually owned by the business, not IT, so technical teams shouldn't be making decisions on access and retention policies without clear business direction. Meanwhile, business data now frequently moves outside IT's visibility and control - through business units making their own SaaS arrangements, or sending data to partners and agencies. Even when IT is driving, keeping on top of a data estate spanning multiple on-premises and cloud environments has become progressively harder. So who is now responsible for what?

The internal picture

Within your organization, accountability flows upward while responsibility for implementation flows downward. This is probably familiar to you and likely how things work in your organization.

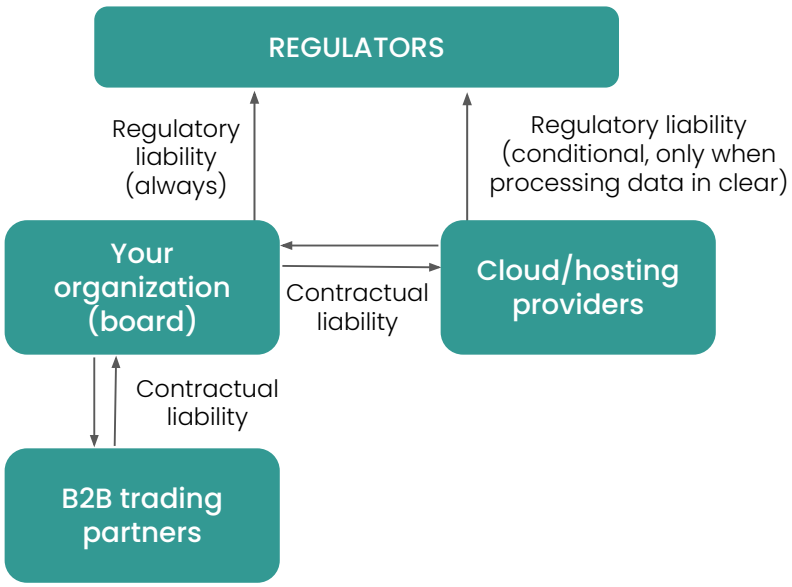
Board-level executives carry ultimate regulatory liability for data protection. This cannot be delegated away - it stays with them regardless of how the organization is structured. Senior risk officers typically own strategy and direction. Finance and legal teams handle compliance frameworks and contractual matters. IT and security teams take care of implementation and day-to-day operation.



Each group is internally accountable to those above them, but none of them - except the board - carry personal regulatory liability. When a regulator investigates a breach, they're looking at the top of the organization, not the people who configured the firewall.

The external picture

External relationships involve a mix of regulatory and contractual liability. Agreements in place with suppliers, customers, agents, service providers and other business/trading partners, for example, typically include data protection, confidentiality and duty-of-care clauses, along with terms relating to indemnities and penalties. It's critical to understand these when considering overall data risk and protection requirements.

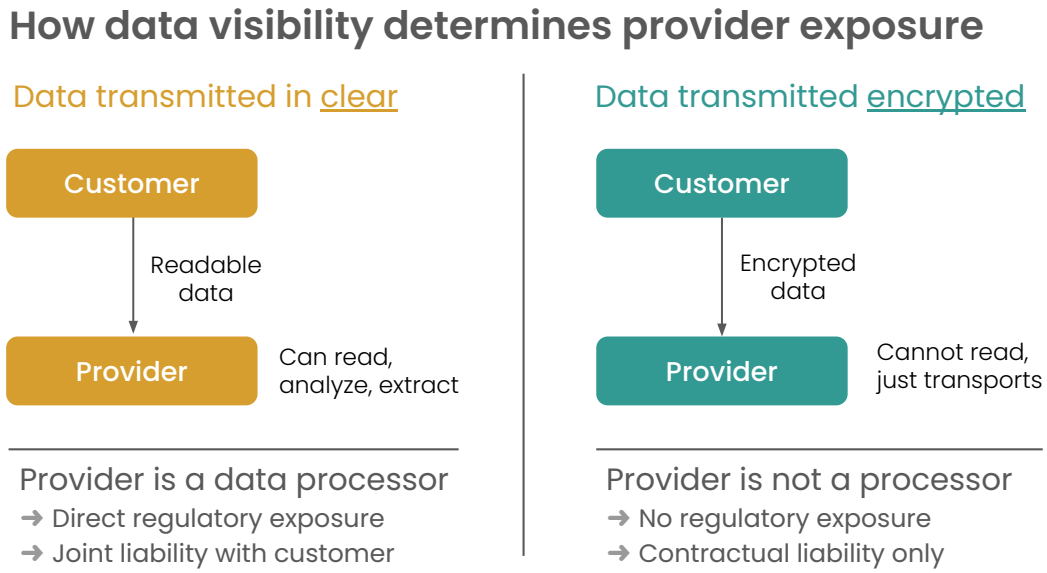


When others handle your data

The relationship between service providers and their customers in the context of data related risk and liability is a common cause of uncertainty and confusion, so let's clear up some common misunderstandings in this area.

For customers, we've said it before, but it's important enough to repeat - engaging a cloud service provider, hosting company, or some other third party to take care of all of the hard and complicated security stuff for you doesn't mean that you have transferred your obligations and liabilities. If a service provider who is handling your data screws up, and a breach or leak occurs, it's still you (specifically your board members) that regulators or injured parties will come for.

However, for service providers reading this, it's important to recognize that you're not automatically exempt from regulatory liability - it depends on your role in the data processing chain.



Why this matters

For providers, the implication is straightforward - if you can see customer data in the clear, your regulatory exposure may be significantly higher than you realize. Many providers have inadvertently taken on processor liability simply by having visibility into customer data flows.

For customers, the picture is more nuanced. Your regulatory liability doesn't change based on what your provider can or can't view - you're accountable either way. But your actual risk does change. If your provider never sees data in the clear, they can't leak it, lose it, or be hacked for it. A security breach at the provider therefore doesn't become a data breach for you. Due diligence becomes simpler too - their internal data handling practices matter far less when all they're transporting is ciphertext they can't read.

The upshot is that both parties benefit when data remains encrypted throughout its journey - providers reduce their regulatory exposure, and customers reduce the likelihood of a breach occurring in the first place.

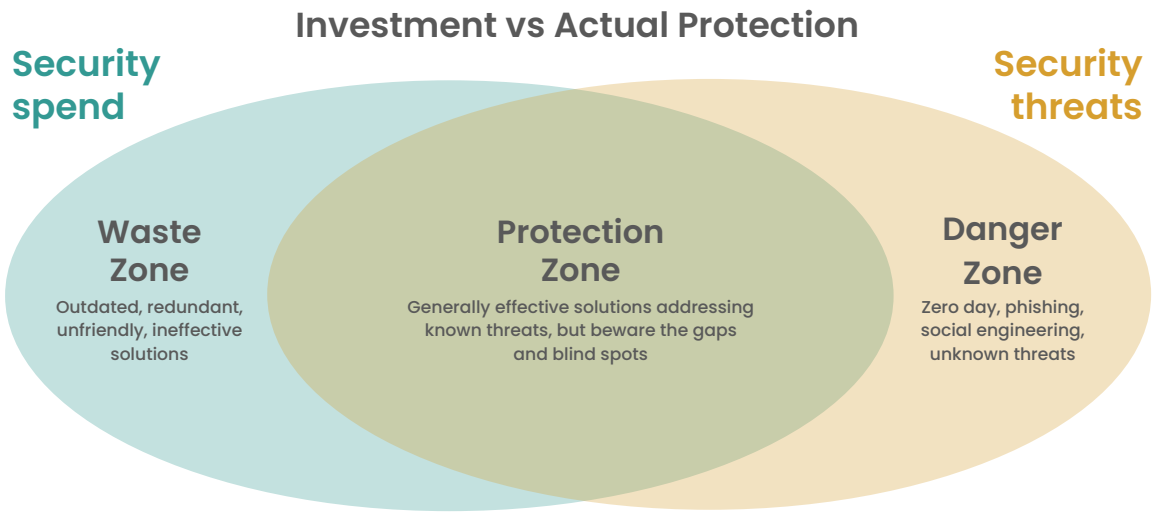
With this in mind - and remembering that internal system-to-system data flows present risks for every organization - let's turn to the realities of most current security landscapes, and explore how a more data-centric approach can dramatically reduce risk exposure.

Time for a reality check

If you were to draw a diagram of your security infrastructure - capturing all the hardware and software components and how they relate to each other - two things would immediately leap out. First, the sheer complexity. Second, the number of moving parts.

Now imagine mapping onto that diagram the threats and risks your infrastructure is intended to protect you against. Would you end up with a clear view of what's protected and what's vulnerable? Probably not. Even if you succeeded, the picture would likely be out of date within weeks.

Add to this the fact that no matter how much you spend on security infrastructure, it's impossible to completely protect your environment. To one degree or another, you will still be vulnerable to zero day exploits, phishing and other social engineering attacks, plus don't forget user and admin error. One way to look at this is to consider the actual level of protection all that money has bought.



Some might regard this as an exaggerated view, and to be fair the overlap between spend and threats has been set arbitrarily for illustration purposes. That said, it's not uncommon for security teams to overestimate the efficiency and effectiveness of their security infrastructure, not least because there's a tendency to focus on the threats you know you can address with the tools available. Conversely, the threats we think we can do little about often get downplayed.

Looking for answers

Over recent years, frameworks like Secure Access Service Edge - commonly known as SASE - and zero trust architectures have promised a more comprehensive answer. The vision is appealing. Verify everything, trust nothing, apply consistent policy everywhere. But the reality of implementing these frameworks has proved challenging. They require fundamental changes to network architecture, identity systems and operational processes. Many organizations that started down this path have found initiatives stalling, budgets expanding, and timelines stretching indefinitely. Quite a few have quietly abandoned their efforts altogether.

Meanwhile, some argue that we need to extend our approach beyond investing in yet more security infrastructure aimed at preventing intrusion. Necessary though this is, adding more direct focus on protecting the data itself can allow us to think differently about how we manage data-related risk.

A different starting point

Acknowledging that attackers will find a way in no matter how much you invest in security is the basis of the "assume breach" principle that underpins modern security thinking. If you accept that intrusion is a matter of when rather than if, then containment becomes just as important as prevention. One way to do this is to ensure that any data the attackers find is worthless to them.

Protection that travels with the data

When considering data protection, encryption is usually the first thing that comes to mind, particularly data at rest - e.g. encrypted databases, encrypted storage, and encrypted backups.

However, data is often most vulnerable when it's moving between systems, passing through networks where malicious agents using compromised credentials are sitting and watching. Traditional approaches like VPN tunnels protect connections, but once inside the network, data often moves in the clear between applications and services. Of course, there are plenty of approaches that go beyond basic VPN tunnels, including microsegmentation, zero trust architectures and encrypted service-to-service connections. But largely speaking, protection remains tied to infrastructure and access controls. If credentials are compromised, or data moves beyond the protected environment, the data itself remains exposed.

This brings us to the notion of protection travelling with the data. Encrypt at source, maintain that encryption throughout the journey, and only decrypt when the data arrives where it's supposed to be. Anyone who intercepts it along the way sees nothing they can use.

What to look for

Solutions that address data-in-motion protection have been around for a while, including dedicated hardware appliances. But software-based approaches bring some real advantages - they can be deployed incrementally, scale across hybrid environments, and adapt as your architecture evolves without requiring infrastructure replacement.

Attributes of a modern software-defined solution

Encryption that persists
Protection that remains in place wherever and however data travels, whether it's movement between internal and/or external systems or escape of data out into the big wide world.

Customer-controlled keys
You hold the encryption keys, not your cloud provider or security vendor. This limits your overall exposure and avoids the complication of providers becoming data processors.

Policy-driven controls
Central definition of who can read what data, with consistent enforcement across all environments, including those you don't control or aren't currently even aware of.

Operational simplicity
A software-defined approach that allows non-disruptive deployment based on your risk priorities, with incremental adjustment and refinement of protection as things change.

Complementary capability
Works alongside your current security tools, network monitoring and operational processes, enhancing protection while preserving the value of existing investments.

Visibility and auditability
Doesn't blind security and network monitoring tools. You can still see/optimize traffic patterns and detect threats, while maintaining a definitive record of what's protected over time.

It's also worth considering the future arrival of Quantum Computing, which may not be for a while, but when it does get here it will render most current encryption techniques ineffective. Beware that some attackers are collecting encrypted data today on the basis that they will be able to decrypt it down the line. Security vendors are increasingly introducing 'Quantum Safe' solutions to future-proof protection. One of these is Certes, which we will use as a worked example.

Certes: a worked example

Having explored the principles and challenges of protecting data-in-motion, let's look at how these concepts translate into practical reality. To do this, we'll use Certes, an established player in this area, to illustrate what a modern data-centric protection solution looks like.

Please be aware that the solution details presented here are based on information provided by Certes and conversations with its team. Our aim is to help you understand how data-in-motion protection principles can be implemented, not to provide a formal solution assessment.

Background and philosophy

Certes has been around for over 20 years, though you'd be forgiven for not having heard of it. As a senior member of the executive team put it: "Historically, we've largely worked with governments, public sector and three-letter agencies", which explains the relative lack of visibility. More recently, though, the company has moved more into the mainstream enterprise space in response to data-related risk and regulatory liability receiving significantly more attention.

The company name is an anagram of "secret," which hints at its origins and focus. But what's interesting about Certes' current positioning is how firmly it regards data protection as a business risk issue rather than a purely technical one. It's core philosophy can be summed up in a phrase it returns to repeatedly: "You cannot fix a data problem with a pure infrastructure approach."

The "DPRM" proposition

Certes packages its approach under the banner of DPRM, which stands for Data Protection and Risk Mitigation. The framing is deliberate. Rather than positioning this as another security technology, Certes is all about trying to drive more purposeful conversations.

Understanding DPRM

DPRM (Data Protection and Risk Mitigation) is a term coined by Certes to describe its approach to dealing with data-in-motion risk. Traditional security tools aim to prevent breaches from occurring. DPRM accepts that breaches will happen and focuses on eliminating harmful outcomes by ensuring any data intercepted or exfiltrated remains encrypted and inaccessible.

If attackers can only access data they cannot read, regulators may not classify this as a reportable breach. No exposed data means no notification obligations, no regulatory fines, and nothing for attackers to exploit. Hence the risk mitigation aspect. In this sense, DPRM addresses a specific slice of organizational risk - the financial, legal, and reputational exposure that arises when unprotected data falls into the wrong hands.

However, despite the business focus, this proposition is backed by some proven patented technology. Let's take a closer look.

The technology behind DPRM

Encrypting data-in-motion isn't new. But a lot of traditional approaches have struggled with two significant limitations:

> **Visibility:** Most encryption wraps entire network packets in encrypted tunnels. This protects the data, but blinds your monitoring and security tools to what's happening on the network. You've secured the data at the cost of operational visibility.
>
> **Scalability:** Encryption has historically been complex and expensive to deploy, so it gets reserved for the most sensitive data flows. Everything else travels unprotected.

Certes claims to have solved both problems through a patented approach that operates at Layer 4 of the network stack. Rather than encrypting entire packets, it encrypts only the data payload while preserving the original packet headers. Network monitoring tools, security infrastructure, and operational processes continue to function exactly as before. The network stays transparent while the data itself is protected.

The move to a software-based model has also changed the economics. Protection can now be applied across the entire environment - data centers, cloud platforms, endpoints - without the cost constraints of dedicated hardware. Add in customer-controlled encryption keys and you have the basis of a solution where protection genuinely travels with the data, under your control, wherever it goes. Certes summarizes it as follows:

Key components of DPRM

Crypto segmentation

Logically segments individual data flows through separate policies and strong cryptography, ensuring data sovereignty, irrespective of physical geographic limits, using high-grade encryption.

L4 data payload protection

Safeguards the actual data, regardless of the infrastructure it traverses. Different from L3 as it means all visibility, monitoring and optimization tools still work.

Customer controlled key management

Encryption keys reside solely with the customer or data controller instead of a vendor or service provider. Significantly reduces the chances of data breach or leakage.

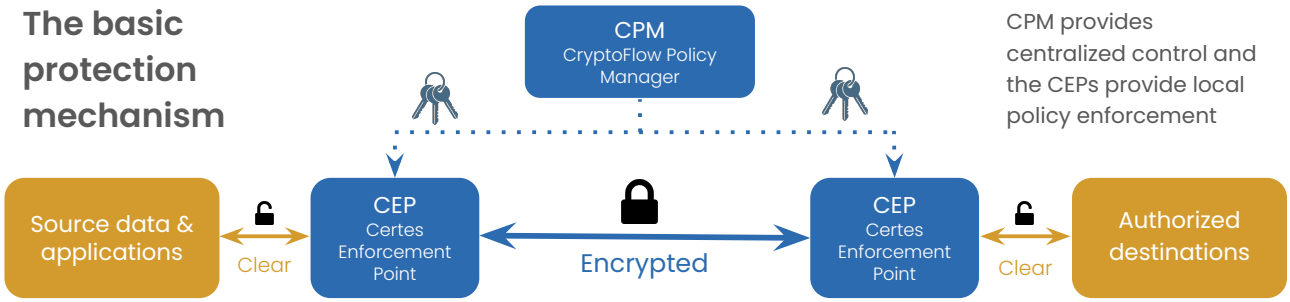
Data security unified reporting

Provides a clear view of protected, blocked and allowed data flows as proof points for audit and record-keeping. Particularly useful for resolving disputes between parties when breaches occur.

These principles are delivered through a straightforward architecture. Policies and encryption keys are managed centrally, then pushed out to enforcement points deployed across your environment. Let's look at how the pieces fit together.

A peek at the Certes architecture

The Certes architecture has two main components. A central control node (the CPM), which handles policy definition and key management, and multiple enforcement points (CEPs) that are distributed across your environment to apply the actual protection. Basically, CEPs sit in front of each important data source (e.g. your HR system) and authorized destination (e.g. your HR team) and make sure all of the data flowing between them is encrypted.



Depicted in this way, you can see that the basic idea is very straightforward, but it's worth talking through some of the specifics in a bit more detail to get a better feel for the practicalities.

Central control

The CPM (CryptoFlow Policy Manager) is where policies are defined and managed. Using a drag-and-drop interface, administrators specify which data flows to protect (based on source and destination), what encryption to apply, and who should have access. The CPM then generates the necessary keys and pushes policies out to enforcement points across the network. Key rotation happens automatically at scheduled intervals, without manual intervention.

The centralized model means you can define policy once and enforce it everywhere. Add a new application or data flow, update the policy in the CPM, and it propagates automatically. This is how Certes delivers the "policy-driven controls" we mentioned earlier.

Distributed enforcement

CEPs (Certes Enforcement Points) sit close to the data sources and destinations, applying encryption before data hits the network. The further upstream you can place them, the less exposure you have. Ideally, data is protected before it leaves the application server and only decrypted when it reaches its authorized destination. A range of CEP variants help with this.

Types of CEP

Physical appliances for data centers and high-throughput requirements
Virtual appliances (vCEP) for virtualized environments
Cloud-native versions (cCEP) purpose-built for platforms like AWS
Endpoint agents (eCEP) for laptops, workstations and distributed devices

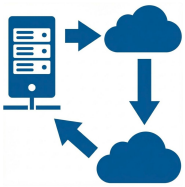
This flexibility means protection can extend from the data center to the cloud to individual endpoints, all managed through the same central console. Let's explore some common deployment scenarios to get more of a feel for what can be achieved.

Some common deployment scenarios

The architectural flexibility we've just explored allows straightforward deployment across a range of scenarios. Let's look at a few common situations and how organizations typically address them.

Hybrid and multi-cloud environments

One of the significant advantages of a software-based approach is that it overlays onto existing hybrid and multi-cloud infrastructures without requiring changes to applications or network architecture. Virtual or cloud-native CEPs sit within each environment, encrypting data as it leaves one location and only decrypting it when it reaches the authorized destination.



Cloud migrations

When pulling apart existing application dependencies and moving components to the cloud in phases, CEPs can protect the data flows between the parts that have moved and those that haven't. This provides protection during transition periods when your architecture is inevitably more fragmented and exposed. The same CEPs remain in place once the migration completes.

Distributed workforces

Endpoint agents (eCEP) installed on laptops and workstations apply encryption before data leaves the device and maintain protection until it reaches its destination. Protection doesn't depend on VPN tunnels or network controls. A sales team member accessing customer data from a hotel connection has the same cryptographic protection as someone in the office.

IT and operational technology separation

Physical or virtual CEPs create a cryptographic boundary between IT and OT environments, allowing specific data flows while preventing lateral movement. An IT system can send production schedules to the OT environment, but any attempt to access other OT systems fails because the encryption keys and policies don't permit it. This addresses the regulatory need for isolation.

IoT and edge devices

The software-based endpoint model makes it economically viable to protect distributed devices that were previously difficult to secure. ATMs, payment kiosks, sensors, and other edge devices can now have data-in-motion protection without requiring dedicated hardware at each location. This extends consistent policy enforcement to the edges of your infrastructure.

Most organizations don't attempt to protect everything at once. The typical approach is to identify the highest-risk data flows - perhaps financial data moving to cloud services, or customer records accessed by remote workers - deploy CEPs to protect those, then expand coverage based on priorities and compliance requirements. Because DPRM is essentially an overlay on existing infrastructure you can deploy incrementally, at your own pace, without major disruption.

Beyond specific technologies

Having looked at Certes as a worked example of how the latest generation of data-in-motion protection can be implemented, it's worth stepping back to look at the bigger picture. While players like Certes clearly offer some very capable technology, it's important to recognize there are no magic bullets or certainties in this whole space.

Acknowledging the game we are playing

Fundamentally, when it comes to security and data protection, we are all playing a probability game. The objective is not to achieve 100% protection - that would be totally unrealistic - but to reduce the chances of an attack or mistake causing business harm and/or regulatory exposure.

With this in mind, it's necessary to blend the right mix of ideas and technologies, with each one stacking the odds a little more in your favour. For example, effective identity and access makes it less likely that an intrusion will occur, but if an attacker does get in, the DPRM approach lowers the chances of real data damage being caused.

A word for practitioners

It's easy to become wedded to particular solutions and ways of thinking. When you've built expertise in certain tools and frameworks, there's a natural tendency to frame every problem in terms you know how to deal with. The flip side is avoiding problems you don't think can be solved - why waste time on them when you can focus on the stuff that works?

The trick is to stay current on technology developments, new ideas, evolving threats, and changing regulations, with a watchful eye on how business needs are changing. What worked three years ago might not fit today's distributed, cloud-heavy, AI-driven environment. Acting purposefully while keeping higher-level objectives and imperatives in mind means regularly questioning whether your current approach and scope of consideration still serves those goals.

A good example here is quantum computing. While practical quantum computers are still some years away, threat actors are already harvesting encrypted data with the intention of decrypting it later once quantum capabilities mature. Worth keeping an eye on, particularly if you handle data with a long shelf life.

A word for executives

Delegation is necessary, but "delegate and forget" doesn't work for data protection anymore. Personal liability frameworks like DORA and NIS2 have made that clear. You need to listen and learn, help security and data protection teams understand what you need or expect, then be willing to discuss their input and take their questions seriously.

One specific point worth emphasizing - it's rarely a good idea to starve teams of budget for investments in technology, training and investigation of new methods, then expect them to keep pace with evolving threats. If money is tight, by all means press teams on waste. Ask whether all the technology in place is earning its keep from a time and maintenance perspective. You too need to stay focused on higher level objectives, weighing costs against confidence and peace of mind.

Key imperatives

As you continue to develop and invest in security and data protection measures, we'd highlight three key imperatives. You may already have these covered - if so, just take them as a reminder or checklist for your next strategic review. However, if you know you need to improve, we strongly suggest prioritizing the first imperative as so much else stems from this.

1

Achieve organizational alignment

Dedicate time to aligning around priorities and decision-making processes. This means executives becoming more engaged than many have been in the past - not micromanaging technical decisions, but understanding enough to ask the right questions and make informed choices about risk and investment. It also means creating forums where technical teams, risk professionals, and business leaders can have productive conversations about what matters most.

2

Establish ongoing review processes

Put a program of regular reviews in place. This isn't about generating reports nobody reads. It's about looking at the latest threat intelligence, assessing how well current protections are working, identifying gaps, and making pragmatic decisions about where to focus effort. These reviews need to involve both technical depth and business context - what's technically possible needs to meet what's operationally practical and what the business can actually afford.

3

Adopt an assume-breach mindset

Accept that intrusions and user/admin mistakes will happen and shift some focus from preventing them alone to limiting the damage when they occur. This is where approaches like data-centric protection become relevant. If you can't guarantee keeping attackers out or preventing internal incidents, make sure what is stolen or leaked is worthless. This isn't defeatism - it's pragmatism that acknowledges the reality of modern threat landscapes.

Moving forward

The good news is that while the challenges are real, we now have so many insights, tools and approaches to address them. But you do need to be proactive. Whether you work with large vendors with broad portfolios, or explore what specialists have to offer, it's critical to stay on top of the way the security space is continually developing and innovating. The trick is to always keep an open mind, and be particularly receptive to new ways of defining problems and thinking about requirements. Certes reframing the discussion around data rather than infrastructure, and risk mitigation rather than intrusion prevention, is a good example of this. If you want to find out more, check out the links on the last page.

In the meantime, we hope our discussion has helped you evolve your own thinking.

About

Freeform Dynamics

Freeform Dynamics is an IT industry analyst firm. Through our research and insights, we help busy IT and business professionals get up to speed on the latest technology developments and make better-informed investment decisions.

For more information, please visit: www.freeformdynamics.com.

Certes

Headquartered in the U.S. and boasting a global presence spanning Europe, the Middle East, and Asia Pac, Certes has been a pioneer in delivering cutting-edge security technology solutions, with a specific focus on Data Protection Risk Mitigation (DPRM). With over 20 years of expertise, our technology is deployed across a diverse clientele of 1000 customers in almost 100 countries, holding certifications for FIPS 140-2 and CC EAL 4+, with FIPS 140-3 and EU-CC EAL 4+ coming during 2026. Our extensive global footprint includes organizations leveraging Certes technology, facilitating compliance with national, international, or industry-specific regulations through robust DPRM strategies.

For more information, please visit www.certes.ai or check out the following links from the Certes site:

DPRM Overview
https://certes.ai/dprm/

Deploying DPRM
https://certes.ai/dprm-how/

Quantum Readiness Checklist
https://certes.ai/post-quantum-cryptography-download/