Bitdefender

CYBERSECURITY ASSESSMENT REPORT

Global Insights from 1,200 Cybersecurity Professionals

June 2025

Bitdefender

Summary

The 2025 threat landscape is defined by speed, stealth, and scale. Cyberattacks are more adaptive and harder to detect, fueled by stolen credentials, fileless techniques, and generative AI tools that empower low-skilled adversaries. At the same time, internal cybersecurity teams are battling growing complexity, a disconnect between the C-suite and the frontline, and pressure to keep reportable breaches quiet.

Our annual Bitdefender Cybersecurity Assessment Report is based on two things: an industry survey of 1,200 IT and security professionals across six countries; and internal analysis conducted by our threat research team. The data reveals that some of today's most dangerous risks are also the quietest. Attackers are weaponizing common and trusted tools to evade detection as they move through networks of organizations around the world.

The 2025 findings reveal that proactive security is no longer optional. Organizations are overwhelmingly looking to reduce their attack surface in addition to relying on detection and response. The survey data also confirms ongoing concerns around AI: worry about usage by attackers, yes, but also the risk created by organizations themselves as they increasingly utilize the immense number of AI tools flooding the market.

In the final analysis of the research results, it's likely the next generation of security leaders will be defined not only by how fast they react but also by how smartly they prepare.

84%

of modern attacks leverage Living Off the Land (LOTL) techniques, bypassing traditional detection systems.

68%

of security leaders agree they need to reduce their attack surface by disabling unnecessary tools or applications.

58%

of respondents say they were told to keep a breach confidential, often in conflict with compliance and ethical standards.

Only **19%**

of mid-level managers report strong confidence in their organization's cyber readiness, despite 45% of C-level executives saying they feel "*very confident.*"

SECTION 1

Proactive Defense — Shrinking the Attack Surface

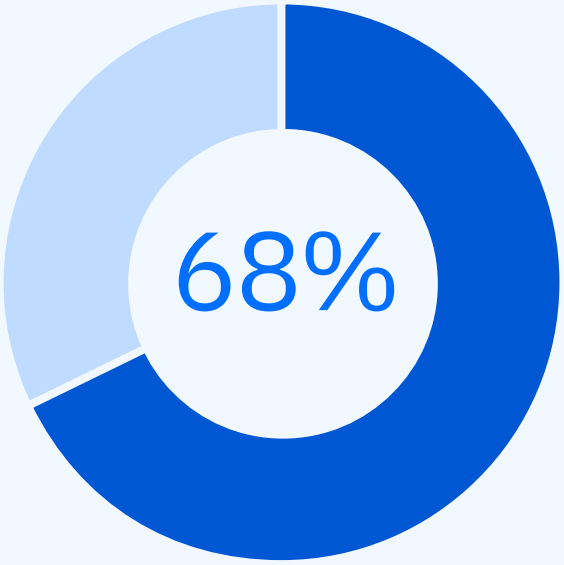
Detection alone is no longer enough, as modern threats are increasingly stealthy. Today, attackers are more likely to "log in, instead of breaking in" using stolen credentials, legitimate tools, and native access to quietly blend into their target's environment. This makes traditional security strategies insufficient. The path forward begins not with more alerts but with shrinking the attack surface itself.

The urgency is clear: 68% of security leaders agree that reducing the cyberattack surface by disabling unnecessary tools and applications is critical. This shift alone would give threat actors fewer ways into an environment and fewer places to hide once they are inside. This pivot toward proactive defense reflects the growing understanding that every unused admin account, dormant application, or excessive permission is an open invitation to a threat actor.

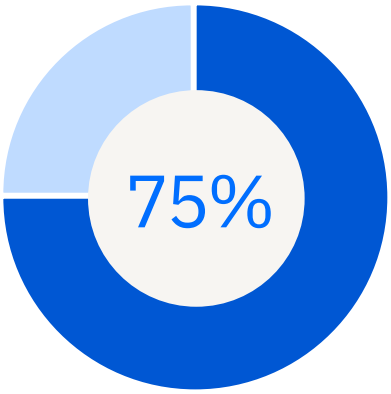
Survey Results

We need to reduce our attack surface by disabling unnecessary tools or applications.

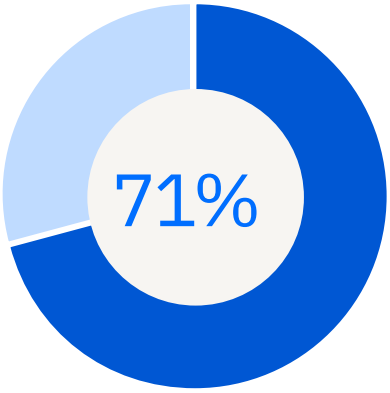
Overall



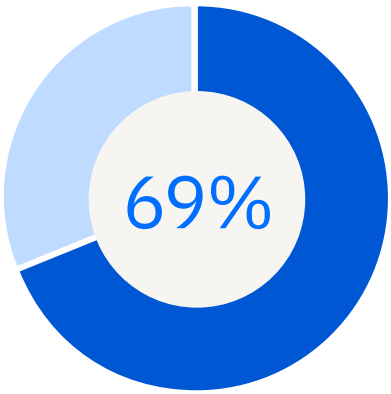
USA



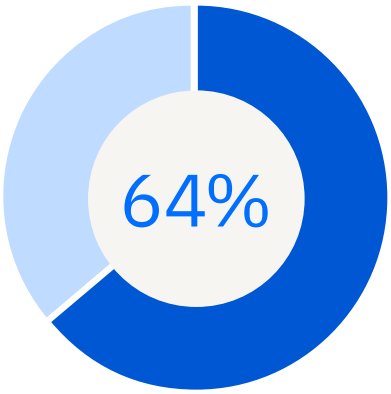
Singapore



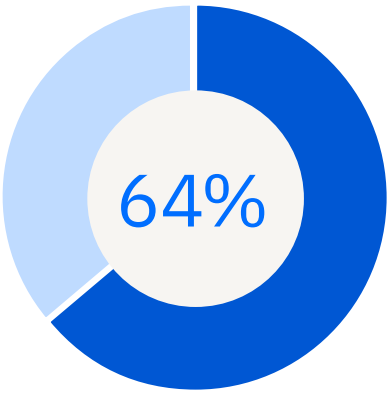
Italy



Germany



UK



France