BTR: As Workloads Move Back On-Prem, Hypervisors Emerge as a Quiet Mid-Market Risk

WASHINGTON, DC, UNITED STATES, February 11, 2026 /EINPresswire.com/ -- For much of the past decade, organizations of all sizes have appeared to pursue an overarching IT strategy focused on a steady migration to public cloud services. Today, rising costs, regulatory demands, and the growing use of AI are leading many, especially in the mid-market, to reconsider how much computing should be outsourced and how much should be brought back on-prem for more direct management.


Anthony Gadient, Vali Cyber

As a result, a growing share of computing is moving back to dedicated data centers and private cloud environments. Manufacturing firms, healthcare providers, retailers, and logistics operators are reassessing where mission-critical workloads run and how much control they retain over sensitive data. In so doing, it is elevating a layer of risk that has not received a lot of attention: the hypervisor.

At its simplest, hypervisors are the software foundation that lets organizations consolidate many servers and applications onto shared infrastructure. It determines how computing resources are used, creating a single management layer that supports dozens or hundreds of systems at once. This is what most executives may know as “virtualization,” the technology that allows computing resources to be pooled, shared, and managed in a flexible rather than a fixed manner. For many executives, virtualization has long been synonymous with investments in VMware, which has, for years, dominated enterprise and mid-market virtual infrastructure.

In a recent BizTechReports executive vidcast interview with the father and son team of Anthony J.

Gadient, Chief Executive Officer and Cofounder of Vali Cyber, and Austin Gadient, the company's Chief Technology Officer and Cofounder, the two argued that hypervisors are increasingly attractive targets for attackers precisely because of their central role in modern infrastructure.


Austin Gadient, Vali Cyber

Virtualization's Return to Center Stage

Virtualization has long been foundational in large enterprise IT environments, enabling organizations to consolidate hardware, balance workloads, and scale applications efficiently. While often associated with Global 2000 organizations, virtualization has in recent years become more deeply embedded in mid-market environments as declining virtualization costs brought enterprise-class capabilities within reach for smaller IT budgets.

In the past year or so there has been growing interest in IT repatriation from the cloud as a result of private AI initiatives. They have introduced a new class of workloads that place a premium on control, cost predictability, and data stewardship. As a result, rather than relying exclusively on public large model providers, many organizations are deploying their own language models inside their environments to preserve data privacy, manage costs, and reduce dependency on external platforms.

> For mid-market leaders, the message is pretty clear. Hypervisors need to be treated as critical infrastructure and reviewed accordingly, not left outside formal security and resilience oversight."
>
> *Austin Gadient, Vali Cyber*

Because these models are resource-intensive, executives have started looking for ways to extract maximum value from expensive GPUs and servers through virtualization, triggering renewed and heightened interest in hypervisors as the operational backbone for sensitive, high-value workloads.

It is a trend that has not been missed by individuals and entities looking for breach opportunities because hypervisors can be a single point of failure that can wreak havoc on otherwise well protected organizations.

“If hypervisors are compromised,” Austin Gadient said, “you’re not dealing with one system. You’re dealing with everything that runs on top of it.”

Hypervisors Enter the Formal Threat Model

Hypervisors, as a point of vulnerability, have been largely overlooked until recently. In April 2025, MITRE formally updated its ATT&CK framework [https://attack.mitre.org/resources/updates/updates-april-2025] to recognize VMware ESXi and other hypervisor environments as a distinct area of interest for bad actors. A nonprofit organization that develops widely used cybersecurity and defense frameworks for government and industry, MITRE has observed and tracked a growing array of tactics that target virtualization layers directly rather than individual endpoints or applications.

“For mid-market leaders, the message is pretty clear. Hypervisors need to be treated as critical infrastructure and reviewed accordingly, not left outside formal security and resilience oversight,” he added.

The Economics of Control

The return of workloads on-prem is not a rejection of cloud computing, but a recalibration. Analyst research suggests that organizations are becoming more deliberate about which workloads belong in public cloud environments and which are better suited to private infrastructure.

Forrester’s 2025 cloud predictions [https://www.forrester.com/blogs/predictions-2025-cloud] highlight accelerating private cloud adoption alongside AI initiatives, particularly in organizations facing data sovereignty, security, and cost-management pressures. Rather than a wholesale retreat from the cloud, Forrester describes a hybrid equilibrium, with sensitive or high-cost workloads deliberately placed closer to home.

That equilibrium has architectural consequences. These hybrid environments rely heavily on virtualization to achieve efficiency and scale. In concentrating workloads on shared infrastructure, they also concentrate risk, making hypervisors high-value targets for disruption.

Ransomware and the Supply-Chain Multiplier

“Attackers have proven adept at identifying where disruption carries the greatest economic impact. Hypervisors provide precisely that leverage. A successful attack can disable dozens or hundreds of virtual machines at once, magnifying downtime and increasing pressure to pay ransoms,” said CEO Anthony Gadient.

The supply-chain implications are particularly acute for mid-market organizations whether they

are manufacturers, distributors, or service providers because they often serve as critical links in larger ecosystems. A single outage can cascade downstream, halting production lines, delaying shipments, or emptying retail shelves. For mid-market firms operating on thin margins, prolonged downtime can not only be painful but also existential if larger trading partners question their ability to protect themselves in today's fraught cyber landscape.

Adding insult to injury, while the hypervisor risk is growing, the resources to manage it are not. This further stacks the odds against mid-market players. Large enterprises maintain security operations centers staffed around the clock. Mid-market organizations rarely can. They rely on lean IT teams, managed service providers (MSPs), or managed security service providers (MSSPs) to cover a broad and growing attack surface.

While this mismatch is not new, it is becoming more pronounced as infrastructure grows more complex. Gartner's 2025 cybersecurity trends research warns that persistent shortages of experienced security professionals are colliding with rising attack sophistication, particularly as AI expands both defensive and offensive capabilities. Gartner reports that many organizations will be unable to sustain purely reactive, detection-and-response security models without unsustainable increases in cost and headcount.

This reality is forcing a shift toward automation and autonomy, especially in infrastructure layers where response time is critical, assuming time is even available to prevent damage from taking place.

Security professionals are consequently challenging traditional assumptions about the time needed to detect suspicious behavior, time to alert analysts, and time to respond when hypervisor attacks compress that window dramatically. By the time human responders engage, damage may already be widespread.

From Detection to Preemption

Anthony Gadient described a growing emphasis on preemptive controls that operate autonomously at the infrastructure layer. Rather than relying on cloud-based analysis, and therefore delayed response, a new generation of systems is emerging to enforce protections locally and immediately to stop malicious activity before it cascades across virtual environments. Logs and telemetry can still be forwarded to MSPs or MSSPs for visibility and forensic analysis, but the initial containment must happen right away without human intervention.

It is an approach that aligns with broader architectural trends toward keeping intelligence closer to the workload, particularly in environments driven by private AI and data sovereignty concerns. For many mid-market organizations, these conditions make it increasingly difficult to rely on security approaches that focus on continuous monitoring and rapid human response.

Preparing for the Pendulum Swing

As workloads rebalance between public cloud and private environments, the challenge for mid-market organizations is scaling protection without scaling headcount. The emerging consensus among analysts and practitioners alike is that resilience must be designed into the architecture itself, rather than bolted on through manual processes that assume constant human oversight.

That reality is shaping how Austin Gadient approaches product design at Vali Cyber. Rather than assuming the presence of a fully staffed security operations center, he said the goal has been to build protections that operate autonomously at the infrastructure layer, containing attacks before they cascade and minimizing the need for real-time human intervention.

That starts with identifying which systems would cause the greatest operational damage if compromised and ensuring those layers are not left to reactive controls alone. Hypervisors increasingly meet that test, as they concentrate both computing capacity and operational risk in a single control plane.

Click here to read the Q&A based on this interview.

Airrion Andrews
BizTechReports
email us here