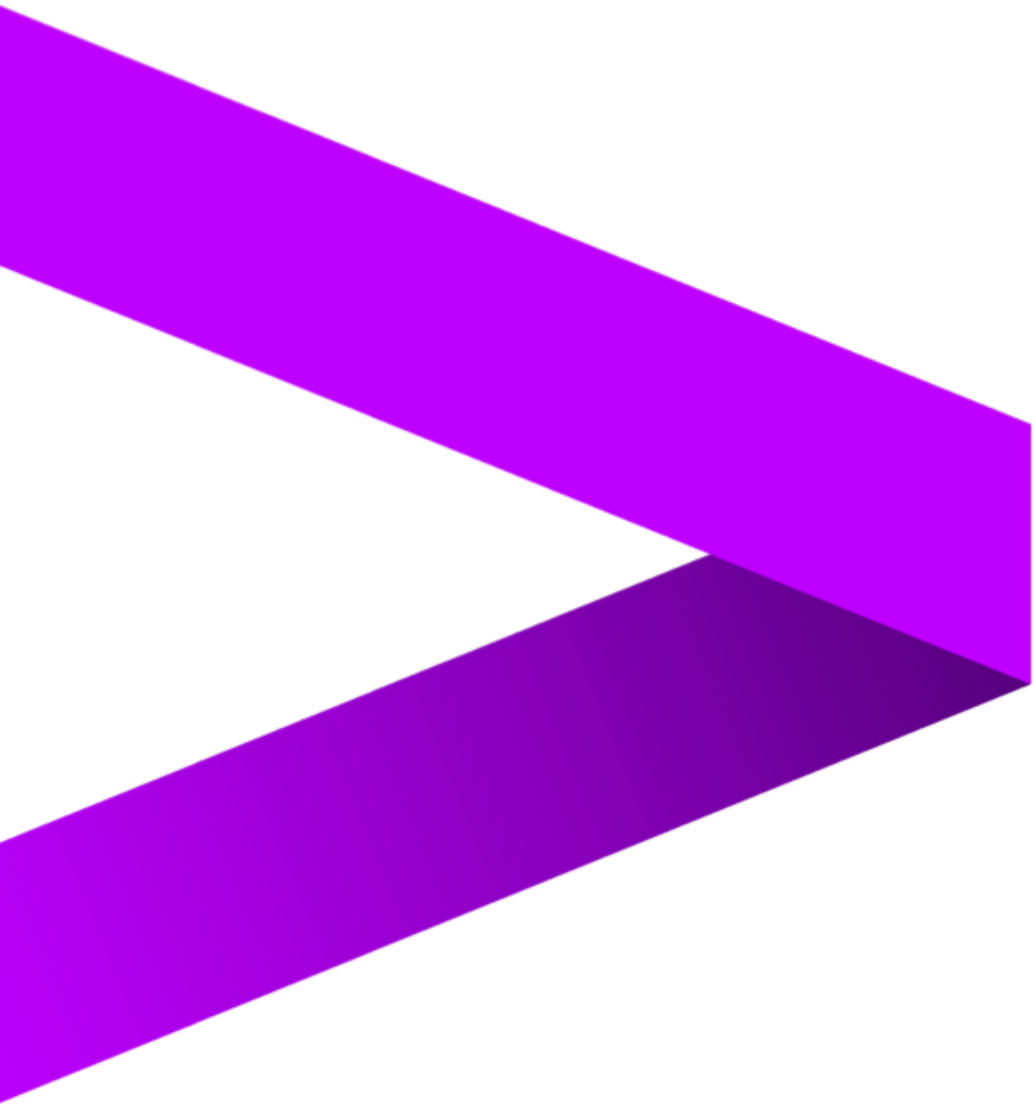
Accenture Security



# GAINING GROUND ON THE CYBER ATTACKER:

## 2018 STATE OF CYBER RESILIENCE

Companies report that attacks on their businesses have more than doubled since 2017, when 1 in 3 caused considerable damage. Now, organizations are gaining ground, with only 1 in 8 getting through.

What's changed? Our research reveals five key findings.

Security teams have made great progress, defending against 87% of attacks. But the basics, including internal threats, still need attention.

The pressure grows daily, yet organizations need two to three more years to embed cyber resilience into the business. Over that time, 90% plan to increase spending.

Breakthrough technologies such as AI and automation will be critical. But only 40% are investing in them to evolve their security programs.

Confidence remains high. But a proactive approach is needed, with 71% saying they still don't know how or when cyberattacks will affect them.

And while the C-suite is treating security as a business risk, authorizing 32% of cybersecurity budgets, the CISO's role needs to adapt to integrate security into the fabric of the organization.

Learn more, including five key steps to cyber resilience, in our 2018 State of Cyber Resilience:

**GAINING GROUND ON THE CYBER ATTACKER**