HORIZON3.ai

~~TRUST BUT~~ VERIFY

CASE STUDY

Hack Yourself First: How Jerome's Furniture Moved from Compliance to Real Security

How Jerome's Furniture Discovered and Fixed Its Biggest Cybersecurity Gaps Before Attackers Could

The retail industry is facing an unprecedented wave of cyber threats. With the rapid adoption of cloud-based operations, digital payment systems, and third-party integrations, retailers have become prime targets for ransomware, data breaches, and supply chain attacks. At the same time, regulatory requirements like PCI DSS and evolving compliance standards demand stricter security controls—but compliance alone doesn't guarantee protection.

Many retailers are realizing that checking security boxes isn't enough; they need proactive, real-world attack simulation to uncover hidden vulnerabilities before cybercriminals do.
This is the challenge that Jerome's Furniture solved by shifting from traditional vulnerability management to autonomous penetration testing.

For decades, Jerome's Furniture has been a trusted name in Southern California, growing from a family-owned business into a regional powerhouse with 15 large-format stores and five smaller locations. As the company expanded, so did its reliance on digital infrastructure: first by transitioning from green-screen terminals to modern networks, and then embracing cloud-based operations. But as technology evolved, so did cyber threats, and IT Director Adam Warren quickly realized that checking compliance boxes wasn't enough to stay secure.

About Jerome's Furniture

Mission: Jerome's Furniture is committed to providing high-quality home furnishings at everyday low prices, treating customers like family, and ensuring transparency, service, honesty, quality, and a family-oriented approach in all interactions.

Year Founded: 1954

Number of Staff: Approximately 600 employees

Area of Operation: Jerome's Furniture operates primarily in Southern California, with multiple showrooms across the region, including locations in San Diego, Los Angeles, Orange County, and the Inland Empire.

Historically, Jerome's followed the traditional cybersecurity playbook: periodic vulnerability scans to satisfy PCI DSS compliance, expensive security tools that produced overwhelming amounts of data, and manual remediation efforts that left the lean IT team stretched thin.

HORIZON3.ai
~~TRUST BUT~~ VERIFY

But despite their best efforts, the fundamental problem remained: "*We were staring at thousands of vulnerabilities, trying to figure out what mattered most*," Adam recalled.

The Gap Between Compliance and True Security

Retailers like Jerome's faced two major attack vectors: cybercriminals looking for exploitable weaknesses to steal data or deploy ransomware, and regulatory bodies tightening compliance requirements that didn't always translate into real security. As Adam explained, "Ransomware attacks are still a big deal. Data breaches are another one. That's what keeps me up at night."

For example, in 2023, a major British Retailer suffered a large cyberattack which exposed sensitive employee data due to outdated security measures. This is just one example of the growing risks in the retail sector.

> "The interesting thing about governance, risk, and compliance… there's compliance programs, and then there's actual security. They overlap somewhat, but they don't totally overlap. **You could be totally compliant with NIST and still get taken out.**"
>
> - Adam Warren

The realization was stark: *Jerome's needed think like attackers before attackers struck.*

Rethinking Security: Discovering Autonomous Pentesting

The turning point came when Adam attended a cybersecurity conference, where he was introduced to Horizon3.ai's NodeZero® autonomous penetration testing platform. Unlike traditional vulnerability scanning tools, which produce long lists of issues without context, NodeZero emulates real attack vectors, demonstrating how an attacker could exploit weaknesses, move laterally, and escalate privileges—all in a safe and controlled manner.

Intrigued by its proactive approach, Adam initiated a trial at Jerome's. The results were immediate and shocking.

Immediate Impact: Testing Like an Attacker

As soon as NodeZero was deployed, Jerome's entire security alert system lit up. The autonomous pentest exposed vulnerabilities that no other tool had flagged, identifying gaps in both their cloud and on-premises infrastructure. "***We rattled everybody's chain!***" Adam admitted, recalling the flood of alerts when NodeZero first ran.

Spend the effort on stuff that actually matters
because there's a lot of noise you can waste time on!
- Adam Warren

Rather than drowning the IT team in thousands of findings, NodeZero prioritized what actually mattered, showing exactly which vulnerabilities an attacker would exploit first. Even more importantly, it provided step-by-step remediation guidance, enabling the team to fix critical issues in days rather than weeks.

This wasn't just another compliance tool. It was a tool that enabled Jerome's to look at their environment from the perspective of an attacker, while also allowing them to continuously test their defenses, instead of waiting for costly annual or quarterly security reviews.

> "In the real world, if you put a computer on a public IP, it's got constant noise of things attacking it 24/7. **You need to do that to yourself, think like an attacker.**"
>
> - Adam Warren

Measurable Results: Strengthening Jerome's Security Posture

With NodeZero fully integrated into their security operations, Jerome's saw significant improvements right away:

- The IT team reduced vulnerability mean-time-to-remediation (MTTR) by 75%, eliminating critical security gaps that had gone unnoticed for years.
- PCI DSS compliance became more than just a checkbox exercise. For the first time, Jerome's could validate that their security measures were actually working against real-world threats.
- By replacing legacy security tools with NodeZero, the company reduced costs while improving security efficiency.

Adam explained that NodeZero is invaluable for PCI compliance. NodeZero proves that their security measures are truly effective, instead of just checking boxes, enabling them to see firsthand that their defenses are actively preventing real-world attacks.

The shift from reactive to proactive security meant that instead of scrambling to address vulnerabilities before an audit, Jerome's could now continuously test and improve its security posture on its own terms.

The Future of Security: Preparing for AI-Driven Threats

While NodeZero transformed Jerome's cybersecurity operations, Adam knows that cyber threats are constantly evolving, especially with the rise of AI-powered cyberattacks. The same automation and intelligence that helps defenders is also empowering attackers, making it critical to stay ahead.

To stay ahead, Jerome's is expanding its use of autonomous penetration testing, integrating continuous assessments into its broader security strategy.

> We're saying great, AI raises your skill level, raises your productivity… **but the problem is that the bad guys can do that too.** They're going to have all the same tools. So, I think we have to have our robots fighting their robots.
>
> - Adam Warren

Lessons for Other Retailers

Adam's experience at Jerome's offers key takeaways for retailers and security leaders everywhere:

Compliance ≠ Security

Passing an audit doesn't mean your company is safe.

Attack Yourself First

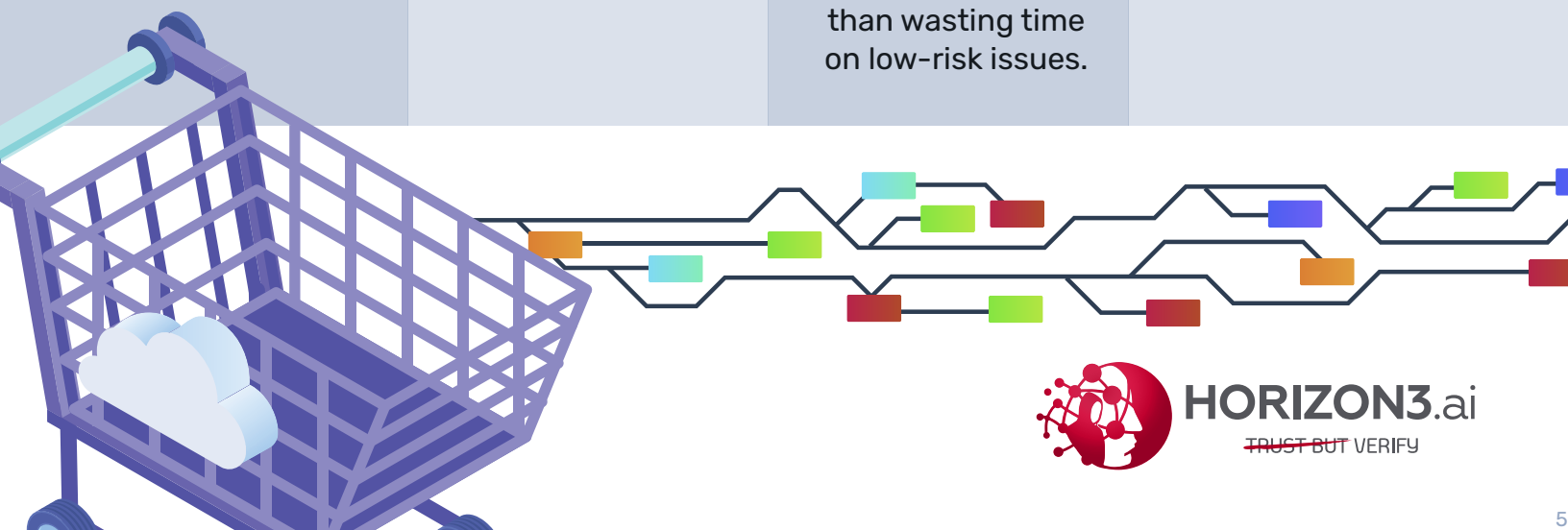
If you don't, attackers will.

Prioritize What Matters

Fix vulnerabilities that are actually exploitable rather than wasting time on low-risk issues.

Continuous Testing is the Future

Cyber threats don't wait for annual scans.



HORIZON3.ai
~~TRUST BUT~~ VERIFY

> "Retailers need to start thinking like attackers—
> **before attackers do."**
> - Adam Warren

Conclusion: A New Standard for Retail Cybersecurity

Jerome's Furniture has revolutionized its security strategy by embracing autonomous penetration testing, shifting from a reactive, compliance-driven approach to a proactive, attack-driven defense model where offense informs and strengthens defense. Instead of relying on periodic scans and hoping their security measures are enough, they now validate their defenses continuously, just like an attacker would.

With NodeZero, Jerome's has flipped the script on their cybersecurity strategy. No longer waiting for annual audits or external tests, they now run real-world attack simulations on demand, uncovering weaknesses before adversaries can exploit them.
This shift has transformed their security posture, giving them actionable insights, faster remediation, and confidence that their defenses are truly effective and not just compliant. By hacking themselves before attackers can, Jerome's is staying ahead of cybercriminals, setting a new cybersecurity standard for the retail industry.

- **Built for organizations of all sizes, you can experience the game-changing power of NodeZero today!**

 𝕏 @Horizon3ai ✉ info@horizon3.ai www.horizon3.ai

HORIZON3.ai
~~TRUST~~ BUT VERIFY