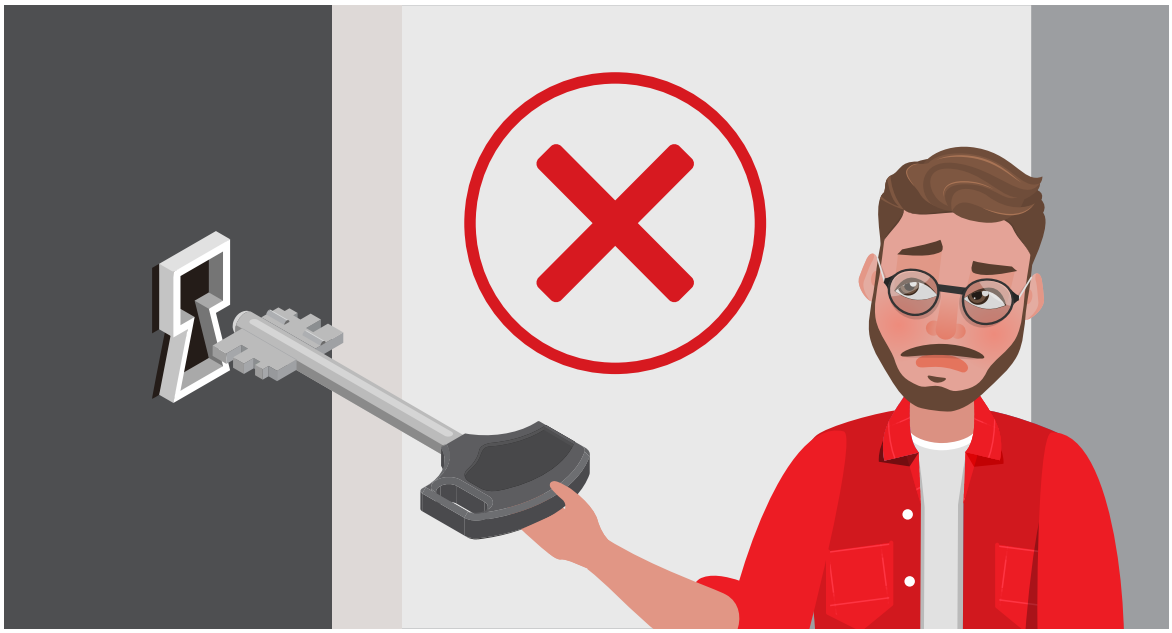
3 Major Benefits of Cloud Migration: Visibility

On the fence about migrating to the cloud because security seems complex and abstract? Let go of your on-premises point products and discover how a platform with enhanced visibility can help smooth out your cloud journey.

Maybe you understand **the importance of migrating** to the cloud, but all the unknowns about cloud security are still making you hesitant. Don't worry, you're not the only one. According to **ISC2**, 94% of organizations are moderately to extremely concerned about cloud security.

While security in the cloud requires a different approach than on-premises, considering there is no perimeter to protect and workloads/apps are dispersed across many different environments, that doesn't mean it's more difficult.

Think of it like this—just because your new home has different locks than your old one, that doesn't mean it's harder to unlock. You just need a different key, or in this case, a different security strategy. And don't try jamming your old key (legacy products) into that lock—82% of respondents in an **ISC2 survey** reported that traditional security solutions don't work at all or have limited functionality in the cloud.



On-premises solutions put a great value into north-south traffic, but traditional methods like firewalls can't always keep up with evolving threats. A firewall, like a motion detector on a door, may alert you to a malicious actor. But being alerted to an intruder is simply not enough to be fully protected. You need security cameras inside to help identify the criminals and their behaviors. In the cloud, visibility on east-west traffic (what's happening within your network), in addition to north-south, is paramount to detecting threat actors before they wreak havoc.

While 52% of organizations in a **SANS survey** reported having high confidence in their visibility of north-south traffic, only 17% said the same about knowing what's happening within their networks.

Let's take a look at how to design your security strategy to maximize cloud visibility so you can minimize vulnerabilities.

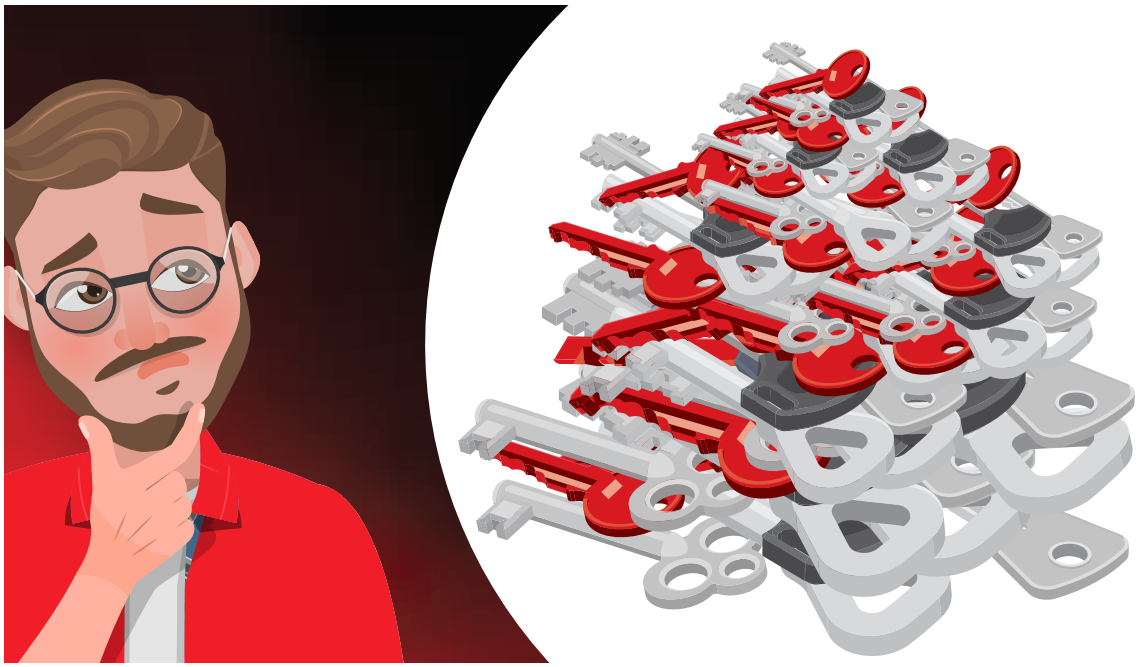
Security by design

The security by design or **DevSecOps approach** enables a smoother on-premises to cloud transition by encouraging collaboration between SecOps and DevOps teams to ensure security from migration to expansion that supports, instead of hinders, innovation.

Security is often an afterthought to the development and migration process. This is like performing a home inspection after you've bought a home without conditions. While you can fix the issues you find, you are incurring a lot of financial risk by purchasing the unknown. Similarly, developers will deploy with security as an afterthought—which leads to security teams using various point products (**108 on average**) to manage vulnerabilities to avoid data breaches or hefty compliance fines.

Encouraging more transparency and communication between teams means choosing a cloud security solution that meets the needs of IT teams and developers. The best way to achieve this is with a security services platform. Think of a security platform like a keyring. It's more efficient to have all your important keys on one ring, instead of having each key in a separate location. With a keyring, you can access whatever you need, whenever you need it, and add new keys as required. Likewise, a platform consolidates security services that are vital for SecOps and DevOps teams, from cloud workloads to containers, serverless applications, file storage, open source risks, cloud networks, cloud posture, and compliance.

Some security platforms can help **shift security left** for increased cloud visibility into development pipelines and processes for earlier detection and response. Implementing security guardrails early in the pipeline before developers migrate to the cloud helps them hit the ground running, so they can build and deploy quickly and securely.



A platform also provides you with the flexibility to choose, which aligns with the security by design approach. With a platform, you can choose the cloud (hybrid or multi), the environments (public, private, virtual), and the tools necessary to securely meet your organization's objectives.

Security teams may feel over-burdened, and DevOps teams can be resistant to integrating security into their processes—that's where platform-driven automation comes into play. This allows both teams to reap the benefits of security by design, without adding to existing workflows.

Like the infamous catch-22, "which came first: the chicken or the egg?", you might puzzle over whether to prioritize DevSecOps or platform security. But if you adopt a DevSecOps culture, it will lead you to a security services platform, and vice versa. And as DevSecOps continues to go mainstream, the benefits of the approach are showing. In 2020, a **GitHub DevSecOps survey** found that 93% of security professionals said developers caught 25% or less bugs. However, as teams continue to shift left (up by 5% to 70% overall) the number of disgruntled security professionals plummeted to 45% in 2021.

Considerations for choosing a security platform

While there are tons of platform solutions on the market, not every platform is created equal. Before you buy a house, you usually have a couple of "wants" in mind—big backyard, good schools, or a sound-proofed room where you can work without disturbances. Think carefully about your migration goals and how security will enable you to achieve them. Although security is not one-size-fits-all, in order to get the most comprehensive coverage and protections for your cloud migration journey, consider these key factors:

- More cloud visibility: According to an ESG report, 69% of organizations admit that they have a cloud visibility gap. Reduce blind spots with a single source of truth across your hybrid and multi-cloud environments, with complete security controls and integration.
- Multi-service: Provides a combination of workload, container, serverless, open source and even cloud storage, as well cloud posture and cloud networking protection for optimal flexibility and simplicity.
- Extensive automation: Save time, money, and resources in managing and enforcing security policies across hybrid environments.
- Developer-friendly: Deployment via security as code with API-enabled tools that support continuous integration and delivery to bake security controls directly into developer processes.
- Fast-track compliance: 38% of surveyed AWS customers cited compliance as their main day-to-day operational headache. The right platform will integrate automated compliance scanning into your build pipeline to catch any violations before deployment.
- Defense in depth: Leverage innovations such as virtual patch and integrity monitoring, while utilizing machine learning, AI, and threat intelligence to detect and block threats in real-time.

The cybersecurity vendor supplying your solution of choice is just as important as the product itself. Your cybersecurity vendor should act as a partner, and work with you as your security and business objectives change over time.

Solutions for your cybersecurity problems

Trend Cloud One™ is a security services platform designed to tackle cloud vulnerabilities for SecOps and DevOps teams. This cloud-native platform is compromised of the following eight security solutions:

- Trend Cloud One™ – Workload Security: Runtime protection for virtual, physical, cloud, and container workloads
- Trend Cloud One™ – Container Security: Automated image scanning in your build pipeline
- Trend Cloud One™ – File Storage Security: Security for cloud file and object storage services
- Trend Cloud One™ – Network Security: Cloud network layer intrusion protection system (IPS) security
- Trend Cloud One™ – Conformity: Cloud security and compliance posture management
- Trend Cloud One™ – Open Source Security by Snyk: Visibility and monitoring of open source vulnerabilities and license risks
- Trend Micro™ Cloud Sentry: Visibility of the threats in your AWS environment with quick, actionable insights in the context of your application

Earlier we mentioned a few key features you should look for in a cloud security platform. Here's how Trend Cloud One stacks up:

- More cloud visibility: One console for eight security services that provide complete cloud visibility. No more siloed views from various point products, our platform leverages turn-key integrations and broad APIs.
- Multi-service: Enjoy eight services designed to address all your cloud security needs—like Container Security, Network Security, Application Security, and Open Source Security by Snyk.
- Extensive automation: Benefit from automation within every solution, such as automated file and open source code scanning as well as auto-remediation or automatic post-scan actions.
- Developer-friendly: Our platform deploys via infrastructure as code (IaC) to ensure the most secure and compliant templates are used. Maintain development speed with Application Security, which provides detection and protection for apps and APIs built on your container, serverless, and other computing platforms.
- Fast-track compliance: Conformity takes care of compliance headaches with continuous scans against hundreds of best practice and compliance checks across a broad range of regions and industries.
- Defense in depth: Workload Security protects your new and existing workloads with machine learning, virtual patching, integrity monitoring, and more. You can stay ahead of the curve with insights into the latest threats thanks to Trend Micro™ Zero Day Initiative™, the world's largest bug bounty program.

Next steps

A home inspection before purchase is always a good idea. Similarly, you should always test a potential security solution before committing. See how Trend Cloud One can meet your needs with a free 30-day trial.