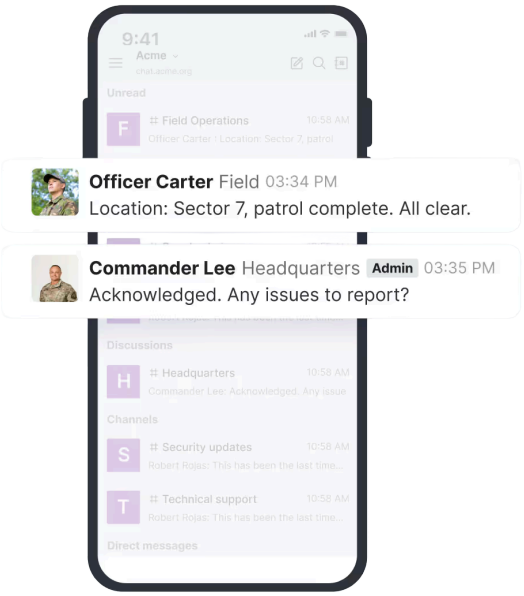
Rocket.Chat + Virtru Data Security Platform

Real-Time Access Governance for Classified Collaboration

The Challenge

In Rocket.Chat, a channel is a dedicated workspace where a team communicates and shares files. A channel's membership is simply the list of people permitted inside, and therefore, the list of people who can see everything posted there. For classified programs and compartmented environments, channel membership is a security control, not an administrative convenience. When personnel change roles, clearances expire, or PERSEC holds are applied, collaboration access must respond in real time — not after IT ticket queues clear. Traditional approaches rely on static rosters: an analyst's compartment clearance expires, an engineer rotates from one program to another, but the channel doesn't know until someone files a ticket. The delay often spans days or weeks, leaving the person inside the channel, still able to read everything in it, long after they should have lost access.

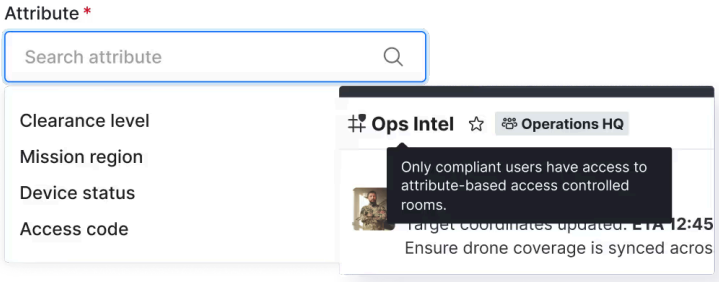


The problem is bigger than any single ticket. Zero Trust, the security model now mandated across federal and defense systems, holds that access should never be granted once and assumed valid forever. The federal blueprint for it, NIST SP 800-207 requires continuously re-evaluated, entitlement-based access decisions. Yet the collaboration layer — the chat channels where the most sensitive work takes place — is usually the last place this principle reaches. Most platforms still decide who gets in at the moment a person is added and never look again, so access reflects the policy in force back then rather than the policy in force now.

The Power of Rocket.Chat + the Virtru Platform

Rocket.Chat delivers mission-critical communications for defense and intelligence organizations operating across NIPRNet, SIPRNet, and JWICS. The platform provides native attribute-based access control, sovereign deployment options, and the operational discipline classified environments require — including DoD Authorization to Operate at Impact Level 6.

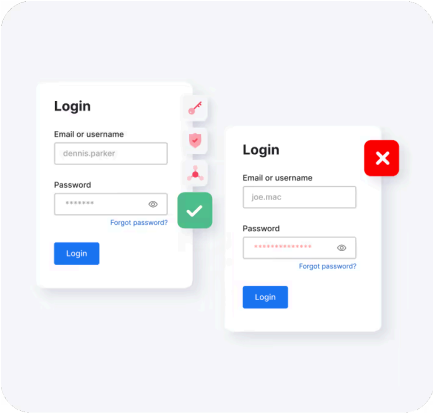
With the **Virtru Data Security Platform**, Rocket.Chat extends channel access governance from provisioning-time decisions to continuous, automatic, real-time policy enforcement. The integration delivers for Rocket.Chat an external decision layer that evaluates every channel membership against current entitlements. Sourced directly from authoritative identity providers, the Data Security Platform will immediately inform Rocket.Chat of any policy or entitlement change, enabling automatic eviction when access no longer satisfies policy, and complete audit trails for every decision.



The combined solution delivers a central policy decision point within the Virtru Data Security Platform that evaluates every channel, every user, and every sync cycle against a single authoritative source of entitlements — without storing entitlement data within Rocket.Chat's collaboration environment. The result is identity-driven enforcement without vendor lock-in, complete auditability that persists beyond the collaboration boundary, and the decision-level evidence that IG auditors and Zero Trust assessors require.

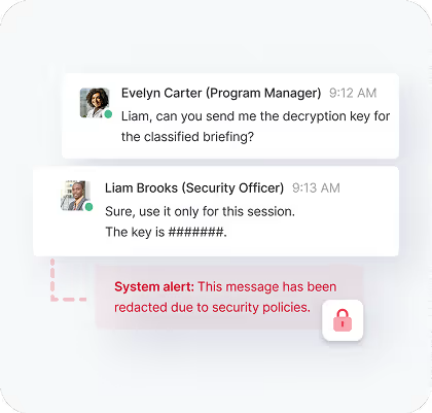
Key Joint Capabilities

Real-Time Access Governance: Rocket.Chat's channel membership responds to entitlement changes each time it syncs with the Virtru Data Security Platform, typically in minutes — not days — eliminating residual access gaps when personnel rotate, clearances change, or operational contexts end.



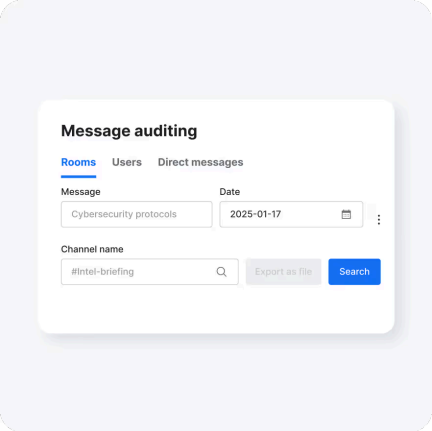
Fail-Secure by Default: Users without assigned entitlements cannot be added to rooms. Existing memberships are preserved unchanged when entitlement data is unavailable — the system never fails open.

Identity-Driven Enforcement Without Identity Lock-In: The Data Security Platform evaluates entitlements from any OIDC/OAuth2-compatible IdP — Okta, Microsoft Entra ID, Ping Identity, ICAM — preserving identity sovereignty while adding data-layer enforcement. User entitlements remain in the organization's IdP, no raw entitlement data is stored within the Rocket.Chat platform.



Add-Time Access Validation: Within Rocket.Chat, any manual change is checked against the current entitlements before it is completed. Room owners cannot circumvent policy by adding users who fail ABAC — the enforcement point is authoritative.

Mission Tempo Operations: Joint Task Force (JTF) stand-downs, PERSEC holds, and program rotations propagate from IdP to the Data Security Platform, triggering Rocket.Chat channels to dissolve alongside the mission without manual cleanup across multi-agency or multi-national teams.



Decision-Level Audit Logs: Every access decision is logged with user, channel, attributes evaluated, decision, and timestamp — citable evidence for IG audits, Zero Trust reviews, and continuous monitoring programs.

Rocket.Chat + Virtru Use Cases

IC Need-to-Know Enforcement

An analyst's compartmented clearance expires pending reinvestigation. In traditional implementations, static access controls leave them in the channel for weeks until discovered. With the integrated solution, changes to IdP entitlements propagate to the Data Security Platform, and the analyst is automatically removed from the Rocket.Chat channel at the next sync. Removals are recorded with comprehensive context — user, timing, and governing policy — providing continuous, decision-level audit evidence for IG reviews that requires no manual assembly.

SAP/SCI Channel Governance Across Program Rotation

An engineer rotates from Program TITAN to Program APOLLO. Traditional offboarding requires an IT ticket that spans several days, leaving TITAN coordination open to unauthorized access. The integrated solution automatically re-evaluates access when program assignment entitlements update in the IdP, removing the engineer from TITAN immediately without manual intervention. Re-enrolling in APOLLO is governed by explicit administrative actions validated against real-time entitlements before access is granted.

JTF Stand-Down at Mission Tempo

A Joint Task Force dissolves over a weekend. Traditional static access controls fail to provide reliable cleanup across multi-agency and international channels, leaving outdated rosters active until administrative tickets are processed. The integrated solution updates the JTF status entitlement in the IdP, upon Rocket.Chat's next sync cycle with the Data Security Platform former members are automatically evicted from all JTF channels, allowing the operational footprint to dissolve alongside the mission.

IG Audit and Zero Trust Posture Review

An IG team requests documented evidence that channel access in classified programs is continuously re-evaluated against current authorization policy. Static access controls record only historical access, lacking context on why access was granted, the specific policy in effect, or whether authorization was verified post-provisioning. The Data Security Platform generates a persistent, decision-level audit trail documenting every access request, blocked addition, and membership removal — along with the specific entitlements and policies evaluated — providing the rigorous evidentiary record required for Zero Trust posture documentation.

Why This Integration Matters

Operational condition	Without this integration	With Rocket.Chat + Virtru
Personnel rotate off a SAP or SCI program	Channel membership persists until an IT ticket is filed and actioned — days to weeks of residual access	Attribute update in IdP triggers removal at the next sync cycle — minutes, not days
Clearance reinvestigation or temporary suspension	No automatic channel impact; manual tracking required across every relevant room	PERSEC hold propagates to the Platform; all affected channels re-evaluate and evict
JTF stood down or operational context ends	Program channels retain all members; no automated cleanup across multi-agency, multi-national teams	Status updated in IdP; the Data Security Platform informs Rocket.Chat to drive automatic eviction across all JTF channels
IG audit or Zero Trust compliance review	Access logs show who had access — not why, not under what policy, not whether decisions were continuously re-evaluated	Every Platform decision is logged: user, channel, entitlements evaluated, decision, timestamp
Room owner or admin attempts to manually add a non-compliant user	Depends on admin awareness and discipline; no systematic enforcement	Blocked at the Rocket.Chat enforcement point regardless of admin action — the Platform decision is authoritative
User lacks entitlement values	Fail-open in most implementations — no decision means no barrier	Fail-secure by design: adds blocked, room entitlement changes rejected, existing memberships preserved unchanged

Technical Requirements

Deploying the Virtru Data Security Platform with Rocket.Chat for ABAC-managed channels requires active deployments of both platforms and an Identity Provider to source the entitlements that govern access decisions.

- **Rocket.Chat deployment**: Supported across NIPRNet, SIPRNet, and JWICS; on-premises, customer cloud, or air-gapped environments
- **Virtru Data Security Platform**: Customer VPC or on-premises; matched to Rocket.Chat's deployment profile and accreditation boundary
- **Authoritative Identity Provider**: Okta, Microsoft Entra ID, Ping Identity, or equivalent OIDC/OAuth2-compatible identity system holding clearance, program, department, and nationality attributes
- **ABAC policy definition**: The per-room entitlement policy (e.g., clearance_level = TOP_SECRET AND project_assignment = OLYMPUS) defined by an authorized admin in Rocket.Chat
- **Sync interval configuration (Rocket.Chat)**: CRON expression set by the organization based on security policy
- **Network connectivity** between the Virtru Data Security Platform and Rocket.Chat services, within the accreditation boundary of the classified network

Security & Compliance

The joint solution applies separation of duties across the access decision chain. Your IdP is the authoritative source of identity entitlements. The Virtru Data Security Platform is the external decision engine — Rocket.Chat sends only the minimum required data and receives an Allow or Deny. Rocket.Chat enforces the decision and logs the outcome. No user entitlement data is ever stored in the collaboration platform. The system fails secure by default: missing entitlement values do not produce permissive decisions.

Compliance posture. The Virtru Data Security Platform and Rocket.Chat can be operationally deployed across NIPRNet, SIPRNet, and JWICS. The integration supports NIST SP 800-162 for ABAC and NIST SP 800-207 for Zero Trust.

About Virtru

Virtru is pioneering the shift from network-centric to data-centric security — embedding protection directly into data so mission owners maintain control wherever sensitive information is shared. The Virtru Data Security Platform is built on OpenTDF, an open standard evolved from technology developed at the NSA by co-founder Will Ackerly, and supports ACP-240, the Five Eyes-ratified Zero Trust standard for secure coalition operations. Trusted by over 6,000 public and private-sector organizations — including the U.S. Department of War, JPMorgan Chase, and Salesforce — Virtru enables secure collaboration across classification boundaries at mission speed, with integrations with leading defense, cloud, and cross-domain solution providers.

About Rocket.Chat

Rocket.Chat is the secure communications platform for organizations with the highest security and compliance requirements. Deployed across NIPRNet, SIPRNet, and JWICS, Rocket.Chat holds DoD Authorization to Operate at Impact Level 6 and is listed in the AWS Intelligence Community Marketplace. Defense agencies, intelligence community organizations, and allied partners rely on Rocket.Chat for mission-critical coordination across classification boundaries — with open architecture, sovereign deployment options, and the operational discipline that classified environments require.