

5 Common Cybersecurity Blind Spots in Mid-to-Large Enterprises



As mid-to-large enterprises scale cloud adoption, digital customer platforms, and AI-led operations, their attack surface continues to expand. Yet many organisations remain focused on visible threats while overlooking structural vulnerabilities that quietly increase cyber risk. Insights from the India Cyber Threat Report 2026 by Seqrite, the enterprise arm of Quick Heal Technologies, suggest that attackers are increasingly exploiting gaps in visibility, identity controls, and partner ecosystems rather than relying solely on traditional intrusion methods. Meanwhile, Barracuda Networks highlights that modern attacks are becoming more evasive, often bypassing legacy defenses through automation and credential misuse. Addressing these blind spots is essential, as enterprise resilience today depends on continuous awareness rather than reactive security.

1. Fragmented Visibility Across Hybrid Infrastructure

Enterprises now operate across multi-cloud environments, SaaS platforms, remote endpoints, and legacy systems. While this hybrid architecture enables flexibility, it often creates monitoring silos. Seqrite's

threat intelligence observations indicate that unmanaged assets and misconfigured environments frequently become entry points for attackers. Without unified visibility, threats can persist undetected and move laterally across networks. Consolidated security platforms that deliver centralized telemetry and real-time correlation are becoming critical for faster detection and response.

2. Identity Risks and Excessive Privileges

As organisations grow, so does identity sprawl — spanning employees, vendors, and machine accounts. Over time, access rights accumulate, leaving many users with more privileges than necessary. Barracuda Networks notes that credential-based attacks remain one of the most dependable methods for adversaries because they allow access without triggering conventional alarms. Enforcing least-privilege access, conducting regular entitlement reviews, and strengthening identity governance can significantly reduce this exposure while supporting zero-trust strategies.

3. Alert Fatigue Within Security Teams

Security tools generate massive volumes of alerts, many lacking actionable context. This often leads to operational fatigue, where critical threats risk being overlooked. Barracuda experts stress that security effectiveness relies not only on detection capability but also on operational clarity — ensuring automation enhances analysts' decision-making instead of overwhelming them. Risk-based alerting, intelligent prioritisation, and clearly defined escalation paths help maintain response readiness without overburdening teams.

4. Underestimated Third-Party Exposure

Modern enterprises depend heavily on vendors for cloud services, analytics, payment processing, and logistics. Each integration expands the threat landscape. Seqrte researchers observe that attackers increasingly target smaller partners as indirect pathways into larger organisations. Treating vendor assessments as a one-time compliance task is no longer sufficient; continuous evaluation, contractual security standards, and shared incident response expectations are now essential components of cyber risk management.

5. Rising Digital Risk and Brand Exploitation

Cyber threats today extend beyond infrastructure to include brand impersonation, fake domains, and social media fraud. Experts at Quick Heal Technologies emphasise that attackers are increasingly weaponising brand identity to power phishing campaigns and financial scams. Proactive digital risk monitoring across open, deep, and dark web environments enables organisations to detect impersonation early and safeguard customer trust.

Looking Ahead

For mid-to-large enterprises, cybersecurity gaps often stem from overlooked fundamentals rather than lack of investment. Strengthening visibility, tightening identity controls, supporting security teams, evaluating partner risks, and monitoring external threats can significantly improve resilience. Organisations that address these blind spots will be better positioned to anticipate disruptions and embed cybersecurity as a strategic business enabler rather than a reactive safeguard.