Teqtivity Analysis: Enterprise ITAM Vendor Response Times Create Critical Security Vulnerabilities Across Organizations

CERRITOS, CA, UNITED STATES, January 22, 2026 /EINPresswire.com/ -- Teqtivity's latest findings reveal a troubling pattern in the enterprise IT Asset Management (ITAM) market: organizations purchasing premium platforms for security and compliance are being locked out of critical vendor support precisely when they need it most. The company's research into mid-market organizations' experiences shows that multi-day and even multi-week vendor response times are creating the exact security gaps these tools were designed to prevent.

The findings highlight a fundamental contradiction in the enterprise ITAM model. Organizations invest in these platforms specifically to maintain device visibility, track asset lifecycles, and ensure security compliance. Yet when urgent situations arise—emergency device recalls, offboarding security incidents, compliance audit preparations—many discover their vendor support operates on timelines incompatible with security requirements.

"We're seeing companies switch to Teqtivity after the same experience: they bought what they thought was enterprise-grade support, but when a critical issue emerged, they couldn't reach anyone who could actually help," says Hiren Hasmukh, CEO and Founder of Teqtivity.

The Real-World Impact of Support Delays

The consequences extend far beyond frustration. When ITAM platforms fail or require urgent reconfiguration, the operational and security impacts cascade quickly. Devices go untracked during critical transition periods. Former employees retain access to company systems. Security teams lose real-time visibility into their infrastructure. Compliance auditors find gaps in asset documentation.

According to industry data, 71% of organizations report ex-employees failing to return company equipment, with 59% of that unreturned equipment containing sensitive information. These statistics shift from concerning data points to active security incidents when IT teams can't access timely vendor support to lock down devices or update tracking configurations.

The problem intensifies in distributed work environments where asset visibility already presents challenges. Organizations managing remote and hybrid teams need responsive ITAM support to address device issues, update configurations, and maintain security protocols across dispersed

infrastructure. Multi-day vendor response times effectively eliminate the real-time asset intelligence these tools promise.

What Creates the Support Gap

Several structural factors contribute to inadequate enterprise ITAM support:

Multi-tiered support structures that prioritize ticket queuing over problem resolution, often routing basic technical questions through multiple levels before reaching platform engineers who can actually address deployment-specific issues.

Response time frameworks optimized for vendor workflows rather than customer urgency, with SLA measurements that may promise 24-48 hour acknowledgment but provide no guarantee of actual resolution timelines.

Limited platform expertise in front-line support teams, requiring escalation for anything beyond standard troubleshooting and creating delays when organizations face unique deployment challenges or urgent security requirements.

Lack of proactive engagement during critical incidents, leaving organizations to manage security situations without the vendor expertise they believed they were purchasing as part of enterprise-grade service.

"The irony is profound," Hasmukh notes. "Companies choose these platforms specifically because they promise enterprise-grade everything. What they often discover is enterprise-grade wait times paired with tier-one support reading from scripts that don't address their specific deployment."

Rethinking Support as a Security Feature

The disconnect between ITAM platform capabilities and support responsiveness highlights a broader industry issue: treating customer support as a cost center rather than a core security feature. In an environment where asset visibility directly impacts security posture, vendor responsiveness becomes as critical as platform functionality.

Organizations increasingly recognize that ITAM support requirements mirror the urgency of their security needs. When a device goes missing, when offboarding protocols fail, when compliance audits require immediate documentation, support response time directly determines security outcome.

Teqtivity's approach centers on treating support as fundamental product functionality rather than post-sale service. Direct access to platform engineers, same-day response commitments, and proactive deployment assistance operate as security features, not service extras—regardless

of organization size or contract value.

"We built Teqtivity because we were frustrated with how IT vendors treated customers," says Hasmukh. "When your ITAM system needs urgent changes for security reasons, you shouldn't wait in a ticket queue. You should have someone who knows your deployment helping you fix it immediately."

Looking Forward

As organizations face mounting pressure to maintain asset visibility across distributed workforces, vendor support responsiveness is shifting from service differentiator to security requirement. The ability to access immediate, knowledgeable vendor assistance when ITAM systems require urgent attention is becoming essential infrastructure, not a premium feature.

The market is beginning to recognize this shift. Organizations evaluating ITAM platforms increasingly treat support response times and engineer accessibility as core selection criteria, alongside traditional feature comparisons. This evolution suggests the industry may be moving toward models where responsive support becomes a competitive necessity rather than a value-add.

For mid-market organizations caught between enterprise-scale ITAM needs and small-business vendor treatment, the support gap represents both immediate risk and strategic consideration. As asset management requirements grow more complex and security stakes increase, vendor responsiveness increasingly determines whether these platforms deliver on their core promise: maintaining the asset visibility that makes security possible.

For more information about Teqtivity's approach to IT asset management and security-focused support, visit www.teqtivity.com.

About Teqtivity

Teqtivity is a provider of IT asset management (ITAM) solutions designed to help businesses track and manage their IT assets throughout their entire lifecycle. Teqtivity's software provides businesses with the visibility they need to make informed decisions about their assets, and it helps them to save time and money. To learn more about Teqtivity, please visit www.teqtivity.com.

Rishi Simbudyal
Teqtivity, Inc
hello@teqtivity.com
Visit us on social media:
LinkedIn

Facebook
X