Rethinking connectivity: Why SMBs need network intelligence to tackle modern DDoS

Consider an e-commerce business during a festive sale. Traffic appears healthy, analytics dashboards show steady user activity. Yet, as customers move to checkout, payment pages begin to lag. Transactions take longer to process, and a small but critical percentage of users drop off. What sits underneath is not a surge in demand, but a sustained stream of bot-driven requests hitting checkout APIs in ways that mimic genuine purchase behaviour.

In a logistics company, shipment tracking, which is an API-driven function, starts to slow down. Customers and internal teams experience delays in retrieving real-time updates. The infrastructure is not down; instead, backend systems are being gradually exhausted by repeated, valid-looking queries that never trigger traditional rate limits.

In SaaS environments, a business platform may notice intermittent delays in user authentication. Login attempts appear legitimate with the correct formats and distributed origins. But they are orchestrated to consume resources at the application layer.

The common factor across all these scenarios is **the modern distributed denial-of-service (DDoS) attack,** and it's hard to detect or isolate. In each of these instances, the network itself appears stable, and bandwidth continues to be available. There are no dramatic spikes, yet business is being actively disrupted. Over time, this creates latency that impacts real users, without setting off conventional DDoS alarms.

New in DDoS attacks: From flooding pipes to impersonating users

A distributed denial-of-service (DDoS) attack is when a website or app gets flooded with fake requests from many sources at once, making it inaccessible to genuine users.

Traditional DDoS attacks were blunt instruments. The idea was to overwhelm bandwidth, exhaust infrastructure and bring systems down. These were easy to detect and relatively easier to mitigate.

Today's attacks are different. These operate at the application layer where business logic lives. Instead of flooding a network, they log in like users, browse like customers, and hit APIs like legitimate applications. This shows up as a kind of 'low and slow' burn rather than a system crash, as slow checkout pages, APIs timing out and an erosion in the customer experience.

Understanding the two faces of DDoS: Volumetric vs. application-layer attacks

Think of volumetric attacks as similar to a highway jammed with traffic until movement becomes impossible. Operating at the network and transport layers, they are visible, measurable and largely manageable with the right security infrastructure.

Application-layer attacks, by contrast, resemble a crowd entering a store and engaging staff with complex, time-consuming interactions without ever making a purchase. The system is not overwhelmed by volume, but by intent. These incidents target how services function rather than how much traffic they can handle. The most effective attacks today are the ones that blend in, becoming more controlled, persistent and difficult to distinguish from legitimate usage. They operate within expected traffic patterns, mimicking real user behaviour and degrading systems without triggering conventional defences.

Why SMBs have become easy targets

As early as October 2023, CERT-In had already signalled a change in attacker strategy, noting the use of multi-layered DDoS techniques, including those operating at the application layer. This marked a departure from traditional volumetric attacks. Instead of overwhelming networks with sheer traffic, attackers began exploiting how applications respond to legitimate-looking requests.

Global data reflects this transition. According to Netscout's Threat Intelligence Report, there has been a noticeable rise in application-layer attacks, surging by 43 percent in H1 2024 over H1 2023. This easily surpassed the 30 percent increase in volumetric attacks. Cloudflare's DDoS Threat Report (Q4 2025) indicates that the scale of attacks has surged dramatically, with over 34 million incidents mitigated in a single year. There has been a sharp growth in HTTP (Layer 7) DDoS attacks, disproportionately impacting smaller organisations.

SMBs are being increasingly targeted because they have become more connected, API-driven, and dependent on real-time interactions, the attack surface has expanded in ways that favour subtlety of threat over scale. At the same time, the tools required by attackers to exploit these systems have become more accessible and easier to deploy. This convergence has created a landscape where attacks are not only more sophisticated, but also more economically viable to execute at scale. This makes SMBs, with their high digital dependence and comparatively lighter defences, particularly vulnerable to modern DDoS attacks.

Three structural shifts are driving this change:

- Attack infrastructure has become economical and highly scalable. Botnets have evolved. Attackers now use distributed, residential IPs and AI-assisted scripts to simulate human behaviour. Tools are commoditised and DDoS-as-a-service is widely available.
- API-first business models mean SMBs are increasingly relying on APIs for payments, logistics and SaaS integrations. These are high-value, high-exposure entry points that are harder to protect than traditional web traffic.
- Large enterprises have layered security stacks and dedicated IT teams. SMBs typically rely on a 'man Friday' and ISP-level or basic firewall protections which may be adequate to handle volumetric attacks, but prove insufficient for behavioural threats.
- SMBs make for easy test targets. Attackers use them to practice before moving on to larger organisations.
- Several cybercriminals are now going via SMBs embedded as third-party vendors to break into larger organisations

This means that threats such as DDoS, ransomware, and service disruption are no longer confined to large enterprises. As attack techniques become more sophisticated and easier to deploy, they are increasingly targeting businesses that are more digitally dependent, but less deeply protected.

Why existing network defences fall short

Most existing network protections were designed around volume thresholds. They could detect spikes, anomalies in traffic flow and containable through perimeter-based filtering to maintain bandwidth availability. That model assumed that malicious activity would look fundamentally different from legitimate usage. Such network security models cannot detect threats cleverly disguised as authentic.

What has changed now is not just attacker capability, but attacker intent. The objective is no longer to overwhelm infrastructure outright. It is to degrade it just enough so that customer trust gets eroded along with a disruption to business outcomes. In this new model, the attacker's ability to disrupt is not by downtime, but by friction that is subtle enough to evade alarms, but persistent enough to impact revenue. This can turn out far more damaging, especially for SMBs.

What needs to change: A practical guide for SMBs

Most SMBs believe that investing in a host of tools will ensure they are better protected against cyber threats. The challenge instead is about shifting how networks 'think' about threats, moving from security as a feature to resilience as a design principle. This means that the system should be able to actively identify and shorten the contain threats so that the system is quickly up and running without

Here's what you should be rethinking while evaluating network security:

- **Monitor behaviour, not just traffic:** It is no longer sufficient to monitor traffic volume alone but also to understand user behaviour. Look at patterns to gauge frequency, intent, session behaviour and deviation from typical user journeys, not just packet volume.
- **Protect the application layer:** Protection must extend beyond the perimeter to the application layer. Ensure dedicated protection for APIs, login systems, and transaction endpoints.
- **Move to always-on mitigation:** Mitigation cannot be episodic as on-demand defence is too slow. Protection must be embedded into the network's operational fabric and capable of responding in real time.

- **Build network intelligence:** Networks need to evolve from passive conduits of data to active systems that can interpret, adapt, and respond. They should be able to distinguish between genuine users and scripted behaviour in real time. Intelligence, derived from usage patterns and contextual awareness, becomes as critical as capacity.
- **Design for resilience, not just speed:** High-speed connectivity is now a baseline. The real differentiator is how well the network sustains performance under stress. The ability to maintain service continuity under ambiguous, low-visibility threats becomes the defining characteristic of a robust connectivity infrastructure.

From an ACT Enterprise standpoint, this evolution in network security is already underway. We understand the evolving challenges of modern threats for our SMB customers and are actively working on enhanced network solutions. Through strategic collaborations with industry partners, our emphasis is moving towards building networks that are not only high-performing, but inherently intelligent and aware. They are capable of distinguishing between genuine and synthetic behaviour, and of adapting dynamically to protect critical services. This is not about adding layers of defence after the fact, but about embedding resilience into core network architecture.