SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Solution Innovation Case Study:
Security Transformation at Twilio: A Data-Driven Approach to Protect People, Assets, and Enable Business Growth

The Security Executive Council (SEC) Solution Innovation Partner (SIP) program evolved to help security practitioners expedite choosing a trustworthy risk mitigation vendor with confidence given the myriad of viable options in the marketplace. Proven Solution Innovation Case Studies help to evaluate performance claims and differentiate security solution providers for business outcomes including risk mitigation, return on investment, and security assurance.

This case study shows how Twilio Inc. redefined its security operations with the Ontic software platform. By implementing a centralized system to collect, store, and analyze security data on incidents, assets, and threats, Twilio transformed its approach to safeguarding employees, assets, and brand. This has allowed Twilio to deliver more impactful employee security solutions with greater efficiency, and increased value to the business. The Security Executive Council and the client end-user validated this.

Risk Issues and Mitigation Opportunities:

- Twilio's corporate security team operated with disparate data sources, with critical security information scattered across Airtable, Google Drive, Slack channels, and slide decks. This caused a consistent loss of valuable institutional knowledge when employees departed or tools changed, making it nearly impossible to locate vital risk information when needed.
- The team lacked standardized processes for collecting and managing assets, threats, and cases, and incident data. Their ability to build knowledge, document cases, track patterns or consistently communicate risk migration options to leadership was limited.
- A lean team of specialists managing multiple critical functions to amplify their capabilities with the right integration tool.
- The security team struggled to quantify impact and visualize insights or trends for leadership.
- Becoming business enablers, rather than inhibitors, and better supporting new corporate initiatives with appropriate risk management systems.

"Prior to Ontic, we didn't have a standard way of collecting critical data that enabled us to capture learnings that we could use to fortify our security posture." - Justus Abhulimen, Security Leader at Twilio

Solution Requirements:

- A configurable technology system capable of nimbly evolving alongside changing security priorities and business objectives.
- Integrated, robust, case management, investigative research, and threat tracking capabilities, with workflows to connect HR, Legal and other cross-functional partners.
- Personalized solutions for Twilio's remote workforce with varying risk profiles within corporate security standards.

- Primary need fulfillment, including the ability to centralize and govern data, procedures, and tools for various security functions.
- Proactive rather than reactive, automated, and systematic risk mitigation option analysis
- Regulatory and standards compliant with SOC 2, GDPR, and other enterprise governance practices.
- Twilio desired a collaborative partner willing to understand their unique needs in an environment of frequent ideation.

Delivered:

- A central platform for collecting and managing security data for assets, threat actors, intelligence, incidents, and cases.
- Advanced analytical trend capabilities, enabling proactive threat identification and risk forecasting before incidents occur.
- Automated incident reporting and triage capabilities, routing incident reports directly into the platform with notifications to relevant teams.
- Collaborative, cross-functional, and customized workflows, integrating partners including HR, employee relations, legal, and investigators.
- Personalized "employee-based solutions" that tailor security measures to individual employee risk profiles.
- Enhanced threat assessment tools, including identities, public research, and adverse media monitoring.
- Performance for value metrics management, dashboards with better visualization of security insights to leadership stakeholders.
- User-friendliness to simplify onboarding and training for new security personnel is particularly valuable in Twilio’s high-turnover environment.

“We went from struggling to find information in disparate systems to building a foundation that incorporates cross-functional partners into the fold, allowing us to be more effective in our duty of care.” - Justus Abhulimen, Security Leader at Twilio

Outcome and Benefits of Service:

- Operational efficiencies:
  - 33% reduction in staffing requirements across analyst, incident manager, and SOC operators, enabling enterprise-grade security across its growing programs without proportional staff increases. (Programs enabled: employee safety, executive protection, travel security, investigations, insider risk, and workplace violence management)

    - 80% reduction in time spent collating and reporting information, saving 750+ hours annually on bi-weekly reporting alone.
    - Threat assessment and investigation timelines shortened from 1-2 weeks to 1-3 days, saving hundreds of manual research hours monthly as case volume grows.
- Technology consolidation:
    - Realized $180,000+ annually in direct cost savings by replacing multiple systems with a single platform.
- Regulatory compliance achievement:
    - Successfully meeting California Senate Bill 553 reporting requirements for workplace violence through improved data collection and standardized procedures, avoiding potential fines of up to $25,000 per violation.
- Enhanced security value and proactive risk management:
    - Providing superior "duty of care" by reducing incident resolution time from 1 week to 48 hours, and meeting industry-leading response service-level agreements (SLAs).
    - Delivering a Trusted Traveler Program with risk assessments tailored to each employee's role, access privileges, and specific threat profile.
    - Improved risk forecasting, threat assessment, and automated monitoring capabilities across the organization.
- Strengthened cross-functional collaboration:
    - For example, Ontic enabled Twilio to implement automated workflows that connect security, legal, HR, and employee relations through customized notification systems to the tune of a 65% increase in operational assurance allowing more consistent and timely multi-department responses to incidents worldwide.

By purchasing Ontic's platform and its capabilities, Twilio's security organization’s confidence in delivering its goals and value proposition to Twilio went from 5/10 before Ontic to 9/10 after Ontic.

“The strength of Ontic is that it allows us to capture data and be insightful. We can tell detailed stories about what's happening in our environment—not just the what, but the how and why. This allows us to demonstrate our value to executive leadership in a tangible way."
- Justus Abhulimen, Security Leader at Twilio

SIP Case Study Authentication Process

This process was overseen by a Security Executive Council subject matter expert with 20+ years of experience in developing and leading people and asset protection programs as a trusted security advisor for global, multinational organizations. Client end-user authenticated **April 2025.**

Note: *The Security Executive Council's Solution Innovation case study represents a snapshot in time to demonstrate a solution to a specific organization's issue. End-user diligence, trial and measurement are strongly recommended for any contemplated risk mitigation activity.*

A General Comparison of Competition

Client Service/Resource Attributes or Capabilities	Ontic	Company A	Company B	Company C	Company D	Company E
1. Enterprise security management system for data tracking, workflow automation and reporting	YES	NO	NO	NO	NO	NO
2. Open-source threat intelligence - keyword-based monitoring	YES	YES	NO	NO	NO	NO
3. Broad risk and news alerts	YES	NO	YES	NO	NO	NO
4. Investigative research	YES	NO	NO	YES	NO	NO
5. Behavioral threat assessments	YES	NO	NO	NO	YES	NO
6. Incident and case management	YES	NO	NO	NO	NO	YES
7. Site risk and vulnerability assessments	YES	NO	NO	NO	NO	NO
8. Data integration with broader organizational data systems (HR, IT, etc.)	YES	NO	NO	NO	NO	YES

See other case studies and learn more about the SIP Program here:
https://www.securityexecutivecouncil.com/solutions/vendor-innovations