N-ABLE™

2025

ANNUAL THREAT REPORT

SMBs IN THE CROSSHAIRS

Table of Contents

Key Takeaways

1

Cybercriminals are targeting SMBs more than ever

Attackers are no longer skipping over smaller businesses. In fact, they're increasingly targeting them. The N-able team observed a surge in detected threat instances—from approximately 48,749 in June 2024 to over 13.3 million by June 2025—a 273x increase.

2

Hackers see big payouts from small targets

Weaker defenses make SMBs easier and more profitable to breach. Cybercriminals target SMBs because the resistance is low while the payoff can be relatively high.

3

Ransomware still reigns supreme

Ransomware remains the most common and damaging risk: 88% of confirmed SMB breaches* involved ransomware or data extortion. The top three threats observed by the N-able Threat Team are Play, Qilin, and Tycoon 2FA.

4

Regulations are catching up to the risk

New rules increase pressure on SMBs to improve security. Fines and penalties often exceed the cost of the breach itself.

5

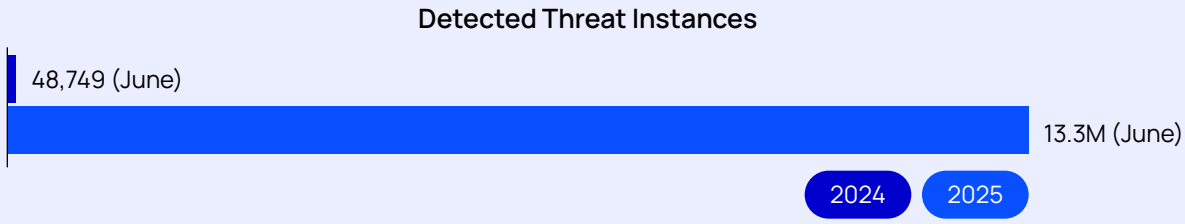
AI supercharges social engineering

Generative AI is helping attackers craft convincing phishing messages that mimic real people and writing styles, fooling even tech-savvy employees.

Executive Summary

The 2025 Annual Threat Report delivers an urgent reality check: SMBs ranging from 100-2500 employees are now primary targets for sophisticated, industrialized cybercrime operations.

This alarming shift is dramatically underscored by data from N-able, which reveals a staggering surge in detected threat instances—**from approximately 48,749 in June 2024 to over 13.3 million by June 2025 —a 273x increase.**



This report breaks down the most dangerous threats: from the pervasive impact of ransomware, accounting for **nearly 1.9 million detections in the first half of 2025**, to the relentless spread of general malware, with **over 3.3 million detections** in the same period. Additionally, it explores why identity is now the front line in cyberdefense and how the rise of AI is driving more sophisticated social engineering and credential theft. It also addresses growing regulatory pressure and the risks of relying on compliance alone.

To help SMBs respond, N-able provides clear, practical strategies focused on high-impact, low-cost defenses, enabling organizations to navigate today's threats with confidence.

Overview:
The evolving SMB threat landscape

The last year made it starkly clear that SMBs cannot fall back on long-held assumptions about their security, namely that attackers bypass small targets and that basic protections are sufficient. In 2024, we saw SMBs move squarely into the crosshairs of global threat actors and witnessed the devastating impacts of attacks on small organizations.

Industry data shows that almost no company is too small or too "offline" to escape the threat. Verizon's 2025 Data Breach Investigation Report, which spanned 139 countries, recorded 3,049 security incidents at SMBs and found ransomware in 88% of the resulting breaches.[1]

Key factors shaping the SMB threat outlook

The N-able Threat Research team has identified the following factors shaping today's SMB landscape:

1. Digital acceleration expands the SMB attack surface

SMBs have rapidly adopted the same digital technologies as larger enterprises, from cloud computing and SaaS applications to IoT devices and remote workforce tools.

This digital acceleration yields efficiency and growth, but also expands the attack surface: an SMB's network and data are often just as accessible to attackers (via the internet, cloud, etc.) as any Fortune 500 company's data, erasing the notion that an SMB might hide in an analog or obscure "safe zone."

N-able Threat Research:

Our internal telemetry reveals an escalation in threat activity: total detected threat instances surged from approximately 48,749 in June 2024 to over 13.3 million by June 2025 —a 273x increase.

2. Threat actor evolution: Crime at industrial scale

Cybercriminals are sophisticated, and they're increasingly operating at industrial scale.

The rise of Ransomware-as-a-Service (RaaS) gangs and plug-and-play attack kits means even relatively low-skilled attackers can launch sophisticated attacks en masse. Meanwhile, organized cybercrime groups run like businesses themselves, complete with customer service and affiliate programs.

N-able Threat Research:

In the first half of 2025 (January to June), our systems detected over 6 million unique threat instances across various classifications, highlighting the sheer volume of attacks SMBs face daily.

The cost and effort to attack an SMB is as low as for any other target, and with these lucrative RaaS affiliate programs, thousands of potential but otherwise unskilled attackers are incentivized to target whomever they can. They cast wide nets and do not discriminate based on company size. If an organization has valuable data or will pay a ransom, it is a target. Automated scanning tools continually probe for any vulnerable system connected to the internet, ensuring that exposed SMB networks could be discovered within hours by opportunistic attackers.

3. The alluring economics of SMB attacks

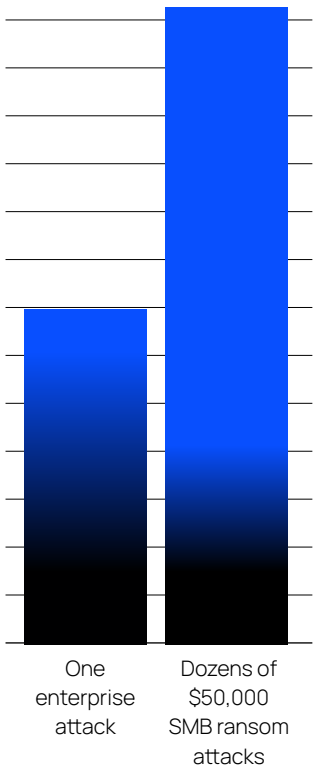
Attackers have realized that SMBs can yield high returns with comparatively lower effort.

A single large enterprise might net a multimillion-dollar ransom, but that attack could take months of planning and advanced techniques to defeat strong security. By contrast, dozens of smaller $50,000 ransoms from SMBs can be obtained faster with commodity malware, exploiting the fact that many SMBs have weaker defenses or cannot afford prolonged downtime.

Stolen data from SMBs (customer records, proprietary designs, financial info) can be sold on dark markets or used for identity theft and fraud. In fact, the criminal return on investment (ROI) for attacking smaller targets has never been higher. Compounding this, many SMBs are more likely to lack incident response plans or backups, making them more likely to pay ransoms.

The result is an economic sweet spot that cybercriminals are exploiting.

Representation of Net Ransom Yields



A Deeper Look:

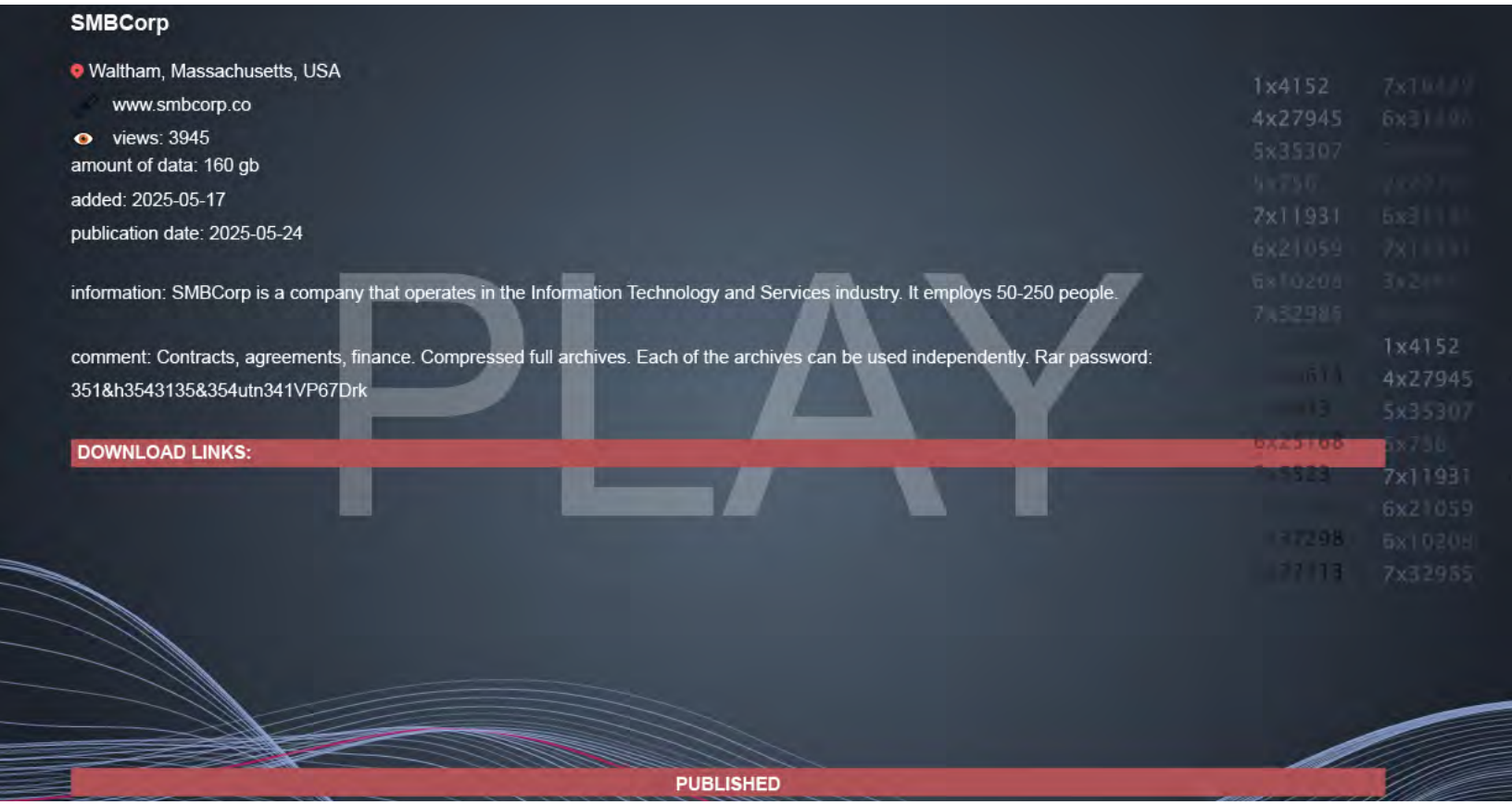
3 Top Threats to SMBs in 2025

The N-able Threat Research team combined recent data and frontline observations to identify three top threats proving especially disruptive for SMBs.

Our analysis of threat classifications from January to June 2025 reveals that while ransomware and general malware constitute the vast majority of detected incidents, other prevalent threats, like potentially unwanted applications (PUAs), cryptominers, infostealers, and Trojans, also pose significant and consistent risks to SMBs.

Nevertheless, a few risks rise to the top in both frequency and impact. These top three threats challenge traditional defenses, and prompt many organizations to rethink how they protect their networks, data, and users.

2025 THREATS



THREAT #1 PLAY

Play was one of the most active ransomware groups of the past year. They target businesses of all sizes across the world, but a majority of their victims have been in North America, in the professional services and manufacturing industries.

Play's most common TTP involves targeting exposed devices—often through known exploits affecting platforms like FortiOS, Citrix Netscaler, and Microsoft Exchange servers. They also use stolen credentials against publicly exposed VPN and RDP servers.[2]

Play has been active since 2022 without any major dips in activity. Their lateral movement and persistence techniques are among the most mainstream, primarily using commercial off-the-shelf tools and built-in Windows applications (known as LOTL, or Living Off the Land). This keeps their profile low inside a network, as traditional antivirus is less likely to detect these techniques. Endpoint detection and response (EDR) software can be more effective at identifying this malicious activity but requires active monitoring to catch the attacker before they spread throughout the network.

THREAT #2 QILIN

Qilin is another major ransomware group that has been prolific since 2022. They also target businesses of all sizes and sectors, and most of their victims have been located in North America. Due to the recent shutdowns and fracturing of other major RaaS groups, the number of Qilin victims has surged in the past six months.

Qilin works with affiliates or Initial Access Brokers, who hand off their victims after gaining initial access to their networks. This means there is a high degree of diversity in their initial access techniques, but they share a common thread with other ransomware groups in that the primary techniques observed have been phishing campaigns, exploiting vulnerable network devices, and using stolen credentials to log in to exposed VPN and RDP servers.[3]

Qilin's affiliates are known to use remote monitoring and management (RMM) tools to gain and maintain access to victim networks. One notable recent attack targeted managed service providers (MSPs) using ScreenConnect. The Qilin affiliates sent phishing emails impersonating ScreenConnect and leading to a fake login page, which would collect the target's ScreenConnect credentials and could even bypass multi-factor authentication (MFA) using an adversary-in-the-middle technique similar to the one discussed in the next threat profile.[4]

THREAT #3 Tycoon 2FA

Business email compromise (BEC) is not often considered in the same league as devastating ransomware attacks, but it can often be just as disastrous. Tycoon 2FA is a Phishing-as-a-Service (PhaaS) provider that allows threat actors to easily and affordably conduct BEC attacks. The service provides everything an attacker needs to impersonate a Microsoft 365 or Google Workspace login page, among other target services, and steal credentials from unwitting victims.

Financially motivated threat actors will come up with a phishing lure to convince their target to click on a link in an email or scan a QR code. Some common ones seen recently have included fake DocuSign signature requests or OneDrive document sharing notifications. When the victim clicks on the link, they are redirected to a perfectly copied Microsoft 365 login page, which is actually hosted on a domain owned by Tycoon.

If the victim enters their Microsoft 365 credentials, they'll next reach a realistic MFA step. But in reality, the Tycoon server is sitting between the victim and the Microsoft server, passing along the MFA prompt and response. Once the victim logs in to the impersonating site, the Tycoon server in the middle intercepts the victim's session and automatically begins collecting data from the victim's account, including emails and contacts.

The session is then available for the threat actor to access later to go deeper into the victim's data. In many cases, the threat actor targets accounting and finance departments. They begin searching for invoices, bills, and other financial documents where there may be an opportunity to insert themselves for financial gain. They also set up inbox rules to automatically hide emails and replies related to the attack to keep the victim unwitting for as long as possible.

Attackers can spend weeks just observing the victim's emails and waiting for the right opportunity. When they find it, they use the victim's account to send emails to others who have established trust with the victim to carry out their attack. Some examples of attacks we have seen include: sending emails from the victim's account to a customer asking to change the routing number for an upcoming payment; emailing another person within the company to change the routing number to pay an outstanding invoice; or even emailing someone else in the company with a new phishing lure to move laterally to a better victim account.

Reality Check:

SMB Threat Buzz vs. Bite

Modern fearmongering, clickbaiting headlines make everything out to be a cataclysmic catastrophe, making it hard for SMBs to focus on the concrete risks that present imminent threats and drain budgets every day.

The N-able Threat Research group put together a list that separates the "buzz" from the real "bite," keeping the focus on pragmatic security ROI for SMBs.

Buzz: **Big headlines**, but limited near-term impact

Quantum-cryptography panic

NIST has already finalized post-quantum cryptography (PQC) standards such as ML-KEM (formerly CRYSTALS-Kyber) and ML-DSA (formerly Dilithium). Migration guidance emphasizes a decade-long, vendor-led transition path; mainstream TLS, VPN, and messaging stacks will embed PQC automatically well before most SMBs need bespoke upgrades.[6][7]

Zero-day frenzy

In 2022, malicious actors still preferred older, unpatched vulnerabilities over brand-new zero-days, according to a joint CISA/NSA/FBI advisory. Unpatched, internet-facing systems were the common path to compromise.[8] ENISA confirms that ransomware operators routinely recycle known exploits rather than spend resources on custom zero-day research.[9] For SMBs, disciplined patch management outranks daily zero-day chatter.

Bite: Threats that routinely **burn SMBs**

Business email compromise (BEC)

The FBI received 21,489 BEC complaints in 2023, with adjusted losses exceeding USD 2.9 billion.[10] Verizon's 2025 Data Breach Investigations Report (DBIR) shows BEC now rivals ransomware as the top incident pattern for organizations under 1,000 employees.[11]

N-able Threat Research:

Data from N-able systems highlights the consistent and growing "bite" of phishing and BEC attacks.

- Our email filters analyzed an average of **4.7 billion messages monthly**, blocking **885 million** of them.
- The percentage of total phishing messages increased by **more than 50%** in the last six months (from 1.49% in January to 2.34% in June), translating to a jump from over 15 million to more than 27 million blocked phishing attempts.
- **30% of phishing messages were blocked** due to failed SPF, indicating widespread email spoofing attempts.

Ransomware-as-a-Service (RaaS)

Affiliate programs such as LockBit, BlackCat/ALPHV, and Play lower the barrier to entry. Recent CISA #StopRansomware advisories detail Play attacks through exposed RDP and unpatched VPNs, and LockBit's exploitation of Citrix Bleed (CVE-2023-4966) against healthcare and professional services firms.[12] ENISA tracks ransomware as the top EU threat for 2023, noting increased multiple-extortion tactics and shrinking dwell times.[13] Regular offline backups, hardened remote access, patch management, and EDR coverage remain the best defense.

Credential stuffing and MFA fatigue

Cloud adoption puts reused passwords in adversaries' crosshairs. CISA warns that push-notification "MFA bombing" and SMS interception can bypass weak factors; it urges a migration to phishing-resistant FIDO/WebAuthn or passkeys.[14] The Verizon 2025 DBIR attributes over 60% of web-app breaches to stolen credentials or brute-force attacks, underscoring passwordless initiatives as a higher-ROI investment than post-quantum pilots.[15]

Outlook for 2025:

Going back to basics to address the threats that bite

SMBs don't need bleeding-edge crypto to stay safe today. Instead, doubling down on email controls, vulnerability management, backups, and phishing-resistant authentication will blunt the attacks that actually bite.

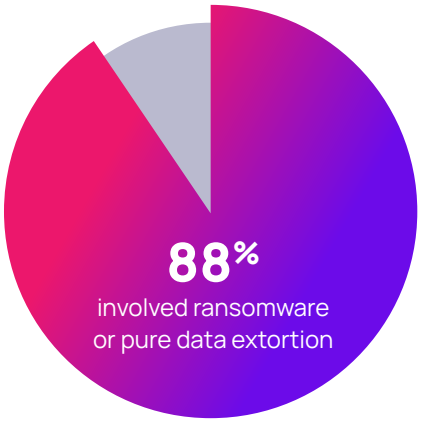
The Ransomware Economy:

Key Trends for 2025

Ransomware remains the heartbeat of the cybercrime economy, and the data shows just how disproportionate the impact on SMBs has become.

According to the Verizon 2025 DBIR, 88% of confirmed SMB breaches in the 2024 reporting window involved ransomware or pure data extortion, up 37% year over year, while median negotiated payments slid to US $115,000 and 64% of victims refused to pay.[16]

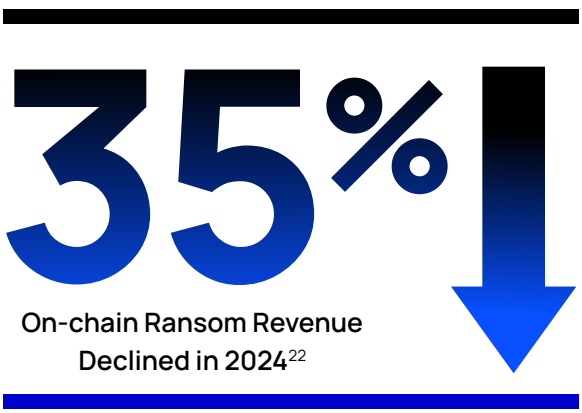
Those headline figures align with broader global data. The FBI's Internet Crime Complaint Center recorded a 9% rise in ransomware complaints in 2024 and again labeled it the most pervasive threat to U.S. critical infrastructure.[17] [18] Australia's cybersecurity agency responded to more than 1,100 incidents in FY2023–24; 11% involved ransomware, and 71% of all extortion cases hinged on ransomware code.[19] In the UK, fully half of businesses reported a cyberattack last year, underscoring how few organizations now remain untested.[20]



Confirmed SMB Breaches in 2024[16]

Economics: Fewer payers, leaner payouts

Attackers are still earning hundreds of millions, but the cash stream is thinning. Chainalysis calculates that total on-chain ransom revenue fell 35% in 2024 to roughly $814 million and that less than half of recorded incidents now end in a payment; typical final payouts cluster between $150,000 and $250,000. Verizon's dataset echoes the trend: two-thirds of victims declined to pay at all, leaving criminals seeking profit elsewhere.[22]



On-chain Ransom Revenue Declined in 2024[22]

N-able Threat Research:

In the first half of 2025 (January to June), ransomware accounted for nearly 1.9 million detections by our systems—compared to 3.3 million general malware detections—underscoring their continued dominance as primary threats.

Tactics: Extortion over encryption

The European Union's threat landscape analysis notes that many affiliates "shifted from double extortion to extorting without encryption," stealing data first and skipping the noisy locker malware altogether.[23] Europol calls out SMBs explicitly as favored prey for these leaner attacks because their defenses are thinner, yet the data they hold, customer records, payment details, operational IP, carries high leverage in public-leak shakedowns. Chainalysis counted 56 new leak sites in 2024, the largest annual jump on record, illustrating how naming-and-shaming has replaced decryption keys as the primary cudgel.[25]

> Chainalysis counted 56 new leak sites in 2024, the largest annual jump on record.

The RaaS machine and the limits of takedowns

RaaS keeps the market liquid. Verizon observed more brands, more affiliates, and faster turnover than in any previous edition of the Verizon 2025 DBIR.[26] Law enforcement landed a few notable blows against attackers: Operation Cronos seized LockBit's infrastructure, froze 200 crypto wallets, and obtained a cache of decryption keys in February 2024[27]; and the FBI infiltration of Hive (revealed at the start of 2023) ultimately prevented an estimated $130 million in ransom outflows.[29]

Yet, the Operation Cronos report shows newer brands rushing in to capture orphaned affiliates. Criminals have learned to fragment and rebrand rapidly after each takedown.

Why SMBs stay in the crosshairs

Several dynamics keep smaller organizations locked in the spotlight.

- Attackers follow the easier path: the 44% ransomware-in-breach rate across all organizations drops to just 39% for large enterprises but explodes to 88% for SMBs.[29]
- Global data shows many SMBs still rely on flat networks, exposed remote access portals, and sporadic patching, all of which make it easier for attackers to gain initial access.[30]
- Ransom demands are calibrated to what an SMB can realistically pay, often under the cyber insurance deductible, making quick settlement tempting even as overall payment rates fall.[31]
- Finally, a quiet breach of a 200-person supplier is far less likely to trigger coordinated, cross-border investigation than an outage at a Fortune 500 manufacturer.[32] [33]

Outlook for 2025:
Undercutting the ransomware business model

The data tells a two-sided story: defenders are finally denting criminal revenue, yet incident volumes, leak site postings, and SMB targeting are all climbing.

For leadership teams in smaller enterprises, the implication is clear: good backups alone are no longer an insurance policy. Encryption of sensitive data at rest, rapid outbound traffic monitoring, and rehearsed breach disclosure processes now sit beside patch hygiene and employee phishing awareness as baseline controls.

Equally, the growing number of victims refusing to pay shows that preparation works. By limiting downtime and reducing data leverage, SMBs can undercut the business model that still fuels this criminal economy.

Identity Is the New SMB Perimeter

Digital identities, not IP addresses, now mark the front line of the attack surface for SMBs.

Over the past 18 months, credential abuse featured in nine out of every 10 confirmed web application breaches, with compromised credentials remaining the single fastest path into an organization's data and cloud workloads.[34]

Attackers have industrialized password theft, phishing, and session hijacking at global scale, generating hundreds of millions of identity attacks every day.[35] Yet most SMBs still protect their crown jewels with methods like reused passwords, leaving a widening gap between threat velocity and defensive maturity.

> Compromised credentials remain the single fastest path into an organization's data.

N-able Threat Research:

The N-able team clearly recognized signs of this industrialization through prevalent schemes such as fake antivirus subscription renewals prompting calls to scam centers, or sophisticated phishing campaigns impersonating financial institutions like Capital One or streaming services like Spotify, all designed to harvest credentials or financial information.

The 2024-25 identity attack landscape: Key findings

Stolen credentials dominated 88% of basic web application breaches in the Verizon 2025 DBIR, while misuse of valid accounts underpinned 44% of all incidents studied.[36] ENISA's 2024 Threat Landscape report similarly ranks "credential theft and abuse" as a top-three European cyberrisk for organizations under 250 staff.[37]

Email remains the preferred credential harvesting tool: employees in firms with ≤250 workers receive one malicious email for every 323 messages.[38]

Once a mailbox is breached, BEC quickly follows; the FBI logged US $2.77 billion in global BEC losses during 2024, with many complaints originating from smaller enterprises lacking dual control on payments.[39]

Cloud identity attacks are relentless. Microsoft stops ~600 million fraudulent sign-in attempts daily across Azure AD and M365 tenants, 99% of which rely on passwords alone.[40] These numbers translate directly into SMB impact because SaaS adoption and thin admin staffing mean compromises scale fast.

Why SMB identity and access defenses still lag

The Cyber Readiness Institute's 2024 global survey found that 54% of SMBs have no MFA on core accounts, and only 13% enforce MFA everywhere.[41]

Excess privilege compounds the problem: 47% of SMBs report users holding access beyond their role, and 1 in 4 have experienced unauthorized use of such accounts.[42] Limited time, perceived complexity, and cost remain the chief barriers cited by owners.

Meanwhile, Microsoft telemetry shows that 99.9% of automated account-takeover attempts succeed only against identities without MFA[43]—a stark reminder of the opportunity cost.

Fortifying the new perimeter in 2025

To effectively address the gaps discussed above and secure the dynamic identity-based perimeter, SMBs should prioritize the following key strategies:

1. Make MFA the default

Government guidance, from Australia's ACSC small-business playbook to UK NCSC recommendations, places MFA in the top three of the "Essential Eight" mitigations for all firms, regardless of size.[44] Low- or zero-cost MFA options now ship with every mainstream SaaS platform.

2. Embrace single sign-on and least privilege

Centralizing identity in Azure AD, Okta, or Google Identity lets SMBs apply uniform policies, automate off-boarding, and audit usage. Quarterly reviews of group membership and service-account scopes close privilege creep.

3. Plan the move beyond passwords

Passkeys and device-bound FIDO2 authenticators are gaining traction: 34% of medium-sized organizations have already run pilots or have them in production as of Q1 2025.[45]

4. Leverage built-in anomaly detection

Risk-adaptive conditional-access rules (impossible-travel, unfamiliar IP, unmanaged device) are now bundled in entry-level cloud licenses, bringing zero-trust principles within reach.

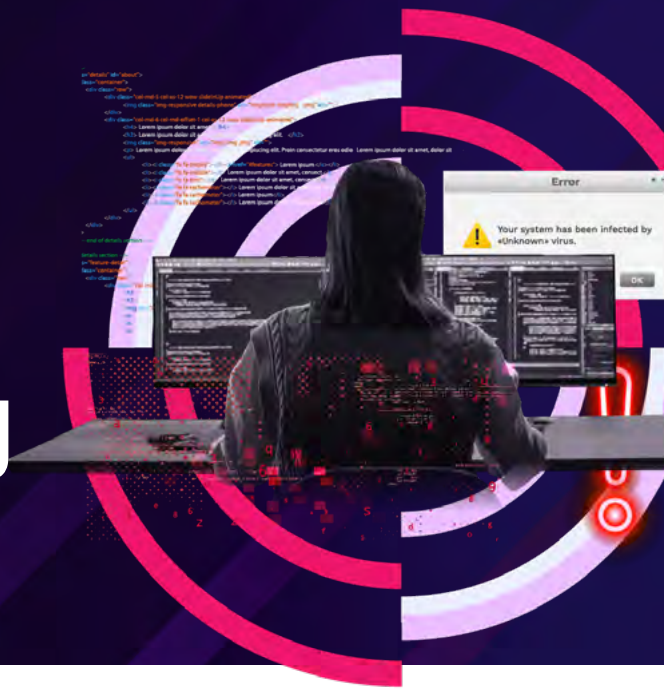
Outlook for 2025:

Identity-centric security is low-cost and high-impact

Identity-centric security delivers outsized risk reduction for minimal spend. Enabling MFA everywhere, curbing privilege, and instrumenting basic identity analytics can eliminate the majority of 2024-25 breach pathways while positioning SMBs for passwordless, zero-trust futures.

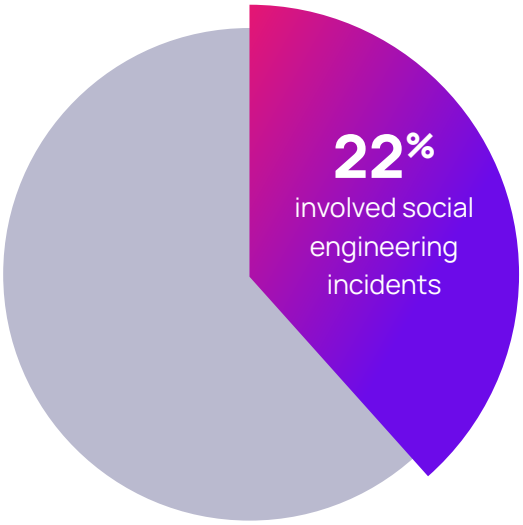
The Human Factor:

AI Threats and the Evolution of Social Engineering

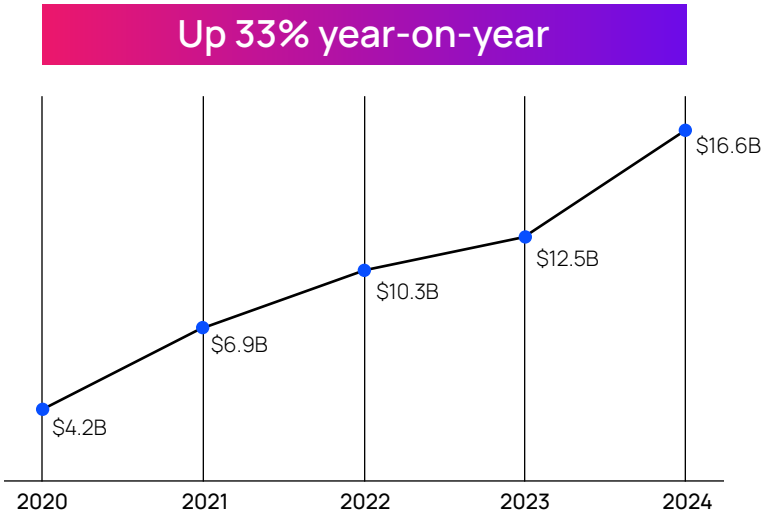


Attackers spent 2024 and the first half of 2025 perfecting trust hacking: using generative-AI to mimic people, writing styles, and even entire identities at near-zero cost.

In the Verizon 2025 DBIR SMB snapshot, social engineering incidents (phishing, pretexting, and MFA prompt-bombing) represented 22% of all confirmed breaches in SMBs, and BEC alone moved US $6.3 billion in 2024. The FBI's latest IC3 Internet Crime Report paints the same picture at the fraud-loss level: overall cybercrime losses hit US $16.6 billion in 2024, with BEC still the costliest tactic at US $2.77 billion—more than investment and crypto fraud combined.[47]



Confirmed SMB Breaches in 2024[47]



Overall Cybercrime Losses Over the Last Five Years - FBI IC3 2024 report[47]

As attackers leverage these advanced capabilities, several key AI-powered threats have emerged as significant concerns for SMBs:

Deepfakes: From novelty to essential fraud toolset

No longer confined to theoretical discussions, deepfakes are now manifesting in various forms as practical tools for malicious actors, including:

Voice clones

FinCEN's November 2024 alert notes "a sharp rise" in Suspicious-Activity-Reports describing deep-fake audio or video used to bypass "Know-Your-Customer" and real-time identity checks at banks and fintechs. Similar synthetic voices are now turning routine BEC requests into high-pressure phone calls that "sound" like the owner of a small company.

Synthetic video and avatars

While live deepfake video calls remain scarce, pre-recorded clips of executives requesting "urgent donations" or "last-minute supplier payments" are surfacing in extortion and stock-manipulation scams. ENISA's Threat-Landscape 2024 highlights AI-enabled disinformation and deepfakes as an emerging mainstream threat class, alongside ransomware and supply chain attacks.[49]

Fake people at scale

AI image generators regularly create profile photos that pass a reverse-image search. Criminal groups build entire LinkedIn personas, harvest OSINT with large language models (LLMs), and launch spear-phishing that references genuine projects, invoices or conference talks scraped from public sources.

N-able Threat Research:

N-able observed how the rise of AI has significantly amplified social engineering tactics. We saw a marked increase in sophisticated techniques like DKIM-reply attacks in 2025—where malicious actors leverage legitimate sender signatures to deliver evasive spam emails with hidden malicious content.

Meanwhile, phishing continues its relentless rise, with AI making it increasingly easy for bad actors to generate highly convincing templates and targeted campaigns, as evidenced by the detailed examples of fake email delivery failures, Capital One account restrictions, and Spotify payment notices.

AI on the Blue Team

Modern email security, EDR, and CASB platforms may now layer LLMs on top of traditional heuristics to detect style anomalies, catch adversary-in-the-middle MFA attacks, and flag AI-generated text. Some managed security providers automatically force password resets or step-up authentication when deepfake indicators (for example audio artifacts) are detected during help-desk calls.

Risk Indicator	Recommended Control	Operational Response
Deep-fake voices remove the "sounds wrong" cue	Verify out-of-band for all money or data moves	Require a second channel (Teams, SMS or in-person) before releasing funds
Prompt-bombing showed up in 14% of social-engineering breaches in 2024[50]	Harden identity (FIDO2 / phishing-resistant MFA)[51]	Move away from push-based OTP; enable number-matching or hardware tokens
Users must recognize that audio and video can lie	Add AI-aware awareness training	Show staff curated fake/real comparisons; drill "pause-and-verify" reflexes quarterly
Major SaaS and UC vendors will flag unverified media	Use content authenticity features as they roll out	Turn on provenance or digital-seal options early in Microsoft 365, Google Workspace, Zoom, etc.
Guidance is free and vendor-neutral	Monitor threat intel feeds from government / ISACs	Subscribe to CISA, ENISA, NCSC-UK, ACSC bulletins

Outlook for 2025:

Resilient barriers against AI-powered social engineering

The World Economic Forum Global Risks Report 2024 ranks "misinformation and disinformation, incl. deepfakes" as the single most severe short-term global risk.[52] As models improve, synthetic media will become harder to spot with the naked eye, making systematic verification and layered controls indispensable. The good news for resource-constrained SMBs: many AI-powered defensive features are now built into mainstream cloud and security tools. Combining those capabilities with a culture that empowers employees to question first and comply second keeps the user as a final resilient barrier.

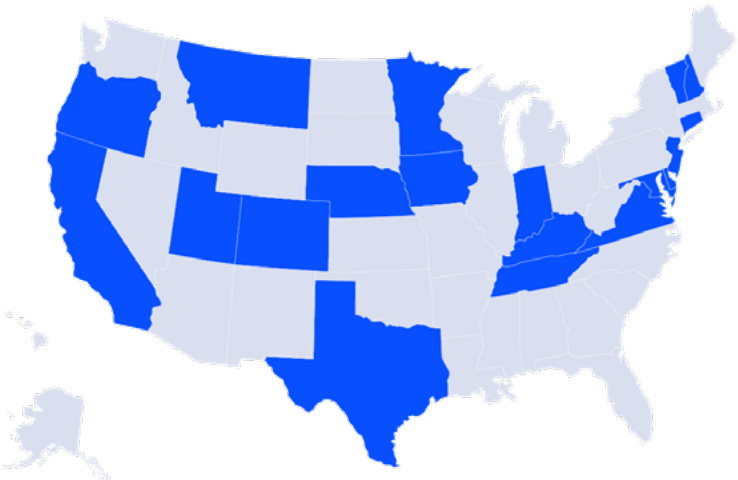
The Regulatory Reckoning:

Compliance Pressures Mount on SMBs

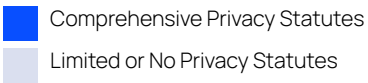
SMBs entered 2025 under unprecedented regulatory scrutiny. Ransomware featured in 88% of confirmed SMB breaches in the Verizon 2025 DBIR[53], while global cyberlosses reported to the FBI's IC3 soared to US $16 billion in 2024—up 33% year-on-year.[54] Lawmakers responded by accelerating disclosure clocks, expanding sectoral rules, and levying fines that can eclipse the direct cost of an incident.

United States: Federal rapid disclosure and privacy patchwork

The Security and Exchange Commission's cyberincident rule now compels even the smallest listed firms to file an 8-K within four business days; "smaller reporting companies" received only a 180-day reprieve to June 15, 2024.[55] Meanwhile, 19 states have enacted comprehensive privacy statutes, creating overlapping duties that capture many growth-stage SMBs.[56] Sector regulators also tightened screws: HIPAA settlements topped US $144 million across 152 cases, including single-office clinics[57], and the Federal Trade Commission's revised Safeguards Rule began enforcement in May 2024, extending security program obligations to small lenders and tax preparers.[58]



States with Comprehensive Privacy Statutes - July 2024[56]



Global regulatory pressure and new directives

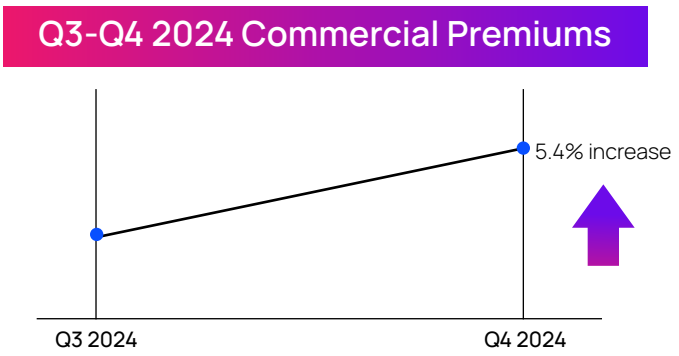
EU data protection authorities issued more than €2.5 billion in GDPR fines during 2024 alone.[59] At the same time, member states transposed the NIS2 Directive, which mandates cyber risk management and 24-hour incident reporting for medium-sized entities in 18 critical sectors with board-level liability for non-compliance.[60]

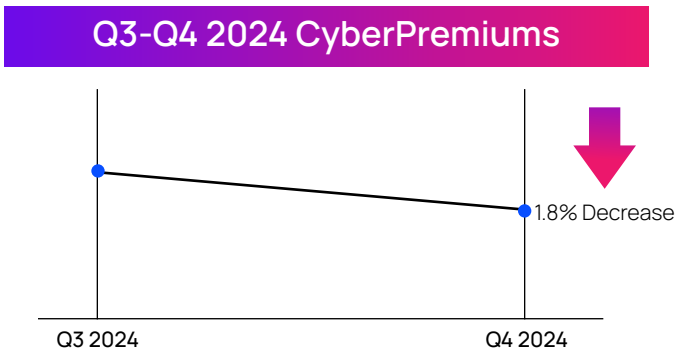
Australia also lifted its maximum penalty to AU $50 million, and India's Digital Personal Data Protection Act moved into phased enforcement signaling a global convergence toward mandatory baselines.

Enforcement gets teeth: Insurance and capital markets

Penalties are no longer theoretical. The Council of Insurance Agents and Brokers notes that globally, overall commercial premiums still rose 5.4% in Q4 2024, yet cyberpremiums fell 1.8%, but only for firms that could prove strong controls.[61]

Carriers increasingly refuse coverage or impose surcharges on non-compliant SMBs, while public companies that miss the SEC's four-day window risk shareholder litigation in addition to regulatory action.



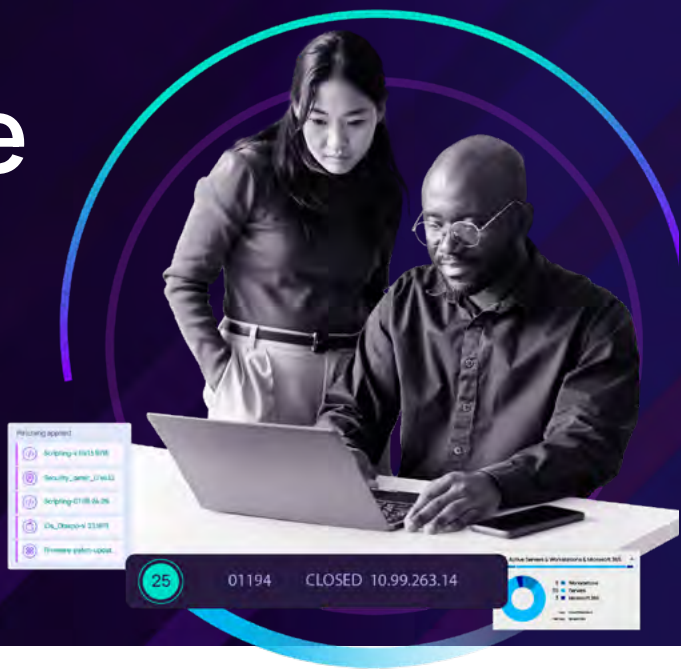


SMBs adapting under pressure from new frameworks

SMBs are fighting back by mapping regulations to common frameworks (NIST CSF, ISO 27001) and automating evidence collection. Encouragingly, SMBs are projected to continue the trend of increasing their IT budgets, with nearly a 7% increase in cybersecurity spending and a 10% increase in infrastructure spending projected in 2025.[62] Those that reach demonstrable compliance gain access to enterprise supply chains and favorable insurance terms while those lagging face mounting fines, higher premiums, and lost business.

Looking Ahead:

The Best Defense Is Going Back to Basics



The constant barrage of breach headlines and fearmongering articles tells a story of sophisticated adversaries launching rapidly evolving, AI-fueled attacks.

The harsh reality in 2025 is that SMBs remain the most attractive targets to the most active and effective cybercrime threats, specifically because they typically lack the defensive depth of large enterprises, including disaster recovery plans and backups, making them more fruitful for ransomware attackers.

Yet there's an empowering irony here: while the threats truly are evolving at an unprecedented pace, the basic tenets and foundational best practices of cybersecurity remain the best defenses against these new threats.

SMBs can drive a low-cost, high-ROI defense strategy by focusing on:

- Implementing phishing-resistant MFA
- Creating policies for handling invoicing and financial transactions safely
- Limiting remote access opportunities
- Maintaining a vulnerability management program
- Backing up data to a secure offline storage solution
- Creating disaster recovery and incident response plans and practicing them
- Deploying an EDR solution

The costs for these layered defenses have never been lower, and N-able provides many of these layers. Improving your SMB security can pay for itself the first time it mitigates a potentially devastating ransomware attack or BEC, let alone the potential regulatory and insurance premium costs of a compromise.

To learn more about the N-able unified cyber resiliency platform visit:
www.n-able.com/platform

References

[*, 1] https://www.verizon.com/business/resources/infographics/2025-dbir-smb-snapshot.pdf

[**, 35, 37] https://www.verizon.com/business/resources/reports/dbir/

[2] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a

[3] https://www.hhs.gov/sites/default/files/qilin-threat-profile-tlpclear.pdf

[4] https://news.sophos.com/en-us/2025/04/01/sophos-mdr-tracks-ongoing-campaign-by-qilin-affiliates-targeting-screenconnect/

[5] https://sublime.security/blog/tax-season-email-attacks-adwind-rats-and-tycoon-2fa-phishing-kits/

[6] https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

[7] https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

[8] https://www.axios.com/2024/12/03/global-elections-dodge-deepfake-threat

[9] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-215a

[10] https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf

[11] https://www.ic3.gov/annualreport/reports/2023_ic3report.pdf

[12, 16] https://www.verizon.com/business/resources/Tea/reports/2025-dbir-data-breach-investigations-report.pdf

[13] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-325a

[14] https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf

[15] https://www.cisa.gov/sites/default/files/2023-01/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

[17, 23, 27, 30, 47, 51, 53] https://www.verizon.com/business/resources/infographics/2025-dbir-smb-snapshot.pdf

[18, 40, 48] https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

[19] https://www.reuters.com/world/us/complaints-about-ransomware-attacks-us-infrastructure-rise-9-fbi-says-2025-04-23/

[20] https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024

[21] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024

[22] https://www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion-2025/

[24] https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf

[25] https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202024%20-%20EN_0.pdf

[26, 32] https://www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion-2025/

[28, 33] https://www.weforum.org/stories/2024/02/lockbit-ransomware-operation-cronos-cybercrime/

[29] https://www.justice.gov/archives/opa/pr/us-department-justice-disrupts-hive-ransomware-variant

[31] https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202024%20-%20EN_0.pdf

[34] https://www.reuters.com/world/us/complaints-about-ransomware-attacks-us-infrastructure-rise-9-fbi-says-2025-04-23/

[36] https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

[38] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

[39] https://www.comparitech.com/blog/vpn-privacy/phishing-statistics-facts/

[41] https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

[42] https://cyberreadinessinstitute.org/resource/2024-global-multifactor-authentication-mfa-survey-insights/

[43] https://www.ninjaone.com/blog/smb-cybersecurity-statistics/

[44] https://learn.microsoft.com/en-us/partner-center/security/security-at-your-organization

[45] https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/small-business-cybersecurity

[46] https://jumpcloud.com/blog/multi-factor-authentication-statistics

[49] https://www.fincen.gov/sites/default/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf

[50] https://www.enisa.europa.eu/topics/cyber-threats

[52] https://www.weforum.org/publications/global-risks-report-2024/

[54] https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report

[55] https://www.sec.gov/resources-small-businesses/small-business-compliance-guides/cybersecurity-risk-management-strategy-governance-incident-disclosure

[56] https://www.reuters.com/legal/legalindustry/new-state-privacy-laws-creating-complicated-patchwork-privacy-obligations-2024-06-07/

[57] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html

[58] https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know

[59] https://www.edpb.europa.eu/system/files/2024-04/edpb_annual_report_2023_en.pdf

[60] https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

[61] https://www.ciab.com/resources/q4-2024-p-c-market-survey/

[62, 63] https://www.analysysmason.com/contentassets/e5187a9660b64aa7a15a9aa5fd3d3df2/analysys_mason_smb_it_spending_forecast_may2024_rsmb1.pdf

N-ABLE™

At N-able, our mission is to protect businesses against evolving cyberthreats with a unified cyber resiliency platform to manage, secure, and recover. Our scalable technology infrastructure includes AI-powered capabilities, market-leading third-party integrations, and the flexibility to employ technologies of choice—to transform workflows and deliver critical security outcomes. Our partner-first approach combines our products with experts, training, and peer-led events that empower our customers to be secure, resilient, and successful. n-able.com **n-able.com**
