White Paper

Intel Security

Enabling Sovereign Landing Zones with Confidential Computing

How Accenture, Intel, and Scontain design confidential landing zones

Authors

Frederik De Ryck

Accenture, Cloud Security Engineer

Giuseppe Giordano

Accenture, Labs R&D Senior Principal

Brian Richardson

Intel, Security Strategy Lead, Data Center & AI Marketing

Paul O'Neill

Intel, Confidential Computing

Control over data has become a complex problem. The need for data collection is driven by many factors: growth of mobility, speed of connectivity, decreasing storage costs, and scale through outsourcing. But the service providers who collect and process this data must navigate a complex, global regulatory landscape to transform data into services for their consumers.

To cope with all these demands, more organizations are building and porting applications to the cloud. This coincides with the rapid growth of data breaches, drawing scrutiny to data privacy and security. Governments have reacted by implementing regulations and enforcing stricter data controls, driving ever-more stringent security and privacy expectations among companies, regulators, and consumers.

All this creates a challenge for businesses that depend on data: how do they meet regulations while leveraging the scale of the public cloud? Can they ensure that data is protected throughout the entire computing process? By using the principles of Confidential Computing, businesses can unlock new opportunities while maintaining data sovereignty.

Understanding Data Sovereignty

Data sovereignty is a growing movement to treat citizen data as a national asset and retain control over its use. This movement addresses the fluidity of data, today's multi-national cloud environment, and competing regulatory and privacy frameworks around the world. It assumes data should be protected according to the laws of the nation where it is being used (regardless of the country of origin or ownership of that data).

Many organizations implementing a data sovereignty strategy often rely on geo-location of data stores and data access, as well as the shipping and processing of data. They build a risk-averse setup that looks at the data and what measures to take. Contractual, organizational, and technical measures are the minimum basic hygiene needed in such a strategy. The strategy extends beyond the sovereign data to both architecture and operations.

In this context, the demystification of sovereign clouds addresses these challenges in an outsourcing mode. Sovereign clouds are designed to provide strong data handling and accessibility, can geographically locate data residency, and can effectively manage compliance risks. From a business perspective, organizations should assess these challenges through technical capabilities grouped by values such as protection, openness, independence, resilience, and interoperability.

Once this strategy is created and a cloud flavor is chosen, the implementation of the strategy raises several questions:

- Is the strategy compliant?

- Is the strategy secure?
- Do database administrators have access to encryption keys?
- Does the outsourcing partner access and store data from outside the country?
- If the outsourcing party dumps system memory, will it be detected?
- Can Cloud Service Provider (CSP) employees dump the hypervisor memory and access the data?
- How can one attest to the integrity of the hardware cluster, virtual machine (VM), and container software?

Protecting Data in Use

We are in an era where powerful, ubiquitous computing and innovation make business transformation both possible and urgent. Public cloud resources provide a cost-effective, infinitely scalable alternative to traditional on-prem infrastructure for many applications, making this an attractive arena for enterprises to build modern applications that require access to data sets.

New data sources, both internal and external, open new opportunities for analysis, new services, and new possibilities for collaboration between multiple parties. While this allows organizations to benefit from shared analyses and solve mutual issues, these opportunities can be hampered by legitimate privacy and security concerns.

The data these opportunities rely on is private, and care is needed when using this data to avoid breaching confidentiality or creating regulatory compliance violations.

Technologies have developed over time to protect data and ease privacy, security, and compliance concerns, but there has always been a gap. Storage and disk encryption evolved and matured to protect data at rest. Network encryption that protects data in transit is strong—and getting stronger. But those techniques don't help when data is in use in the processor and memory.

Despite the potential advantages of using the cloud, concerns about controlling sensitive data may delay migration and cloud-native projects. Organizations are apprehensive about losing control of their data due to regulatory or legal entities outside their preferred framework. Regardless of these concerns, however, some sensitive applications and data present high-value targets for profit-motivated hackers or nation-state actors. While a service innovation may create value and convenience for users, the risk of activating the data beyond a locked-down storehouse may be viewed as too challenging from a compliance perspective.

Landing Zones for Cloud Security

Compliance and security often go hand in hand, but in this situation, businesses often consider supplementary measures that help with neither. An optimized solution starts from the fundamental concept of a *landing zone*.

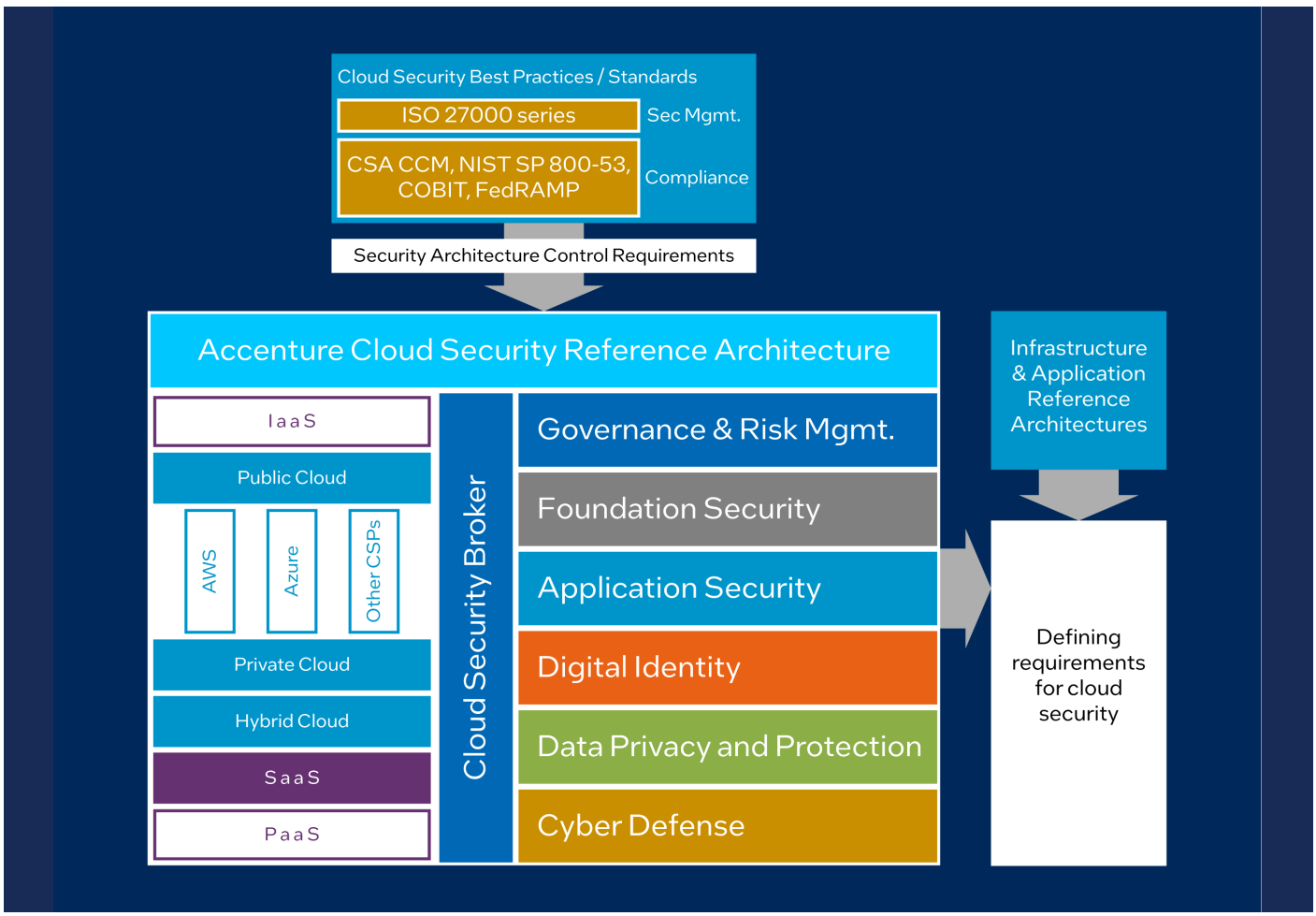

Figure 1. Accenture Cloud Security Reference Architecture – Layers of Protection.

Landing zones are automated functions based on a set of Infrastructure as Code (IaC) elements that enforce guard rails, as illustrated in Figure 1. A secure baseline should address foundational elements of cloud security:

- Governance and risk management
- Foundation security
- Application security
- Digital identity
- Data privacy and protection
- Operational security (cyber defense)

The benefits of a cloud landing zone is that a number of policies are established initially that determine how applications and data are used in a cloud environment.

Once these layers are operating at a decent maturity level and enforcement controls cannot be circumvented, it's time to explore the next potential gap in the data protection continuum: protecting data while in use. Confidential Computing is designed to address this and is paramount to meeting regulations.

Confidential Computing Helps Protect Data in Use

Confidential Computing offers a hardware-based security solution designed to help protect data in use via unique application-isolation technology called a Trusted Execution Environment (TEE). By helping protect selected code and data from inspection or modification, enterprises can run sensitive data operations inside enclaves to help increase application security and protect data confidentiality. Confidential Computing strengthens the security of data and software Intellectual Property (IP) operating inside TEEs verified for proper configuration (Figure 2). Sensitive data should be decrypted inside the TEE. Only software inside the TEE's trust boundary can access sensitive data, and only authorized data owners hold the keys to their data. This implies that encryption keys can only be accessible inside authorized TEEs. Outside of the TEE, data is encrypted; inside the TEE, only authorized software or parties can view it.

Confidential Computing is designed to enforce technological separation from software and entities outside the trust boundary. This includes the cloud provider's management stack, hypervisor, infrastructure admins, and other cloud tenants. The technological separation of data from the cloud provider offers a new level of privacy, security, and control that can enable organizations to move sensitive workloads to the cloud with confidence.

In addition, Confidential Computing uses attestation to verify software running in the TEE is exactly what's expected. This includes cryptographic verification (updated within policy) that the TEE is genuine.

The TEE and granular access controls open possibilities for new services or collaborations using sensitive or regulated data. Previously, sensitive data was locked away and treated only as a source of risk rather than a source of value. Confidential Computing enables organizations to activate their valuable data while keeping it private, protected, and compliant, even during collaboration with other parties.

Confidential Computing with Intel® Xeon® Scalable Processors

Intel's broad portfolio of Confidential Computing technologies allows organizations to choose the level of security they need to help meet their business needs and regulatory requirements. Intel is the only company that offers Confidential Computing solutions at both the application and the VM level.

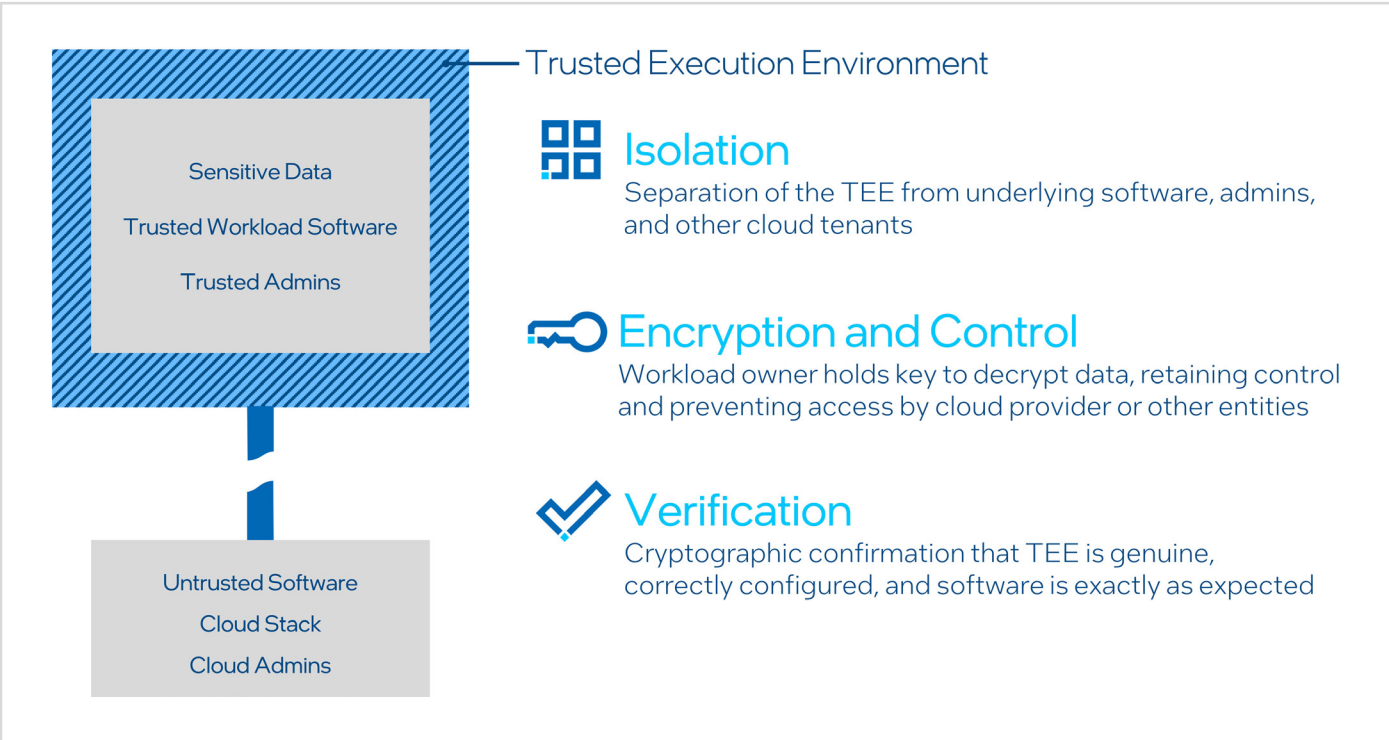

Figure 2. Properties of a Trusted Execution Environment.

Intel released Intel® Software Guard Extensions (Intel® SGX) in 2015. This groundbreaking, hardware-based technology introduced highly performant protection of data in use, combined with attestation. Intel SGX enables developers to protect individual applications from other software and actors by using a TEE. This TEE provides data confidentiality, data integrity, and process integrity for applications. Combining Intel SGX with data protection at rest and in transit enables organizations to confidently run workloads anywhere, even if the environment is not trusted.

In 2023, Intel extended hardware-based security even further with the introduction of Intel® Trust Domain Extensions (Intel® TDX). Intel TDX erects a trust boundary around VMs—a popular method of managing a wide variety of compute workloads. VMs protected by Intel TDX, called Trust Domains, can contain a full operating system or a minimal kernel, as well as one or multiple applications. TDX is designed to help ensure that nothing in the software stack can access code or data within the boundaries of a Trust Domain, including the host OS, hypervisor, firmware, or system administrator. Multiple Trust Domains can run on the same server. They are protected from each other using a combination of different ephemeral keys used for main memory encryption, as well as access controls inside the CPU (Figure 3).

Given the choice between application isolation and VM-level isolation, Accenture and Scontain built a landing zone solution around Intel SGX to deliver the smallest attack surface. Rather than excluding sensitive data from analytics or AI models, businesses using Intel Xeon Scalable processors can create access-restricted data enclaves with Intel SGX. These isolated environments can help organizations extract value from their most sensitive data while helping to keep it confidential.

Intel SGX is the most deployed, researched, and TEE for the data center. By protecting selected code and data from inspection or modification, developers can run sensitive data operations inside enclaves to help increase application security and protect data confidentiality.

With Intel SGX, compliance is enhanced, while at the same time the attack surface of the data plane is drastically reduced. Hypervisor operators, OS, and other admins can no longer access decryption keys. Confidential Computing adds another layer of protection to basic security hygiene. The hardware-backed TEE helps increase the overall security posture, while attestation is designed to validate the underlying hardware and software.

Using Confidential Computing to Build Business Value

Moving to the cloud can solve many business challenges, and Accenture excels at helping organizations understand the big picture. Accenture experts can strategize, identify enterprise business needs, and co-design solutions to meet these challenges.

To strengthen its skills and respond to the needs of the European market, Accenture built five European Centers of Excellence (CoEs). Four of these CoEs focus on sovereign cloud solutions, with the fifth specifically designed to deal with cloud security. All these CoEs assist customers in their journey to the cloud by helping inspire, consult, deliver, and run sovereign solutions. The Accenture sovereign cloud tech radar explains how to look at possibilities through different lenses, or game fields. This vision is ambitious and provides a glimpse into directions to explore when assessing where a workload needs to go in terms of openness, security, resilience, interoperability, etc.

When moving concrete workloads to the cloud, taking a broader look at the full range of possibilities helps organizations select the best cloud flavor to fit the needs of those workloads. A one-size-fits-all cloud deployment model does not work across all levels of confidentiality and regulatory sensitivity.

Setting up landing zones in a model can help solve this because developers can shift from less to more controlled and compliant setup, depending on risk scoring and the data the application is hosting. There are three main landing zones, as illustrated in Figure 4:

- The "Secure Zone" is the lowest in terms of Total Cost of Ownership (TCO). It handles data that is not sensitive or regulated.

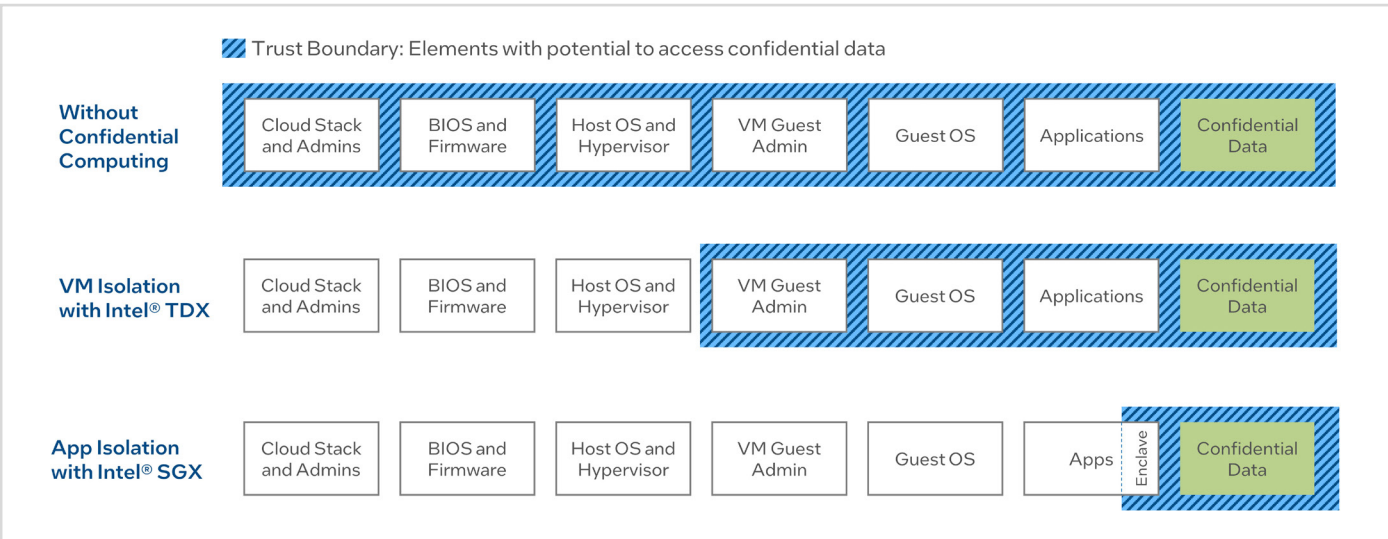

Figure 3. Trust Boundaries.

- The "Private Zone" handles confidential business workloads, such as billing and account management, and uses VM-isolation Confidential Computing, often with off-the-shelf or black box software.
- The "Sovereign Zone" handles personally identifiable and regulated data that requires the highest level of care under GDPR and other applicable laws, including subscriber details. This zone runs purpose-built, privacy-preserving applications inside Intel SGX enclaves on targeted, sovereign European data centers; keys are owned by the customer. This approach enables both geo-location and data control enforcement.

Using containerized platforms helps organizations move towards cloud-native applications at scale. Auto-healing, resiliency, and scalability features are proven and deliver tremendous benefits. To best use these cloud-native applications and micro-services, developers can rely on the Scone platform created by Scontain, a German spin-off of TU Dresden University. Scone helps protect the code, data, and secrets of applications executed in a computing infrastructure managed by an external provider. Sometimes, the external provider even operates the application itself—without being able to access data, code, or secrets. In enabling such confidential outsourcing, the platform also provides features to verify and ensure protection.

Container-based Cloud Foundation Frameworks

Introducing the Scone platform, especially in a public cloud world, enabled the use of Intel SGX on top of container orchestrators that can load and secure containers in pods, like Azure Kubernetes Service (AKS). While basic hygiene still needs to be taken care of, the Scone Configuration and Attestation Service (CAS) enforces security policies that protect code, data, and secrets in use, at rest, and in transit.

The platform uses binary transformation ("Sconification") to convert a container image into a confidential container image. This transformation ensures that:

- Each service starts inside an enclave (i.e., executes in an encrypted memory region).
- Each service is transparently attested and verified to ensure the correct code is executed on an up-to-date CPU.
- A default security policy is automatically generated.
- Files are transparently encrypted and protected against modification and rollback by an adversary.
- A default Helm chart is generated to simplify the deployment of confidential service.

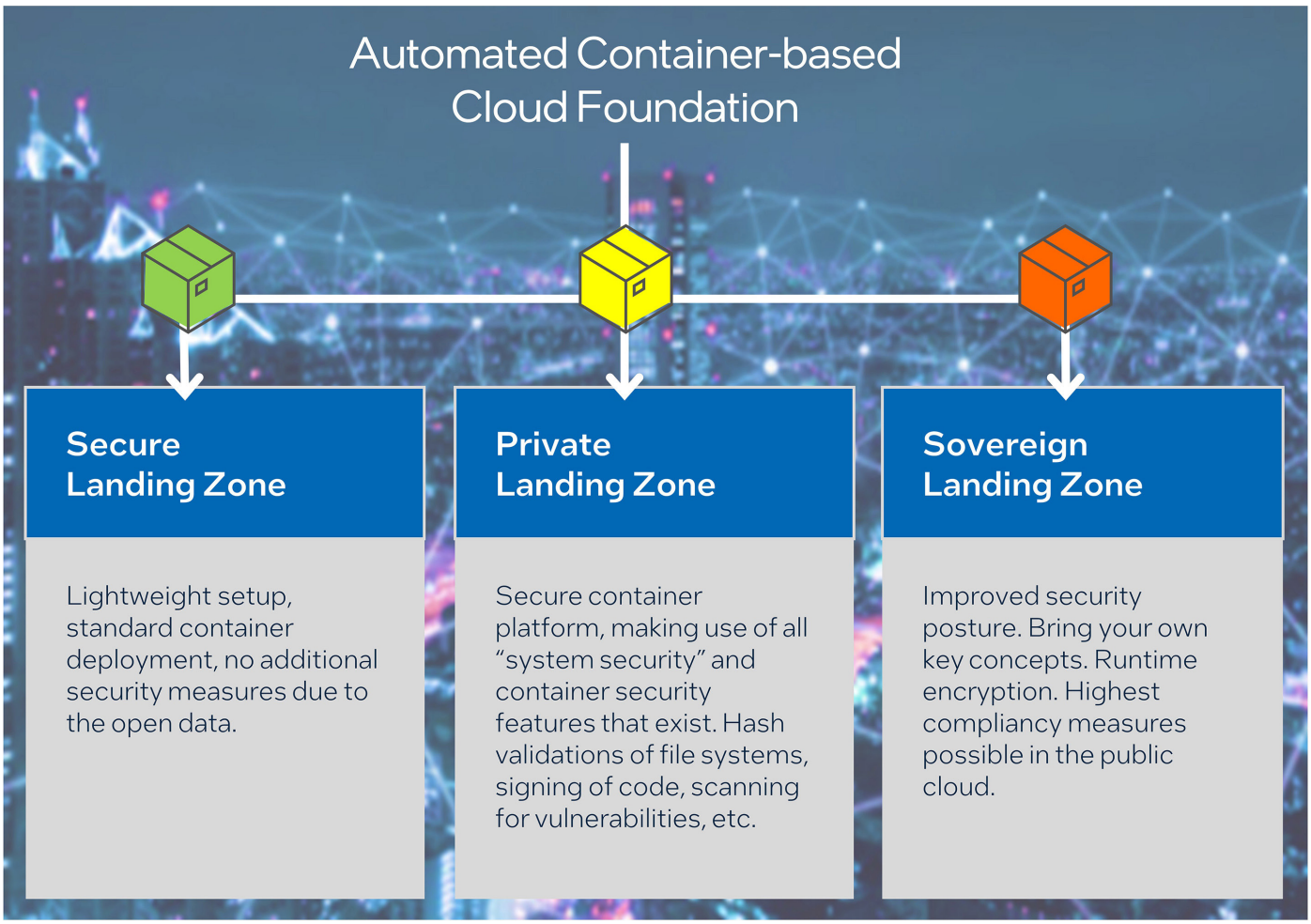

Figure 4. Landing Zones.

Scone security policies and CAS provide enterprise features to ensure that aspects of security policies can be shared between applications and can be managed by different groups. In addition, secrets can be shared between CAS instances operated by different groups; that way, trust can be established between various applications managed by several groups.

At runtime, the platform performs a transparent attestation of container workloads, proving that:

- The application runs inside an enclave on a genuine, up-to-date Intel CPU with appropriate hardware and firmware.
- The application's initial state is correct and up to date.
- All encrypted files are in the expected state (i.e., no unauthorized modification or rollback).

If required by an application's security policy, the container attestation service will ensure that the application runs on an approved server and that a one-time password authorizes the start. A security policy defines what secrets are provided. Only attested and verified confidential applications can access these secrets. CAS permits the creation of secrets and the importing of secrets from local and remote CAS policies, as well as external services like Azure Key Vault or Hardware Security Modules (HSMs).

The power of Intel, Accenture, Scone, and cloud service providers enables:

- Business transformations – design of fit-for-purpose solutions by the COEs
- Enhanced confidentiality, integrity, consistency, scalability, and resiliency
- Extremely secure instantiations of landing zones, including Scone CAS and security guardrails
- Automating the deployment pipeline to land workloads in their respective landing zone

Summary

As the computing landscape advances, so does the urgency for businesses to stay on top of data security. Public opinion and government regulation have set the bar, and technology must innovate to fill the gaps. This is especially critical as businesses continue to look to the benefits of the cloud for their applications. While there are mature solutions to protect data at rest and data in transit, there are still vulnerabilities to consider when it comes to data in use. Confidential Computing addresses these gaps by establishing hardware-enforced TEEs and closely controlling who has access to each piece. This separates the people using the sensitive data from those providing the cloud service. With more and more hands involved in managing data in the cloud, the idea of data sovereignty throughout the entire data hierarchy is pivotal.

Accenture provides an end-to-end solution for cloud security and data sovereignty using procedures, frameworks, and modern hardware and software tools. The combination of Intel SGX and Scone enables container-based cloud foundation frameworks designed to secure the most sensitive data by providing the smallest attack surface for Confidential Computing.

For More Information

- Accenture: Sovereign Cloud: Take control of data and stay compliant
  https://www.accenture.com/us-en/insights/cloud/sovereign-cloud
- Intel Confidential Computing
  Intel.com/confidentialcomputing

NOTICES AND DISCLAIMERS

Intel TDX will be available on select 4th Gen Intel Xeon Scalable instances through four leading cloud providers.
Previews have begun with select providers. Check with your provider for availability.
Intel TDX becomes generally available with 5th Gen Intel Xeon Scalable processors.
The Scontain platform is one of a number of confidential computing solutions that Intel and Accenture partner with as workloads vary across different enterprise needs.

Intel technologies may require enabled hardware, software, or service activation.
No product or component can be absolutely secure.
Your costs and results may vary.

© Intel Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

ACG6288SDS