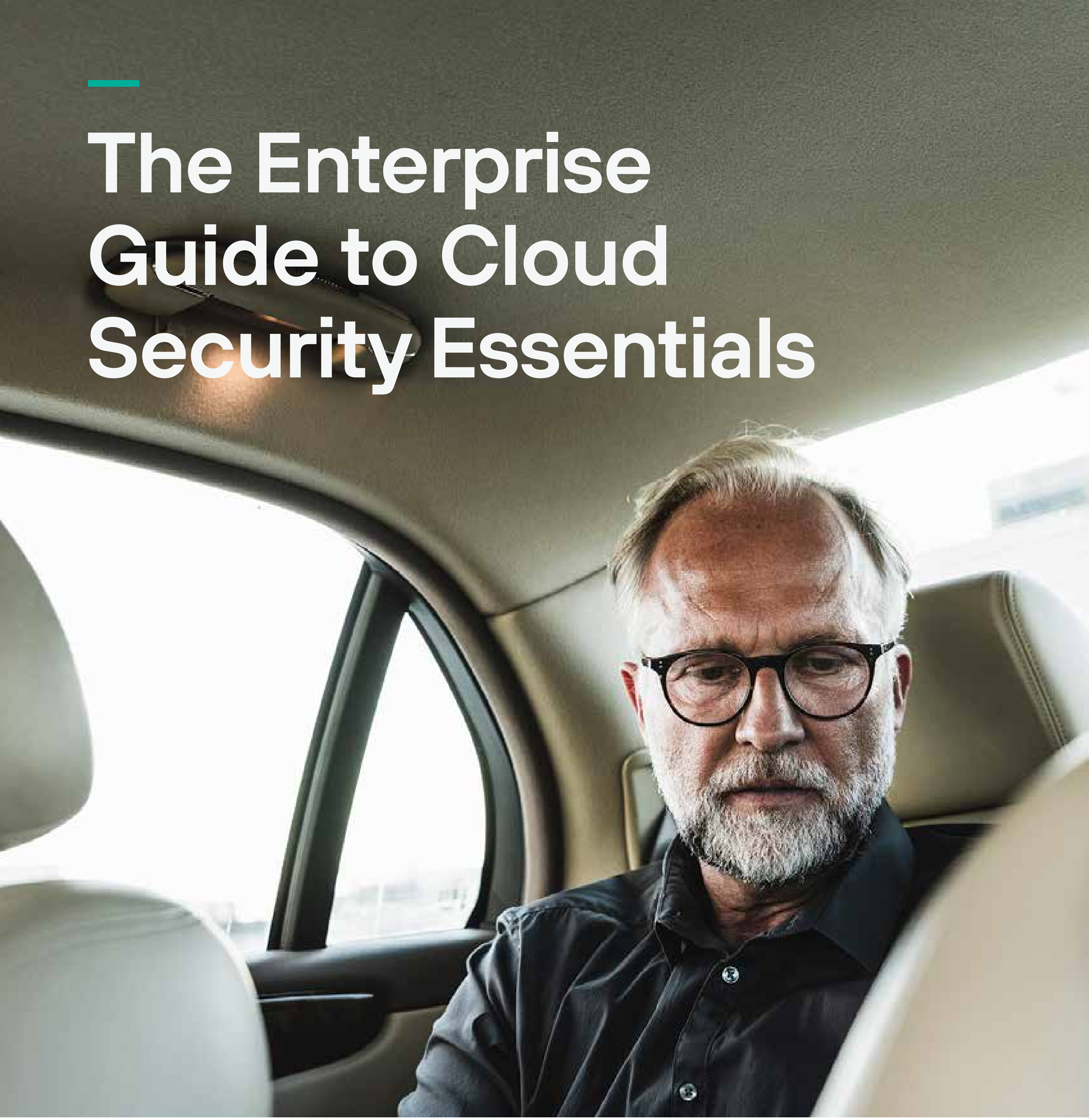
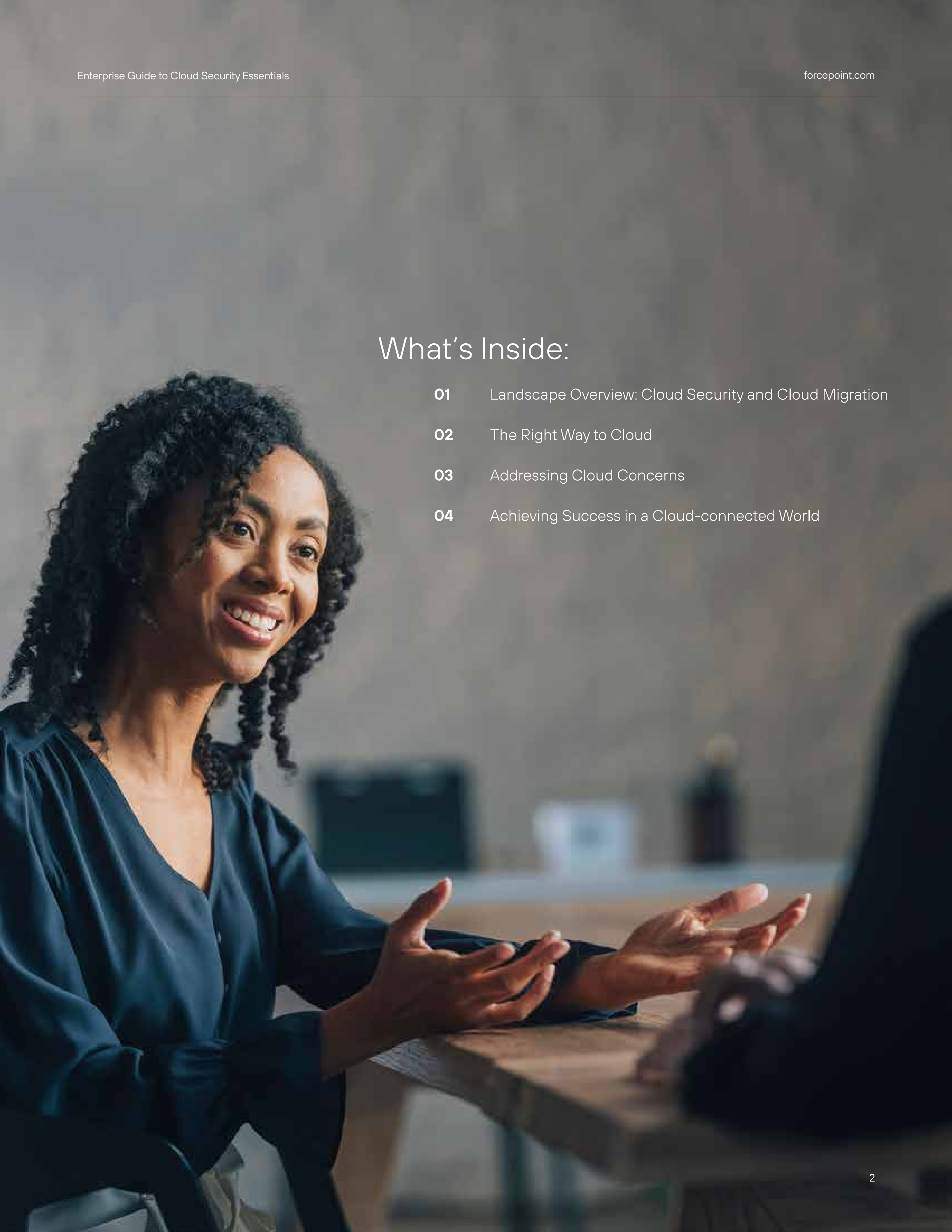
The Enterprise Guide to Cloud Security Essentials



Forcepoint

Brochure



What’s Inside:

Landscape Overview: Cloud Security and Cloud Migration

If it seems to you like cloud is increasingly ubiquitous, well, you're right. But what's driving this fast and furious acceleration of all things cloud? Really, it's consumerism. Yes, the B2C kind.

How people consume cloud every day drives how businesses adopt and secure cloud.

Cloud security is people-driven.

Cloud is instant access.

And cloud is an expectation.

With constant access to content, apps, devices—all seamlessly connected to each other, all the time, without disruption—cloud is an inextricable part of our everyday lives. Deeply woven into the fabric of how the modern person unconsciously functions and operates. So in the workplace, the expectation is the same. You want to use what you need, when you need it. And you want a fluid experience that doesn't hinder your productivity, but instead does the opposite. How do you increase your productivity with cloud? How do you do more with less? Because really, cloud is convenience. But it's also a vulnerability.

Ultimately, workers are consumers. How enterprises secure their organizations, protecting their data and people, needs to match that same expectation and experience we go through every day in our day-to-day. And security needs to evolve to allow for that fluidity while also securing the ever-expanding threat landscape accompanying that freedom and convenience.

This is the general culture of cloud. But what are the specific circumstances that incite action and spur organizations to rethink their approach to cloud and security as a whole? They include:

- The journey of digital transformation, starting with adoption and implementation of O365
- Moving legacy and custom apps to the cloud, like EHR or ERP systems
- People working beyond the confines of an office, off the corporate network or behind other defenses
- Global enterprises operating within and across highly distributed environments, encompassing sites that need the same level of security as HQ—without the need to recreate an expensive, hardware-heavy footprint at each location with backhauled traffic
- Optimization efforts—whether it's consolidating security stacks, streamlining teams' workflows or just reducing CapEx/OpEx
- Moving infrastructure to public clouds like AWS or Azure

The Right Way to Cloud

Cloud security means something different to different people. And it's constantly and rapidly changing. So how do you keep up? How do you ensure your approach is holistic and effective? In order to successfully protect your organization, cloud security needs to be inclusive.

Let's think about the key components of cloud:

Data in the cloud

Users in the cloud

Apps in the cloud

Connectivity in the cloud

Infrastructure in the cloud

Security in the cloud

At its core, this is what cloud security is all about. And all components of the cloud have to be considered, governed, and protected in order to avoid security gaps and keep users and data safe. While cloud security doesn't have one static definition, there is a right way to "cloud."

So, what does this look like?

To protect and connect to the cloud, organizations must:

- Secure access to web content and cloud apps for any user, anywhere, and on any device
- Have visibility and control across the organization to drive cloud security strategy
- Safeguard data as it moves to and from the cloud
- Enable direct-to-cloud connectivity for users and sites without backhauling
- Optimize infrastructure and workflow
- Protect against advanced threats, including zero-day exploits

Great, so now that you know what you have to do, how is it actually achieved? Many organizations might have existing products that can perform some key capabilities, or employ different teams that are responsible for certain elements of cloud security. But what every security organization wants to avoid is overwhelming their already-tapped security teams by implementing multiple point products that aren't integrated and that don't talk to each other.

What organizations truly need is a singular solution—not a concoction of vendor-diverse products. Yes, dependencies do exist—like the need to have visibility in order to have control, or the need to migrate on-premise web security to the cloud in order to protect off-network users. In its optimal state, cloud security is a unified solution wrapped around data, web access, cloud access and cloud data, and connectivity. It serves to alleviate any and all pain points across your security team and avoid security gaps. Whether that's achieved with one vendor or three, enterprises must ensure that what they have, what they want, and where they want to be all align to achieve key business outcomes.

Addressing Cloud Concerns

Moving data to the cloud is a significant undertaking—and if you feel some anxiety about it, you're not alone. How do you maintain ownership and control? How do you continue to keep threats at bay? How do you ensure performance?

Let's resolve some of the most common points in question.

Latency

Coverage is critical to reducing latency. An expansive footprint with abundant PoPs across the globe will deliver low latency as well as other productivity-boosting benefits like content localization. **Tier 1 networks and Tier 4 data centers** helps to ensure a high level of reach, redundancy, connectivity and quality ideal for latency-sensitive applications.

Visibility

You can't protect what you can't see. And you can't make changes or set policy without knowing what it will affect. Pairing a **cloud-delivered web gateway** with a **firewall** offers consistent visibility and enforcement across users and locations, including policy enforcement and control of shadow IT. And **CASB** functionality helps secure enterprises by providing visibility into what users of both sanctioned and unsanctioned apps are doing in the cloud to understand risks and protect users and data.

Compliance

Trust program certifications—not just self-audited compliance. Relevant standards for your organization likely include:

- **ISO 27018**, which governs personally identifiable information (PII)
- **ISO 27001**, a multi-site certification for development, quality assurance, deployment, and support operations
- **CSA**, which governs software security and cross-functional operations in a cloud setting (and is based on the GDPR Code of Conduct)
- **SOC2**, which focuses on non-financial reporting controls relating to security, availability, processing integrity, confidentially and privacy, in addition to data center testing and operational effectiveness

Data Sovereignty

While the cloud itself has no concrete confines, it's not exempt from the legal consequences of geographical borders and boundaries. Digital data is subject to the laws in which that data resides. Utilizing **cloud data centers located in the regions where your enterprise operates** is essential for compliance with local laws and regulations, as well as performance.

Data Loss

A unified approach is the most successful approach. With integrated **data protection solutions**, you can extend your security measures from on-premises to the web, email, endpoint, network and cloud. Leverage your existing policies to protect data at rest in the cloud and data in transit.

BYOD

Today's workforce relies on a multitude of sanctioned and unsanctioned cloud applications, on both managed and unmanaged devices. When securing remote and roaming users, network perimeter defenses and endpoint protection don't cut it. You must distinguish between managed devices and BYOD, using **granular security policies** to give employees the flexibility to use their own devices without presenting additional risk. **Expanded controls** offer security for remote users who use company devices for both work and personal use.

Settling for Good Enough

Eager to become more agile, efficient, etc., companies frequently take a "figure it out later" approach when it comes to the cloud. But just checking the box often sacrifices both security and efficacy. For example, URL filtering alone is not security—the same way a recursive DNS solution is not a replacement for a full web gateway. You can't get full protection with just one element of a solution. Moreover, the bare-minimum approach puts security in a position to have to react, rather than pro-act. Make sure both **security and networking work together and have a seat at the table** as your enterprise creates its roadmap to digital transformation—that way they're working in lockstep with business objectives and can avoid playing catch up.

Achieving Success in a Cloud-connected World

We established at the beginning that cloud security is people-driven. Which is why it must be people-centric.

Thanks to the cloud, **humans are the new perimeter.**

As users, partners, and customers access your enterprise's data from anywhere in the world, the artificial wall that protects the data is no longer enough.

Legacy, infrastructure-centric security that groups trusted users on the inside and untrusted individuals on the outside is no longer relevant.

Inherent trust can't be part of your security stack.

And your security stack is integral—not ancillary—to your digital transformation.

To accelerate and safeguard it, here are some core principles to keep in mind:

Cloud at Your Own Pace
Rome wasn't built in a day. And your cloud migration isn't going to happen overnight. Most enterprises are operating in hybrid IT/multi-cloud environments—and will continue to for the foreseeable future. Ensure your secure web gateway has flexible deployment options that enable you to migrate based on what is right for your organization today, and tomorrow. This will allow you to migrate on your own terms, as you're ready, while maintaining across-the-board security.

Extend Alongside Your Edge
Secure your cloud, network and endpoints to meet your ever-changing business needs. A low-hardware, converged platform with modular security capabilities offers highly distributed organizations the extensibility and agility they need to take advantages of new advances, prevent blind spots and connect across locations—securely and manageably.

Zero Trust, Absolute Insight
"Never trust, always verify" is a key tenant of the Zero Trust framework—meaning the way to protect your organization's data is by evaluating access to that data throughout the user and device interaction. This helps you understand the "who" and "how." Understanding the "why" is what will help you move beyond awareness and into prevention. Layer on behavioral analytics to understand intent.

Are you ready for what's next on the journey to scalable cloud security?

› Check out our ebook, Securing Your Wherever, Whenever Workforce.

forcepoint.com/contact

About Forcepoint

Forcepoint is a strategic cybersecurity partner, entrusted to safeguard organizations while driving digital transformation and growth. Instead of a static one-size-fits-all approach that stifles innovation and creates vulnerabilities, Forcepoint is attuned 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 enterprise and government customers in more than 150 countries.