Synack

CASE STUDY

How Accenture Partners with Synack to Reduce MTTR

Executive Summary

To secure a sprawling digital attack surface and a global workforce of over 800,000, Accenture required an offensive security partner that could scale and truly reduce risk. By partnering with Synack, the company moved beyond point-in-time compliance audits toward a model of continuous offensive security. By integrating the Synack PTaaS platform and the Synack Red Team (SRT), an elite community of researchers, Synack provided a human-led offensive security partner that mimics real-world adversaries. By leveraging the experience of the SRT, Accenture was able to transition to a proactive, intelligence-driven defense. This strategic shift has empowered Accenture to automate internal protections and maintain a rigorous 7-day remediation target for its most critical risks.

The Challenge: Rapid AI Adoption and Static Security

"You can't train your way out of a problem at this scale," says Kris Burkhardt, Accenture Global CISO. "We hire close to 80,000 new people every year. We needed a technical backstop to catch what human training alone cannot." Traditional penetration testing for compliance—often a once-a-year exercise—wasn't enough to secure Accenture's attack surface. They needed a partner that could match their scale, speed and the creative agility of AI-enabled modern attackers.

accenture

CHALLENGE

With 800,000 employees and a 10% annual turnover rate, Accenture couldn't rely on compliance pen testing alone. They needed a testing solution that could match the pace of continuous code deployment and scale to cover their global attack surface.

SOLUTION

Accenture partnered with Synack to implement their Synack PTaaS Platform for continuous, offensive security testing. By moving away from point-in-time audits and utilizing Synack's elite community of researchers, the Synack Red Team, Accenture gained a persistent, 24/7 offensive security partner for their global assets.

RESULTS

- Eliminated entire vulnerability classes over 6 years by turning Synack findings into automated Pen Test Bots
- Helped secure the deployment of 3,000+ internal AI agents
- Reduced mean time to remediate (MTTR) by setting aggressive 7-day fix targets for critical findings
- Secured an expanding AI and data workforce that grew to 77,000 specialists in 2025

"In two years, Accenture grew its AI and data employee base from 40,000 to 77,000 and delivered more than 6,000 advanced AI projects in its 2025 fiscal year." (crn.com, 2025) As Accenture teams rapidly develop AI and LLM-based applications, deployment timelines have also shrunk. They needed a partner capable of matching their speed and providing continuous security validation as they onboard new technical stakeholders. How did they secure their dynamic and growing attack surface from security threats as they deployed these AI technologies?

The Solution: Continuous Offensive Security

Since partnering with Synack, Accenture has moved beyond simple bug hunting. They use Synack's platform data to identify root causes and enhance protections. By analyzing patterns in the vulnerabilities Synack finds, Accenture's security team has created new tools that have almost completely eliminated entire classes of vulnerabilities over the last six years.

One standout success involved identifying unauthenticated objects buried deep within complex web applications. "Synack found these needles in the haystack," Burkhardt explains. "It opened our eyes to a broader issue, leading us to build our own internal scanning tools—we call them PenBots—to proactively hunt for those vulnerabilities across our entire attack surface."

> "We don't just want to fix a bug; we want to make the organization smarter. Synack helps us learn from our mistakes so we don't repeat them."
>
> KRIS BURKHARDT, GLOBAL CISO, ACCENTURE

A key driver of this progress is Accenture's shift toward continuous penetration testing. Instead of relying on periodic scans, they maintain a constant visibility into their attack surface to uncover weaknesses as they emerge, including zero-day exploits.

> In the last 12 to 24 months, zero-day attacks have taken on a different aspect. AI-enabled threat actors now use "zero-day engines"—infrastructure where they can load an exploit and hit as many targets as possible in the least amount of time. To counter this, our defenses must evolve. Continuous pentesting is a straightforward way to address this; by constantly looking for weaknesses, you can break the chain of a zero-day attack before it links several vulnerabilities together.
>
> KRIS BURKHARDT, GLOBAL CISO, ACCENTURE

A continuous testing model is critical in modern environments where teams frequently release code and might unintentionally reintroduce resolved vulnerabilities. Through a combination of continuous penetration testing backed by human expert analysis, Accenture is able to ensure that potential risks are identified quickly for new or critical assets.

Defending at the Speed of AI

As Accenture expands its internal use of AI, risks of vibe coding and rapid-fire deployments increases. This is a critical factor as the company has already deployed 3,000+ internal AI agents. Burkhardt uses Synack's continuous testing as a critical guardrail for this innovation.

"The fun part of AI is enablement; the not-so-fun part is defending against AI-powered attacks," says Burkhardt. "You have to move at AI speed. Continuous testing ensures that as our teams release code every hour, we aren't unknowingly reintroducing old flaws."

Communicating Value to the Board

For the board, Burkhardt doesn't talk about "millions of vulnerabilities." He talks about control systems and business risk. By using Synack's reporting dashboard in the Synack PTaaS platform to show consistent progress in reducing MTTR and preventing repeat vulnerabilities, he demonstrates that Accenture's security enables the success of the company's overall business strategy.

"Synack has been a partner that causes change for good," Burkhardt concludes. "They help us prove to our leadership and our clients that we are securing tomorrow, today."

The Synack Advantage

MOVING BEYOND CHECK-THE-BOX COMPLIANCE

With Synack, Accenture moved from annual audits to a continuous testing model that mimics real-world adversaries, catching the needles in the haystack that automated scans can miss.

FIND VULNERABILITIES THAT MATTER

Synack's platform provides clean, actionable data that allows Accenture to prioritize high-impact fixes, reducing their MTTR and focusing developer energy where it matters most.

ROOT CAUSE ANALYSIS

Accenture uses Synack findings to create automated internal tools that prevent the same vulnerabilities from ever reappearing, giving the CISO more control over the digital attack surface.

About Accenture

Accenture is a leading solutions and services company that helps the world's leading enterprises reinvent by building their digital core and unleashing the power of AI to create value at speed across the enterprise, bringing together the talent of our approximately 786,000 people, our proprietary assets and platforms, and deep ecosystem relationships. Our strategy is to be the reinvention partner of choice for our clients and to be the most client-focused, AI-enabled, great place to work in the world. Through our Reinvention Services we bring together our capabilities across strategy, consulting, technology, operations, Song and Industry X with our deep industry expertise to create and deliver solutions and services for our clients. Our purpose is to deliver on the promise of technology and human ingenuity, and we measure our success by the 360° value we create for all our stakeholders.

Visit us at www.accenture.com.

About Synack

Synack delivers continuous security validation through its Human + AI platform for continuous pentesting. Sara AI Pentesting, powered by the Synack Autonomous Red Agent, combines agentic AI with the Synack Red Team—the world's most rigorously vetted community of security researchers—to help organizations proactively reduce risk, stay compliant, and stay ahead of evolving cyber threats. Sara handles reconnaissance, attack surface mapping, and initial exploit validation at scale, while human experts validate real-world exploitability and provide the creativity and judgement automation cannot replicate. Founded by former NSA operatives, Synack has enabled nearly 10 million hours of security testing to protect critical assets, from global financial systems to U.S. Defense Department networks. Synack was recognized by GigaOm's 2025 PTaaS Radar as both a Leader and Fast Mover, and received Global InfoSec Awards for Market Leader in AI-Powered Cybersecurity and Trailblazer in PTaaS.

Learn more at www.synack.com.

Synack