The data center is becoming a security enforcement layer

March 30, 2026 By: Joan Goodchild CIO

https://www.cio.com/article/4151802/the-data-center-is-becoming-a-security-enforcement-layer.html

At RSAC 2026, two converging trends made one thing clear: security is moving inside the runtime.

The security model most enterprises still rely on assumes there is time to respond, time to patch, time to detect, time to contain when an attacker gets in, but there is still time to stop them before they can move through the environment and do harm.

Last week, I attended RSA Conference 2026 and attended several sessions where that assumption came under pressure from multiple directions. Across talks on runtime defense and Kubernetes security, a consistent theme emerged: both the time defenders have to act and the distance attackers need to travel are rapidly collapsing.

In the session “When AI Steals Your Patch Window: Beating the Clock with Runtime Defense,” Dan Wendlandt, vice president of product management at Cisco, described how quickly the traditional vulnerability lifecycle is breaking down. AI is accelerating every phase of exploitation by identifying vulnerabilities in widely deployed code and generating working exploits.

In one example in Wendlandt’s session, attackers moved from vulnerability disclosure to target identification within hours, with exploit code and active attacks following shortly after. The implication is straightforward: Organizations cannot patch fast enough to keep pace with exploitation timelines that are increasingly measured in hours, not weeks.

Modern infrastructure removes friction for an attacker

If faster exploitation were the only issue, defenders might still rely on segmentation and layered controls to slow attackers down. But modern environments are removing that friction.

In “K8s Post-Exploitation Spinoff,” Roi Nisimi, principal security researcher at Orca Security, explained how Kubernetes fundamentally changes what happens after initial

access. In traditional environments, attackers had to navigate segmented networks, escalate privileges step by step, and work to reach sensitive systems. That process introduced time and resistance. In Kubernetes, that distance largely disappears. Clusters are often flat by default, workloads are tightly interconnected, and identity becomes the primary control mechanism. Once inside, attackers can move quickly across services, access credentials, and escalate privileges.

As Nisimi showed, the gap between access and impact has effectively collapsed. In some cases, attackers can move from initial access to meaningful control in minutes. Taken together, these trends expose a fundamental weakness in traditional security models. By the time an attack is detected, exploitation may already have occurred and lateral movement may already be underway. Controls that rely on perimeter inspection or post-execution response are operating too far from where attacks actually unfold. The response emerging across sessions is not simply faster detection, but a shift in where security is enforced.

Wendlandt pointed to technologies like eBPF, which allow security logic to run directly inside the operating system kernel. From that position, security tools can observe and act on system behavior in real time. Because these controls operate inline, they can prevent actions before they complete, rather than reacting after execution .
That changes the model because processes can be blocked before they start, exploit chains can be interrupted mid-execution and lateral movement can be stopped inside the environment. Instead of relying on visibility alone, organizations can enforce policy at the point where workloads actually run.

The data center is becoming the control layer

One of my takeaways from the sessions is that the combination of faster attacks and more connected environments is forcing a different role for the data center. For years, infrastructure strategy has been framed around where applications run: on-premises or in the cloud. But that question is becoming secondary to a more urgent one: where can control actually be enforced?

Increasingly, the answer is inside the environment itself. The data center is no longer just where applications run. It is becoming the place where security decisions are enforced — where behavior is monitored and actions are either allowed or stopped in real time.

That shift shows up in several ways:

- Workload identity becomes the primary control point. In environments like Kubernetes, identity determines what a workload can access, often regardless of network location. Enforcing least privilege at that layer becomes critical because once identity is compromised, movement is immediate.
- Runtime behavior becomes the enforcement surface. Instead of relying on detection after execution, controls are moving inline — inside the operating system and runtime — where processes can be blocked before they start and exploit chains can be interrupted midstream.
- Internal traffic matters more than perimeter traffic. East-west movement inside environments is now where attacks succeed or fail. That makes visibility and control inside the data center more important than inspection at the edge.
- Policy has to follow the workload. In hybrid and multi-cloud environments, workloads move constantly. The only way to maintain consistent security is to enforce policy wherever the workload runs, not just at a fixed boundary.

As these changes take hold, the data center — whether physical or cloud-based — becomes less about infrastructure and more about control. It is where organizations can enforce consistent security decisions across increasingly fragmented environments. And as the gap between access and impact continues to shrink, that enforcement layer is becoming not just important, but essential.

What CIOs need to rethink

For CIOs, the takeaway is not simply that threats are increasing. It is that the underlying model of defense is changing. For years, security strategy has been built on a sequence: prevent what you can, detect what you miss, and respond before damage spreads. That sequence assumed time and separation — time to react, and distance between initial access and meaningful impact. But both are disappearing.

Three shifts now stand out:

- From patching to protection. Patching remains necessary, but it can no longer serve as the primary line of defense. Vulnerabilities are being exploited faster than organizations can remediate them, often within hours of disclosure. That forces a shift in mindset. Instead of assuming vulnerabilities will be fixed before they are used, organizations have to assume exploitation will happen and design controls that limit what an attacker can do in that window. The focus moves from eliminating risk to containing it.
- From perimeter to runtime . The traditional model placed heavy emphasis on the network edge: firewalls, gateways, and access controls designed to keep threats out. But in environments where workloads are distributed, interconnected, and often ephemeral, the

perimeter is no longer a reliable boundary. Security has to move closer to where applications actually run. That means operating inside containers, virtual machines, and orchestration layers, where identity, behavior, and interaction can be observed and controlled directly.

- From detection to enforcement . Detection remains important, but it is no longer sufficient on its own. By the time an alert is generated, an attacker may have already executed code, established persistence, or begun moving laterally. The priority shifts to controls that can act in-line — blocking a process before it executes, preventing a privilege escalation, or stopping a suspicious connection as it happens. In this model, enforcement is not a follow-on step. It is the control point.

Security is moving from a reactive discipline to a continuously enforced system of control embedded within the infrastructure itself. For CIOs, that requires rethinking not just tools, but architecture, how environments are designed, where controls live, and how consistently they can be applied as applications move across platforms. The question is both if you can stop an attack and also where it actually happens.

Rethinking where security lives

The industry has spent the last decade optimizing where applications run. Now it is being forced to rethink where security happens. As AI accelerates exploitation and modern infrastructure accelerates attacker movement, enforcement is moving closer to the workload itself. The data center is no longer just infrastructure. It is becoming the last place security can still hold.