intertrust®

SOLUTION BRIEF

The transition to virtual secure rooms

A paradigm shift in secure cryptographic operations

Building trust for a connected world.

Contents

Executive summary

A profound shift is underway in how organizations protect their critical cryptographic operations.

For decades, secure compartmented information facilities, or SCIFs, have been central to this mission, providing physically secure environments for managing encryption keys and executing sensitive operations.

However, cloud technology has advanced to the point where organizations now have the option to migrate these sensitive operations into virtual secure environments that deliver equal or greater levels of security while also reducing costs and increasing operational flexibility.

This transition represents the evolution of security into a modern, service-oriented ecosystem where enterprises can focus more on their core missions while relying on cloud-delivered cryptographic services. Virtual secure rooms allow organizations to maintain the highest levels of security for sensitive operations without the capital and operational burdens of maintaining physical SCIFs.

The burden of traditional SCIFs

Traditional secure rooms have been indispensable for managing cryptographic key infrastructure, but they impose significant hidden costs.

Organizations must invest not just in the initial construction of secure facilities, but also in the ongoing maintenance of highly specialized environments. Military-grade countermeasures are required to protect against both physical intrusion and electronic eavesdropping. These measures often include shielding against electromagnetic leakage, biometric access controls, and the installation of dedicated hardware security modules (HSMs) within tightly monitored environments.

Operations within a physical SCIF require dual-operator protocols, multi-party authentication processes, and continuous video surveillance to ensure that no single individual can compromise the system without detection. Personnel management adds another layer of complexity. Only security-cleared, bonded individuals may serve as operators, and they must adhere to rigorous operational guidelines.

Maintaining this specialized workforce imposes direct costs in terms of salaries, certifications, and ongoing training, while also creating indirect costs in terms of organizational focus and flexibility.

Business continuity and recovery challenges

Traditional disaster recovery strategies for physical SCIFs are constrained by the inherent limitations of physical infrastructure. Recovery times are often measured in days because restoring operations requires manual activation of secondary sites, coordination among operators in different geographic regions, and physical access to hardware.

Preserving readiness at multiple sites involves not only the upkeep of redundant systems but also the challenge of ensuring that operational procedures remain synchronized across facilities. The result is an environment where disaster recovery is costly, time-consuming, and operationally rigid, reducing organizational agility in moments when speed and resilience are critical.

Organizations must invest not just in the initial construction of secure facilities, but also in the ongoing maintenance of highly specialized environments.

Advantages of virtual secure rooms

Advancements in cloud computing have made it possible to virtualize secure environments for cryptographic operations. The cornerstone of this transformation is the development of trusted execution environments, or TEEs, which create isolated computing spaces within cloud infrastructure.

Virtual secure rooms can dynamically allocate additional resources, offering flexibility that physical SCIFs cannot match.

These secure enclaves are cryptographically separated from the rest of the system, ensuring that sensitive operations remain confidential even from the cloud service provider's root-level administrators.

Cloud infrastructure now offers robust protections that rival or surpass those of physical SCIFs. Organizations can deploy virtual segmentation strategies using dedicated private cloud environments, eliminating the risks traditionally associated with multi-tenant systems.

Cloud-based hardware security modules are certified to meet stringent government and industry security standards, and advanced key management systems enable secure generation, storage, and rotation of cryptographic keys.

Superior operational abilities

Virtual secure rooms provide continuous security monitoring through automated systems that analyze network traffic, system behavior, and user activities in real time. These environments support AI-driven threat detection and response mechanisms, offering security teams real-time alerts and actionable insights.

Unlike physical SCIFs, where software updates and security patches may be delayed due to the complexities of controlled environments, cloud-based virtual secure rooms enable faster, more consistent patching without compromising operational integrity.

Authentication mechanisms integrate with existing enterprise identity systems, allowing organizations to maintain consistent security policies across both on-premises and cloud environments. Smart card authentication, biometric verification, and multi-factor protocols work seamlessly within virtual secure rooms. Additionally, these systems provide immutable logs that record all activity, supporting audits and compliance checks with greater ease than manual processes in physical environments.

Scalability represents another key advantage. Virtual secure rooms can accommodate sudden increases in cryptographic workload by dynamically allocating additional resources, offering flexibility that physical SCIFs cannot match.

The financial case for change

The economic advantages of virtual secure rooms are substantial. Organizations migrating from traditional secure facilities can eliminate costs related to building construction, specialized hardware acquisition, and ongoing maintenance of physical sites.

Personnel costs decrease significantly since there is no longer a need to staff multiple locations with security-cleared operators for manual processes. Travel expenses for disaster recovery testing and audits drop substantially, as these processes can be performed virtually with faster and more reliable results.

Introducing Intertrust iSCIF™

Intertrust's virtual iSCIF offers a breakthrough in a cloud-native environment that exceeds the security guarantees of physical SCIFs while delivering significant cost, operational, and scalability benefits.

At its foundation, iSCIF provides a comprehensive virtual secure compartmented information facility that maintains the highest levels of security while offering unprecedented operational flexibility.

The iSCIF solution addresses the fundamental limitations of traditional secure facilities by delivering enterprise-grade cryptographic operations through a fully managed cloud service.

Intertrust iSCIF eliminates the need for massive infrastructure investments, annual personnel burdens, and complex physical facility management. Instead of maintaining air-gapped bunkers, organizations can now deploy scalable, secure key management that adapts to their evolving needs.

Core iSCIF capabilities

At its foundation, iSCIF provides a comprehensive virtual secure compartmented information facility that maintains the highest levels of security while offering unprecedented operational flexibility. The platform creates cryptographically isolated environments within cloud infrastructure, ensuring that sensitive cryptographic operations remain protected from both external threats and cloud provider access.

The iSCIF architecture incorporates hardware-backed trusted execution environments that provide tamper-resistant processing for critical operations. These secure enclaves maintain the integrity of cryptographic keys and sensitive data throughout their lifecycle, from generation to destruction.

Multi-party authentication protocols ensure that no single individual can compromise the system, digitally enforcing the same security controls traditionally maintained through physical oversight.

Key benefits of iSCIF

Immediate cost reduction

Organizations typically achieve 60-80% cost savings compared to traditional SCIF operations. The elimination of physical infrastructure, specialized facility maintenance, and reduced personnel requirements creates substantial budget relief. HSM infrastructure investments, which can run into millions of dollars for redundant physical deployments, are replaced with cloud-native security modules that scale with demand.

Enhanced security posture

iSCIF provides continuous monitoring and automated threat detection capabilities that surpass manual surveillance systems. The platform incorporates AI-driven anomaly detection, real-time behavioral analysis, and automated incident response mechanisms. Immutable audit logs provide comprehensive forensic capabilities, while encrypted communications ensure that all data transmission remains secure.

Operational agility

The platform enables rapid deployment of new cryptographic services without the lengthy procurement and installation cycles associated with physical infrastructure. Organizations can provision new secure environments in minutes rather than months, supporting dynamic business requirements and emergency response scenarios.

Scalable architecture
iSCIF automatically adjusts computational resources based on workload demands, ensuring optimal performance during peak operations while maintaining cost efficiency during low-activity periods. This elastic scaling capability supports organizations with variable cryptographic workloads or seasonal demand fluctuations.

Compliance integration
The platform maintains compliance with federal security standards including FIPS 140-2 Level 3 and Common Criteria certifications. Built-in compliance reporting and audit trail generation simplify regulatory oversight, while automated policy enforcement ensures consistent adherence to security protocols.

Integration and migration support

Intertrust provides comprehensive professional services to ensure successful iSCIF implementation. The migration process begins with a detailed assessment of existing SCIF operations, identifying optimization opportunities and potential challenges. Custom integration development ensures seamless connectivity with existing enterprise systems, while comprehensive training programs prepare operational teams for the transition.

The platform's API-first architecture enables integration with existing security tools and workflow systems. Organizations can maintain their current operational procedures while benefiting from enhanced security and reduced costs. Progressive migration strategies allow for gradual transition, minimizing operational disruption while building confidence in the new platform.

Strategic positioning for the future

Virtual secure rooms represent part of a broader shift toward next-generation security ecosystems. These cloud-native environments facilitate integration with threat intelligence platforms, automated response systems, and advanced security analytics. Organizations adopting solutions like Intertrust iSCIF position themselves to take advantage of future innovations while reducing management complexity today.

Early adopters gain not just cost savings but competitive differentiation. By moving beyond the limitations of physical security infrastructure, they can respond faster to market changes, regulatory updates, and emerging threats. This agility provides a strategic advantage in sectors where security, speed, and compliance are mission-critical.

Elastic scaling is critical for organizations with variable cryptographic workloads or seasonal demands.

Conclusion

The transition from physical to virtual secure rooms represents a pivotal moment in the evolution of enterprise security.

Intertrust iSCIF enables organizations to achieve this transformation while maintaining the highest levels of security and compliance. By eliminating the operational overhead and cost burdens of traditional SCIFs, iSCIF allows security teams to focus on strategic initiatives rather than infrastructure maintenance.

Organizations implementing iSCIF gain immediate value through dramatic cost reduction, enhanced security capabilities, and operational flexibility that was previously impossible with physical infrastructure. The platform's proven ability to exceed traditional SCIF security guarantees while providing cloud-native scalability positions adopting organizations for long-term competitive advantage.

For cryptographic operations teams, the decision is no longer about whether to make the move to virtual secure rooms, but about how quickly they can leverage Intertrust iSCIF to position themselves for a secure and scalable future. The era of air-gapped bunkers is ending—the age of intelligent, cloud-delivered secure operations has begun.

Ready to explore how Intertrust iSCIF can modernize your cryptographic operations? Connect with our security experts to discover how to get started SCIFs and transform your approach to enterprise key management.

The era of air-gapped bunkers is ending—the age of intelligent, cloud-delivered secure operations has begun.

Learn more at:
intertrust.com/moving-scifs-to-the-cloud
Contact us at: energy@intertrust.com
+1 408 616 1600

intertrust®

Building trust for a connected world.