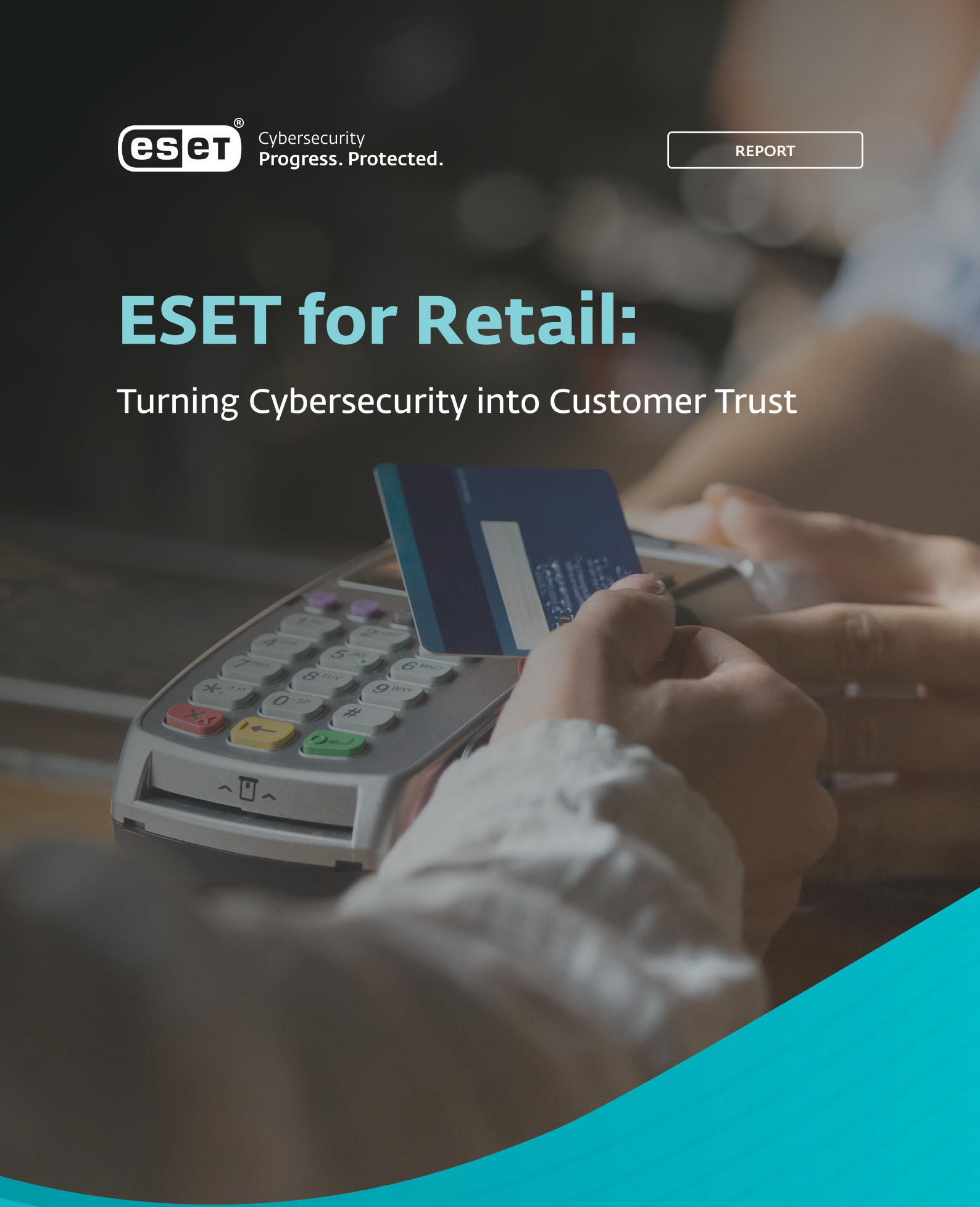
Cybersecurity
Progress. Protected.

REPORT

ESET for Retail:

Turning Cybersecurity into Customer Trust

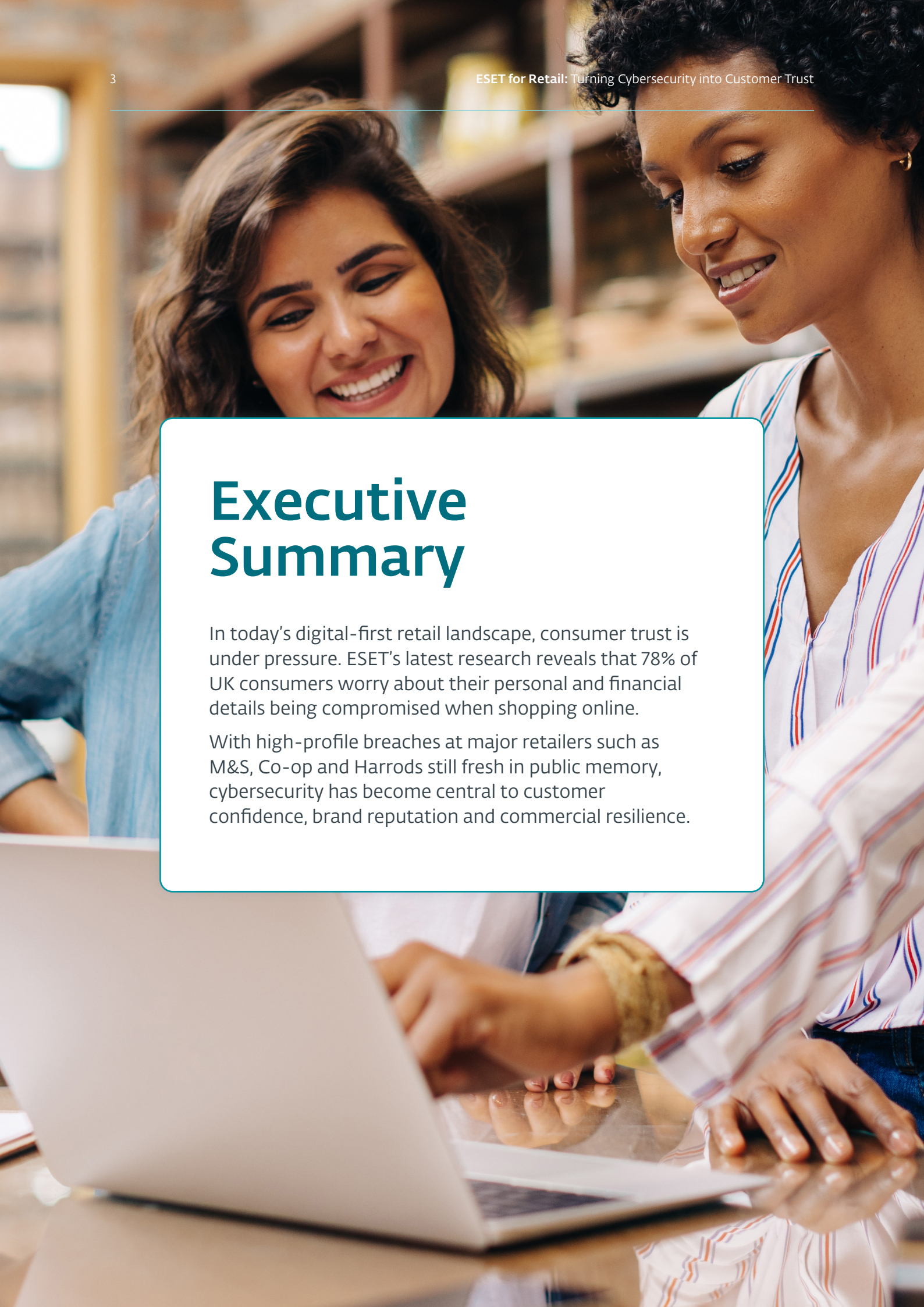


Progress. Protected.

Introduction

78% of UK consumers are concerned about their personal and financial details being compromised when shopping online. Trust in online shopping has never been more fragile and never more important.

With high-profile attacks against the likes of M&S, Co-op and Harrods still fresh in consumer minds, our latest research finds that over three quarters (78%) of consumers are concerned about their personal and financial details being compromised because of online retail transactions. And it's no surprise. Less than two thirds (65%) admit they trust online retailers to protect them, a clear sign that cybersecurity is no longer just an IT issue, but a matter of brand trust and commercial resilience.



Executive Summary

In today's digital-first retail landscape, consumer trust is under pressure. ESET's latest research reveals that 78% of UK consumers worry about their personal and financial details being compromised when shopping online.

With high-profile breaches at major retailers such as M&S, Co-op and Harrods still fresh in public memory, cybersecurity has become central to customer confidence, brand reputation and commercial resilience.

What our research shows

→ RECENT ESET RESEARCH REVEALS HOW CYBERSECURITY FEARS ARE RESHAPING SHOPPING HABITS ACROSS THE UK:

- 60.9% consider data protection and cybersecurity when deciding where to shop.
- Only 65% trust online retailers to protect their data — and younger consumers are especially cautious.
- Nearly 50% of 16–24 year olds say they'd pay more for secure shopping.
- 46% of shoppers say it would take them over five months to trust a brand again after a data breach.
- Fear of fraud (31%) and loss of trust (26%) are the top reasons customers stop shopping with a brand post-breach.

At a time when consumer confidence is already fragile, this knowledge gap has serious repercussions for retailers to consider. Over two thirds of consumers now say strong cybersecurity measures or clear privacy policies would make them more likely to shop with a brand. But once that trust is lost, it's a long road back, with nearly half admitting it would take them more than five months to shop with a brand again after a breach.

When a breach happens, the fallout can be immediate and severe. Just over four in five consumers say they have stopped shopping with a brand after a cyber attack, and only 2% would be willing to return within less than a month of an incident. Fear of fraud (31%) and loss of trust (26%) are the leading reasons cited for abandoning retailers after a breach.

Notably, younger consumers (aged 16-34) are nearly twice as likely as over-55s to be influenced by the fear of fraud to stop shopping with a brand post-breach. For some, the damage is permanent; 13% of consumers say they would never shop with a brand again following a cybersecurity breach.

And the concerns are understandable, over a third (35%) of people are aware of having their personal or financial details being compromised in the last three years alone due to a retailer's attack and of those, 43% lost £100 or more as a result.

The findings show that action is required to win customers back, not just apologies. Almost half of consumers say they will only return to a brand post-breach if the company demonstrates security improvements over time with no further incidents (49%). Meanwhile, 47% expect compensation for personal losses and just over a third (34%) would be satisfied with a public apology.

→ WHY THIS MATTERS FOR RETAILERS

Cybersecurity is no longer just an IT issue, it's a brand trust issue. Retailers who ignore this risk customer loyalty, revenue and reputation. But there's also an opportunity:

- 68% of shoppers are more likely to buy from brands with strong cybersecurity measures or clear privacy policies.
- 49% would pay more for a secure shopping experience.
- 59% say trustworthy retailers start with recognised, secure payment methods.

68%

of shoppers are more likely to buy from brands with strong cybersecurity measures or clear privacy policies.

→ HOW TO REBUILD TRUST AFTER A BREACH

Consumers told us what really matters:

- Demonstrated security improvements over time (49%)
- Compensation for losses (47%)
- Public security updates (40%)
- (A simple apology is no longer enough.)

It's clear that cybersecurity isn't just about risk mitigation, it's a business opportunity. Almost half of consumers say they would pay more for a secure shopping experience and 59% say this starts by offering recognisable payment methods which they believe signals a trustworthy online shopping experience. Currently, there's a communication gap that retailers must overcome. Forty per-cent of people reveal they don't believe retailers are clear enough about their data protection measures. A clear missed opportunity for brands to lead with transparency.

40%

of consumers who said that public security updates are important for rebuilding trust after a data breach.

"Strong security isn't just a business expense, it's a differentiator. Brands that invest in cybersecurity and clearly communicate those efforts can boost conversion, retention and even margin. Today's shopper is increasingly security-savvy, and retailers who ignore that do so at their peril. But for those who embrace transparency and security innovation, there's a clear competitive edge to be gained."

MATT KNELL
UK COUNTRY MANAGER AT ESET

→ THE TAKEAWAY

Strong security isn't just a cost of doing business it's a competitive advantage. Retailers who invest in visible, transparent cybersecurity can boost trust, retention and even margins. Those who don't risk losing an entire generation of customers.

40% of people reveal they don't believe retailers are clear enough about their data protection measures. A clear missed opportunity for brands to lead with transparency.

How ESET Can Protect Retail Businesses

Retailers require robust, intelligent and proactive security solutions to ensure business continuity and customer trust. ESET's suite of security products provides layered protection tailored to the unique challenges of the retail sector from safeguarding point-of-sale (POS) systems to protecting cloud applications and employee endpoints.

→ ESET PROTECT MDR ULTIMATE – 24/7 EXPERT-LED PROTECTION

ESET Protect MDR Ultimate offers a fully managed detection and response service, combining AI-powered threat defence with expert human oversight. This premium solution delivers round-the-clock monitoring (24/7/365), ensuring that any potential security incidents are identified, analysed and mitigated in real time.

For retail businesses that operate continuously across multiple locations, this means uninterrupted protection, rapid response to cyber threats and reduced risk of downtime or data breaches. ESET's security experts provide the insight and intervention needed to defend against even the most sophisticated attacks, offering defence without compromise.

→ ESET PROTECT COMPLETE – COMPREHENSIVE SECURITY WITH NO BLIND SPOTS

ESET Protect Complete delivers all-in-one protection designed to eliminate vulnerabilities across every layer of a retail business's IT infrastructure. It secures endpoints, cloud applications and email systems, preventing malware, phishing and ransomware attacks from disrupting daily operations.

The addition of vulnerability and patch management capabilities ensures that systems are always up to date, reducing the risk of exploitation through unpatched software. This comprehensive coverage helps retail businesses maintain compliance with data protection standards such as GDPR while protecting both employee and customer information.

→ ESET PROTECT ADVANCED – PROACTIVE THREAT PREVENTION

ESET Protect Advanced focuses on the principle that prevention is better than cure. Using advanced threat detection technologies, it stops cyber threats before they can cause harm, ensuring data remains secure and operations remain uninterrupted. The solution includes multi-layered protection against ransomware, targeted attacks and data breaches, giving retailers peace of mind that their sensitive customer and transaction data is locked down.

By combining intelligent automation with human expertise, ESET provides retail businesses with scalable, reliable and cost-effective security solutions. Whether through full managed detection and response, comprehensive endpoint protection, or proactive threat prevention, ESET empowers retailers to focus on their customers and operations, not cyber threats.

24/7/365

monitoring ensures that any potential security incidents are identified, analysed, and mitigated in real time through ESET Protect MDR Ultimate solution.

SUCCESS STORY

Discover how ESET helps retailers protect customer trust...

boohoo

→ WHY BOOHOO CHOOSE TO WORK WITH ESET

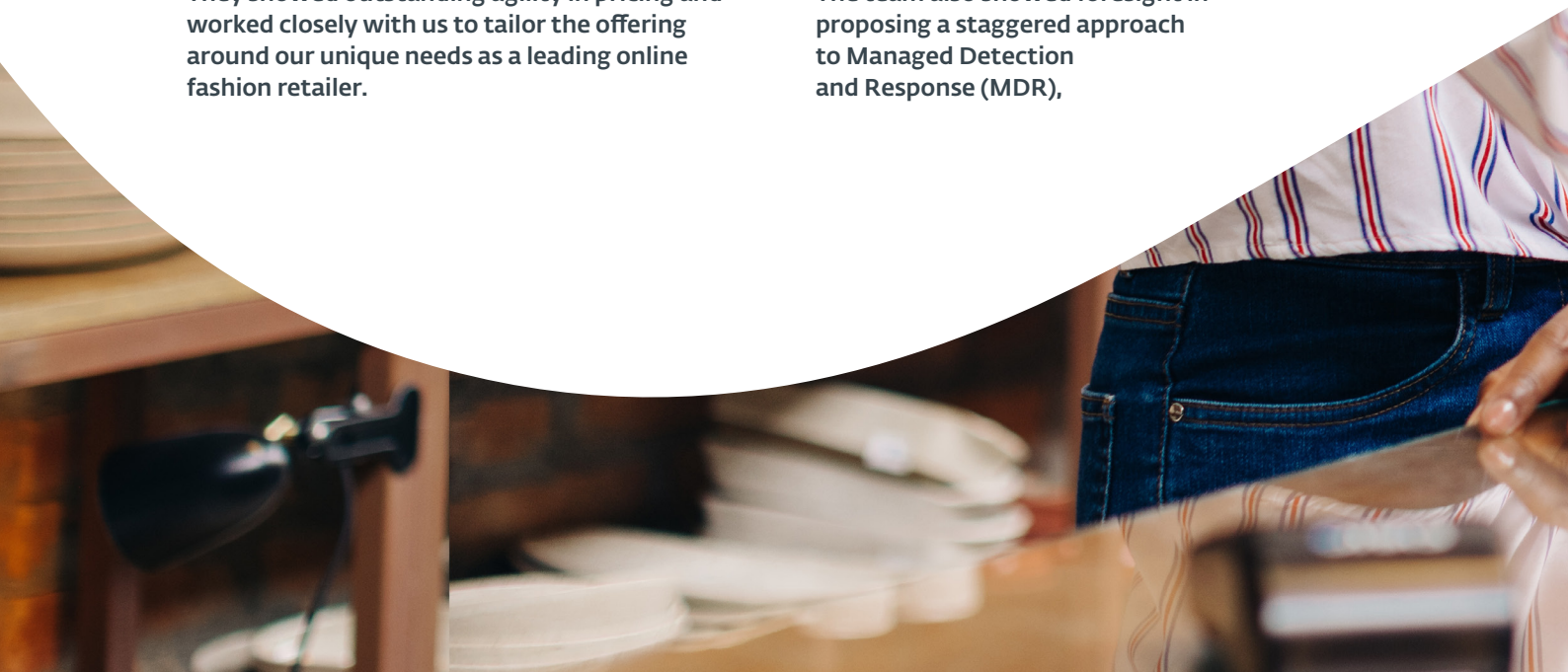
"At Boohoo Group, securing our digital operations across a fast-paced, high-growth retail environment is a top priority. As a business that operates entirely online, our digital footprint is not just core to how we trade — it is the business. This makes us a high-value target for cybercriminals, with constant pressure to defend against threats that could disrupt operations, compromise customer data, or damage brand trust.

Partnering with ESET and deploying their PROTECT Complete offering has been a pivotal step in strengthening our cybersecurity posture.

From the outset, ESET demonstrated exceptional pre-sales support, offering hands-on assistance during proof-of-concept testing to ensure the solution met our complex requirements. They showed outstanding agility in pricing and worked closely with us to tailor the offering around our unique needs as a leading online fashion retailer.

ESET's PROTECT Complete suite not only consolidated multiple security tools into a single, efficient bundle — including Microsoft 365 security, patch management, and next-gen antivirus — but also delivered significant value by reducing both operational overhead and costs.

The team also showed foresight in proposing a staggered approach to Managed Detection and Response (MDR),



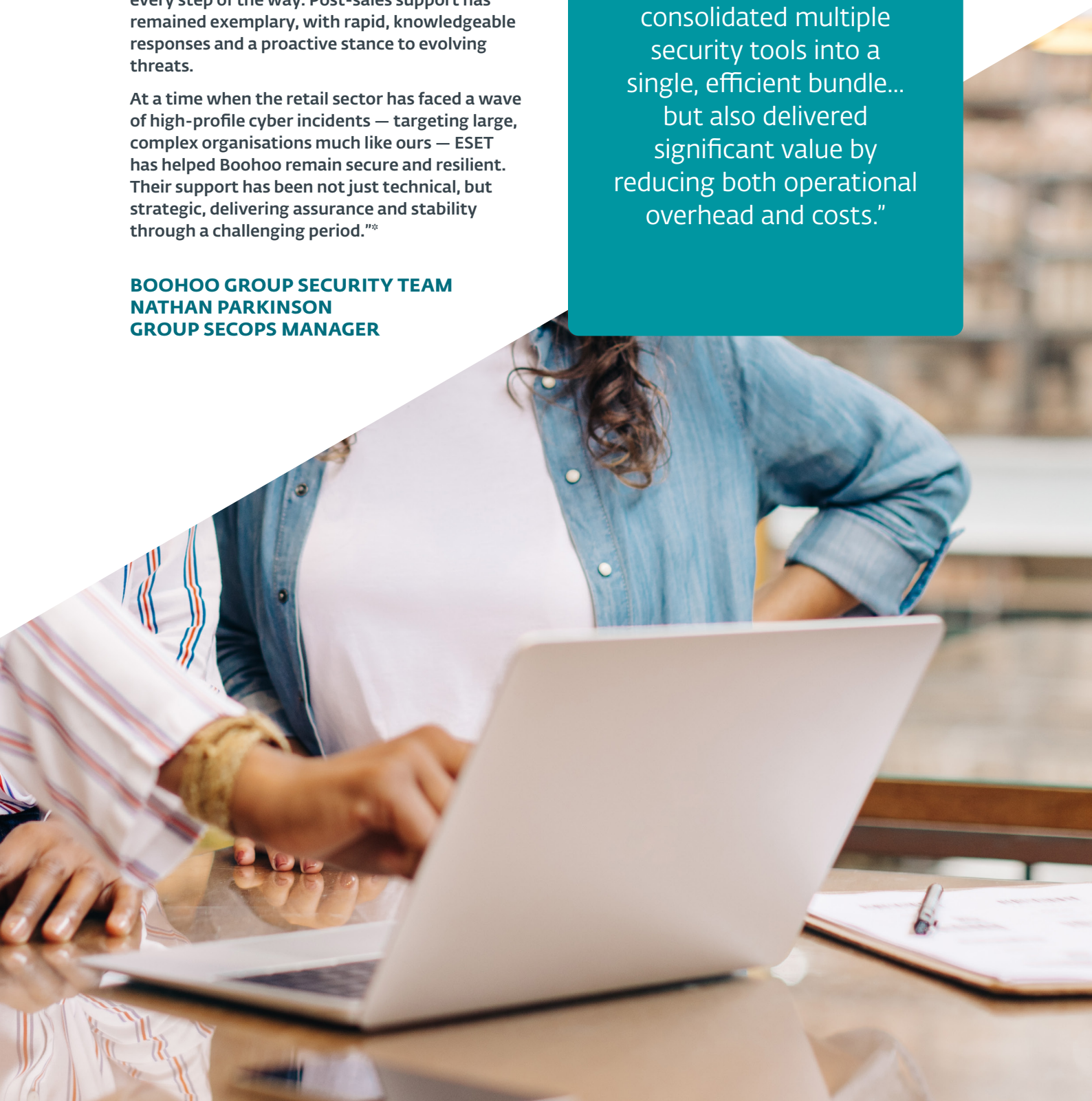
allowing us to prepare for the transition while honouring existing contracts. This level of flexibility was critical as we navigated major internal structural changes across our group.

Deployment was handled seamlessly, even in our complex enterprise environments, with ESET respecting our stringent change control policies every step of the way. Post-sales support has remained exemplary, with rapid, knowledgeable responses and a proactive stance to evolving threats.

At a time when the retail sector has faced a wave of high-profile cyber incidents — targeting large, complex organisations much like ours — ESET has helped Boohoo remain secure and resilient. Their support has been not just technical, but strategic, delivering assurance and stability through a challenging period."*

BOOHOO GROUP SECURITY TEAM
NATHAN PARKINSON
GROUP SECOPS MANAGER

"ESET's PROTECT Complete suite not only consolidated multiple security tools into a single, efficient bundle... but also delivered significant value by reducing both operational overhead and costs."



SUCCESS STORY

Ann Summers

→ WHY ANN SUMMERS CHOOSE ESET

"Ann Summers has trusted ESET as our cybersecurity partner for over a decade — a relationship built on consistent performance, trusted support, and a deep understanding of the challenges we face as a retail business.

For many years, ESET's antivirus technology formed the foundation of our threat protection. As our needs evolved, we moved to ESET PROTECT Enterprise, gaining critical Endpoint Detection and Response (EDR) capabilities to stay ahead of increasingly sophisticated threats. Most recently, we've taken our security posture even further by upgrading to ESET PROTECT Elite, enabling us to leverage powerful tools like patch management and Microsoft 365 security — all within a consolidated, streamlined solution.

As a retailer operating in a highly cost-conscious environment, with a lean IT team supporting a wide and demanding business, we needed a solution that could scale with us without adding operational burden. ESET's Managed Detection and Response (MDR) service has been a key enabler, delivering advanced monitoring and incident response while freeing our team to focus on core priorities.

Through a period marked by rising cyberattacks across the retail sector, ESET has continued to keep our systems secure and our operations resilient. Despite numerous approaches from larger, high-profile vendors, we've remained with ESET — not just because of the strength of their technology, but because of their deep customer focus, transparent communication, and proven results.

ESET provides more than just protection — they offer partnership, expertise, and peace of mind. We value them as a critical extension of our IT and security function."

ANN SUMMERS IT & SECURITY TEAM

Methodology

The research was conducted by Opinion Matters, among a sample of 2000 UK Respondents (Nat Rep 16+). The data was collected between 23.07.2025 - 25.07.2025. Opinion Matters abides by and employs members of the Market Research Society and follows the MRS code of conduct and ESOMAR principles. Opinion Matters is also a member of the British Polling Council.