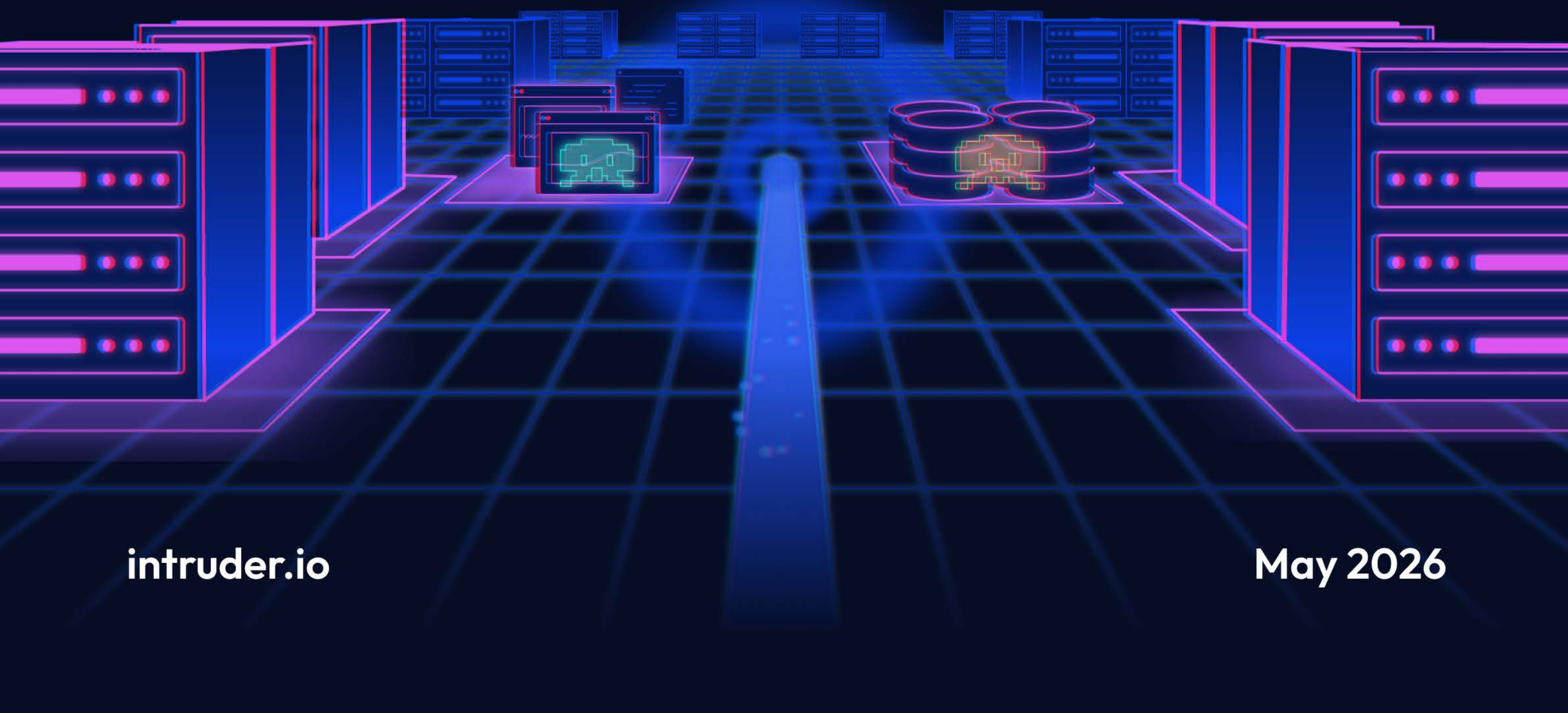
intruder

2026 Attack Surface Management Index

Top exposures, remediation trends, and industry benchmarks from 3,000 organizations



intruder.io

May 2026

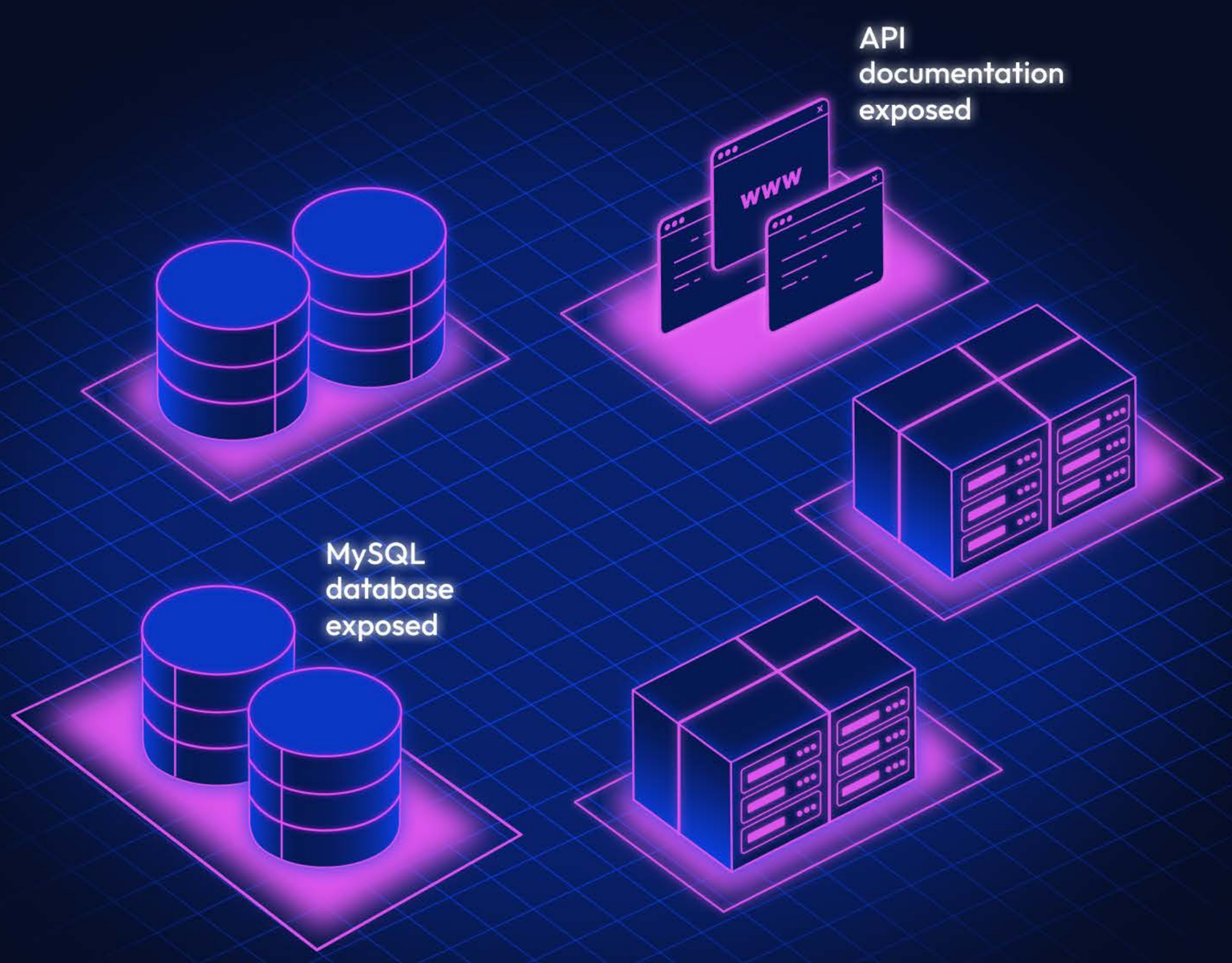
The exposure problem

With AI models like Anthropic's Mythos now capable of autonomously discovering thousands of zero-day vulnerabilities, any unnecessary software left facing the internet is carrying more risk than ever. When a new vulnerability is disclosed—like the SMB vulnerability that allowed WannaCry to infect 230,000 computers within days—every exposed instance becomes a target overnight.

And not every breach starts with a CVE. An exposed admin panel can be compromised with just a guessed password. It wouldn't get flagged by a traditional vulnerability scanner, but it could be the overlooked exposure that gives an attacker their initial foothold.

The 2026 Attack Surface Management Index shows what this risk actually looks like across 3,000 organizations: the most common exposures, how quickly they’re being fixed, and how that varies by industry and organization size.

Based on anonymized data from Intruder customers covering the 12 months to March 2026



Attack surface exposures by category

Proportion of organizations affected by at least one attack surface exposure in each category over the past 12 months, and the three most common issues within each.

60%

HTTP panels

1. WordPress Admin
2. phpMyAdmin
3. Dell iDRAC

49%

Ports and services

1. Remote Desktop (RDP)
2. SNMP
3. UPnP

42%

Databases

1. MySQL
2. Postgress
3. MS SQL

30%

Files and information

1. API documentation
2. web.config files
3. Apache configuration files

RDP tops the ports and services category. It's a common initial access vector in ransomware attacks (Mandiant M-Trends 2025), and was notably affected by BlueKeep, a pre-auth code execution weakness that left nearly a million exposed systems immediately exploitable without credentials. It's one of the clearest cases of a service that shouldn't be internet-facing.

Databases were given their own category, separate from ports and services, due to their prevalence. In 2020, the PLEASE_READ_ME ransomware campaign targeted internet-facing MySQL servers, compromising over 250,000 databases by brute-forcing weak credentials. Similar attacks have hit exposed MongoDB and Elasticsearch instances, with attackers wiping data and demanding ransom for its return.

The leading files and information exposure is API documentation. While some API docs need to be public by design, it's often overlooked when the documentation is for private admin-side APIs that don't need to be publicly accessible.

Top 10 attack surface issues

HTTP panels, ports, services, databases, files, and information exposed to the internet that shouldn't be. Percentages represent the proportion of organizations affected by at least one issue in the past 12 months.

1	**MySQL Database Exposed**	**26%**
2	**Postgres Database Exposed**	**16%**
3	**API Documentation Exposed**	**15%**
4	**WordPress Admin Panel Exposed**	**15%**
5	**Remote Desktop Service Exposed**	**11%**
6	**SNMP Service Exposed**	**9%**
7	**phpMyAdmin Admin Panel Exposed**	**8%**
8	**UPnP Service Exposed**	**8%**
9	**NTP Service Exposed**	**7%**
10	**RPC Portmapper Service Exposed**	**7%**

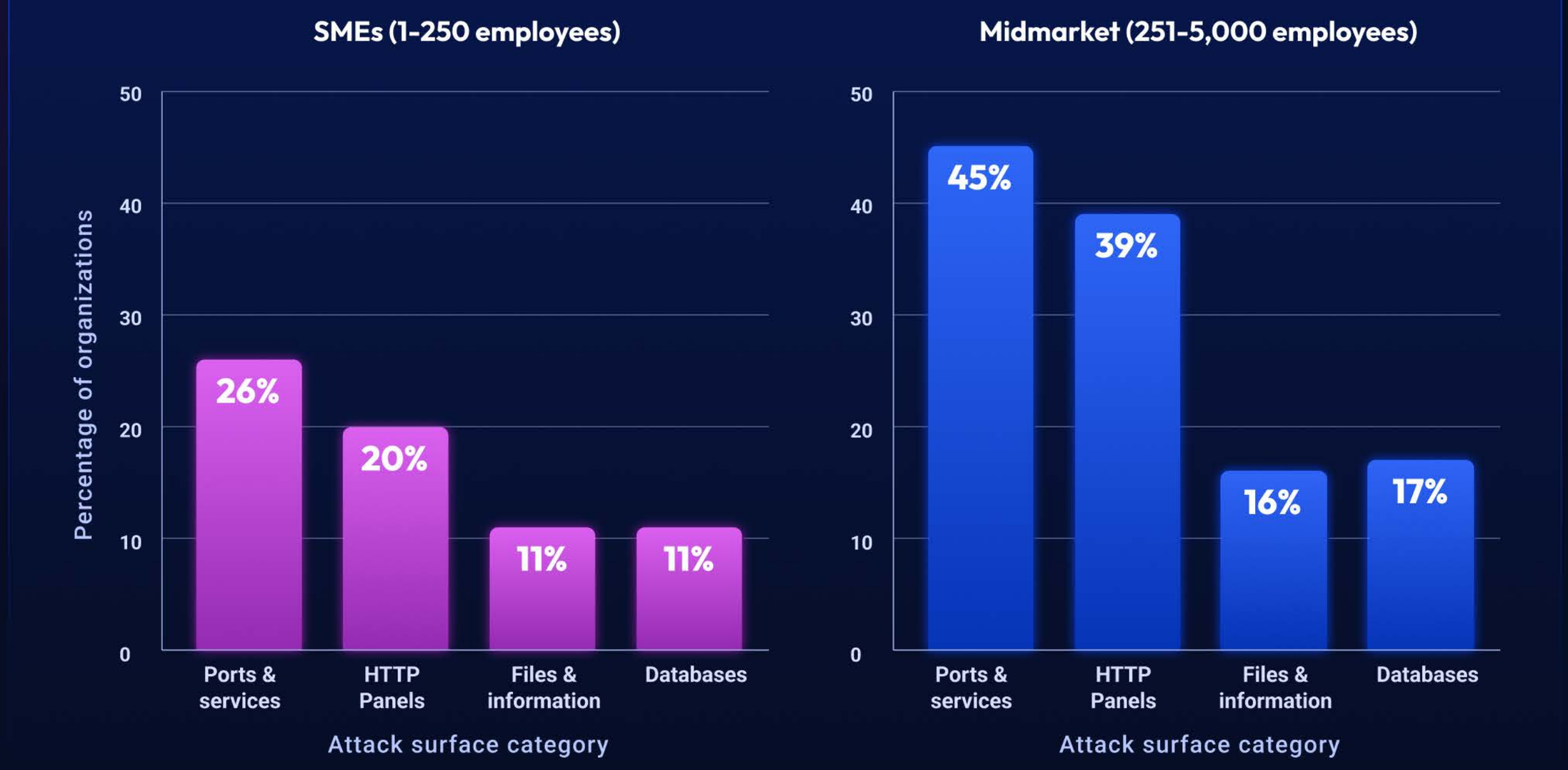
Exposed databases take the top two spots, with over a quarter of organizations having an exposed MySQL database, and Postgres affecting 1 in 6.

More than 1 in 7 organizations exposed API documentation, ranking ahead of Remote Desktop—a common entry point in ransomware attacks.

Legacy services intended for internal networks, rather than the internet, make up the rest of the top 10 (SNMP, UPnP, NTP and RPC).

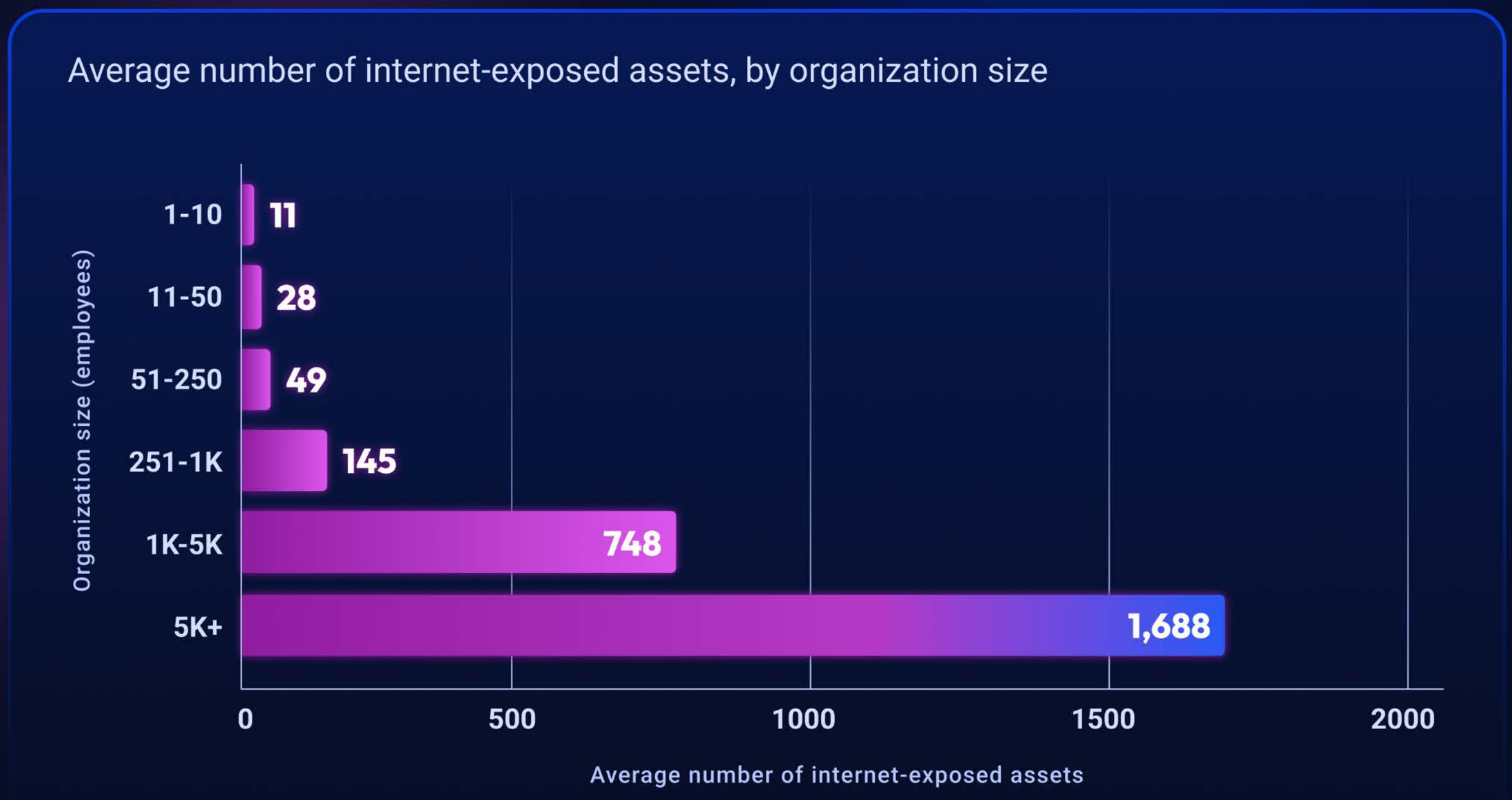
Attack surface exposures by organization size

Proportion of organizations affected by at least one issue in each category over the past 12 months, comparing those with 1-250 employees (SMEs) and 251-5,000 employees (midmarket organizations).



As organizations grow, so does the problem. 54% of SMEs had at least one attack surface exposure in the past 12 months—for midmarket organizations, that rises to 70%. The gap is consistent across every category. Among SMEs, 26% had risky ports and services exposed and 20% had admin panels exposed. For midmarket, those numbers rise to 45% and 39%.

How the number of exposed assets varies by organization size



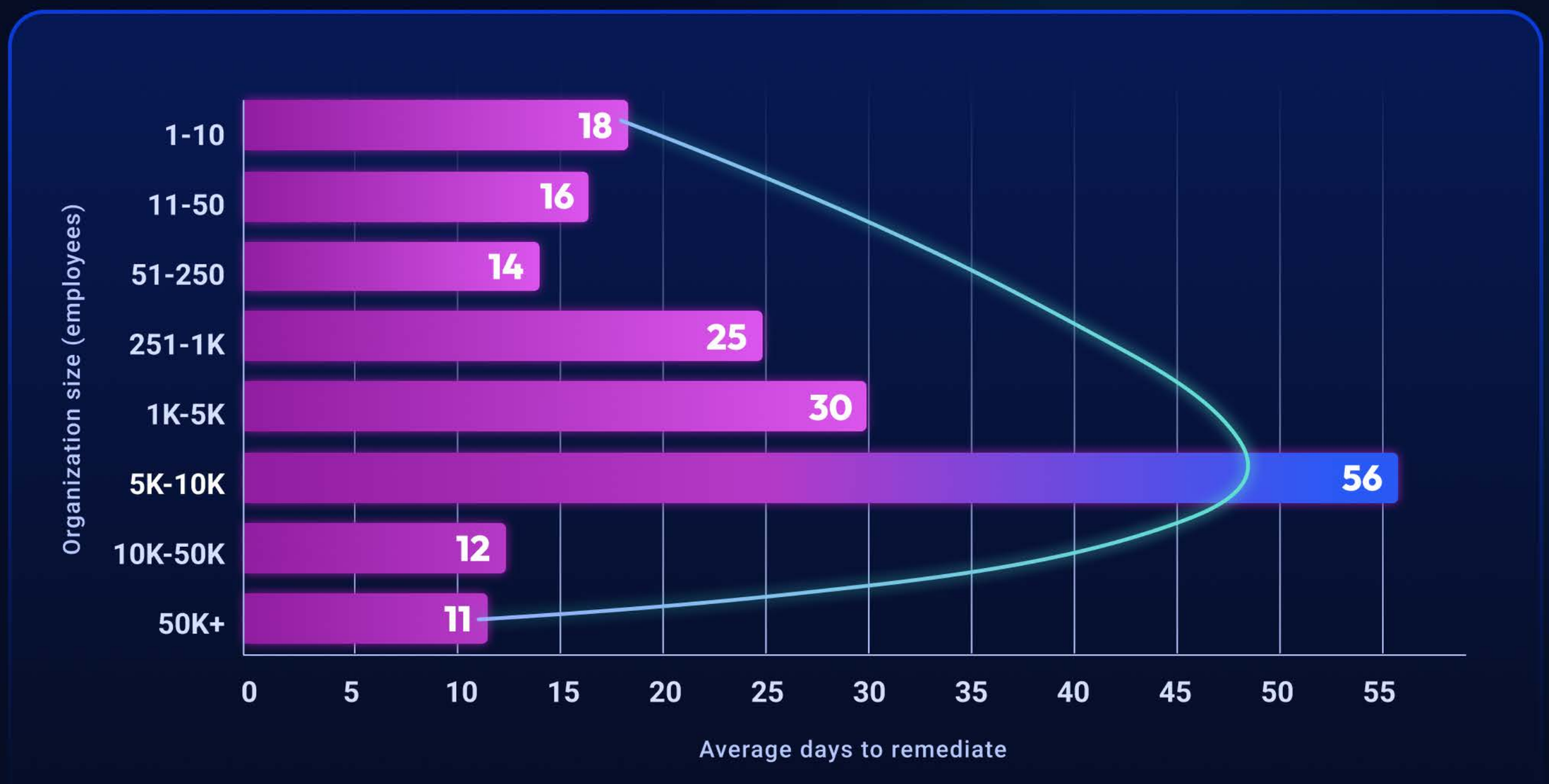
It's no surprise that the number of internet-exposed assets grows with organization size. What stands out is the scale of the jump at the upper end of the midmarket.

Organizations in the 5,000+ band manage an average of nearly 1,700 external assets—more than twice as many as those in the 1,000–5,000 band.

This is where attack surface management gets significantly harder. The infrastructure is scaling fast, but security teams, budgets, and tooling don't always grow at the same rate.

That strain shows up in longer remediation times: organizations with 5,000–10,000 employees also have the slowest average time at 56 days (page 7).

Average days to remediate attack surface issues, by organization size

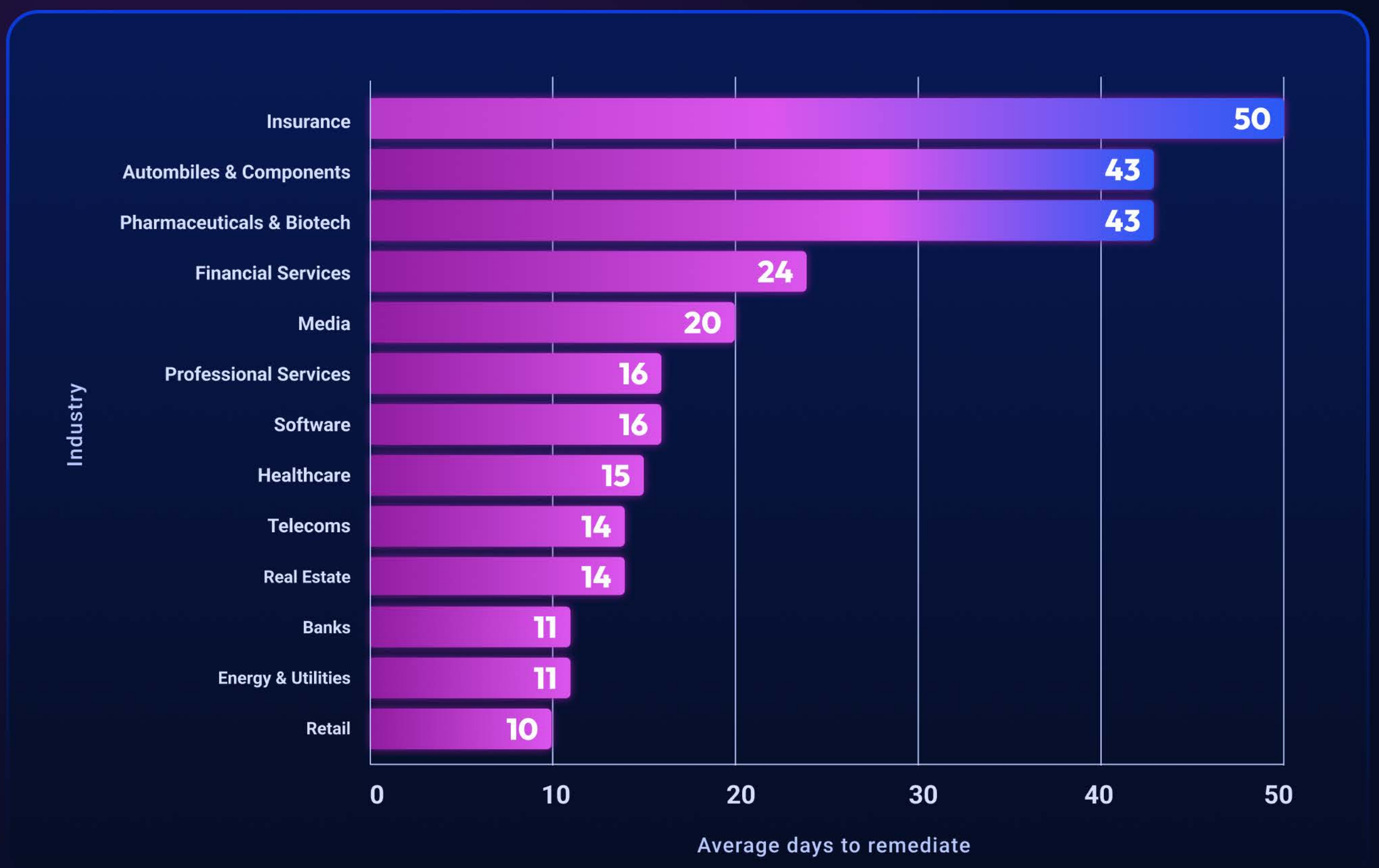


Small organizations (1–250 employees) remediate fastest, averaging 14–18 days. As organizations grow into the 250–10,000 range, remediation slows, peaking at 56 days for the 5,000–10,000 band.

This aligns with what we found in our 2026 Security Middle Child report: midmarket organizations have large attack surfaces, but lack the headcount, budget, and tooling maturity of enterprise security teams, which could explain the longer remediation times.

Remediation times improve again at the largest sizes, suggesting that the midmarket is the hardest hit.

Average days to remediate attack surface issues, by industry



Insurance is the slowest at nearly 50 days, which is five times longer than the fastest industry (Retail). It also has the largest average perimeter size (see appendix), which may partly explain the gap.

Pharmaceuticals & Biotech and Automobiles & Components aren't far behind at 43 days—industries you might expect to have the resources to move faster.

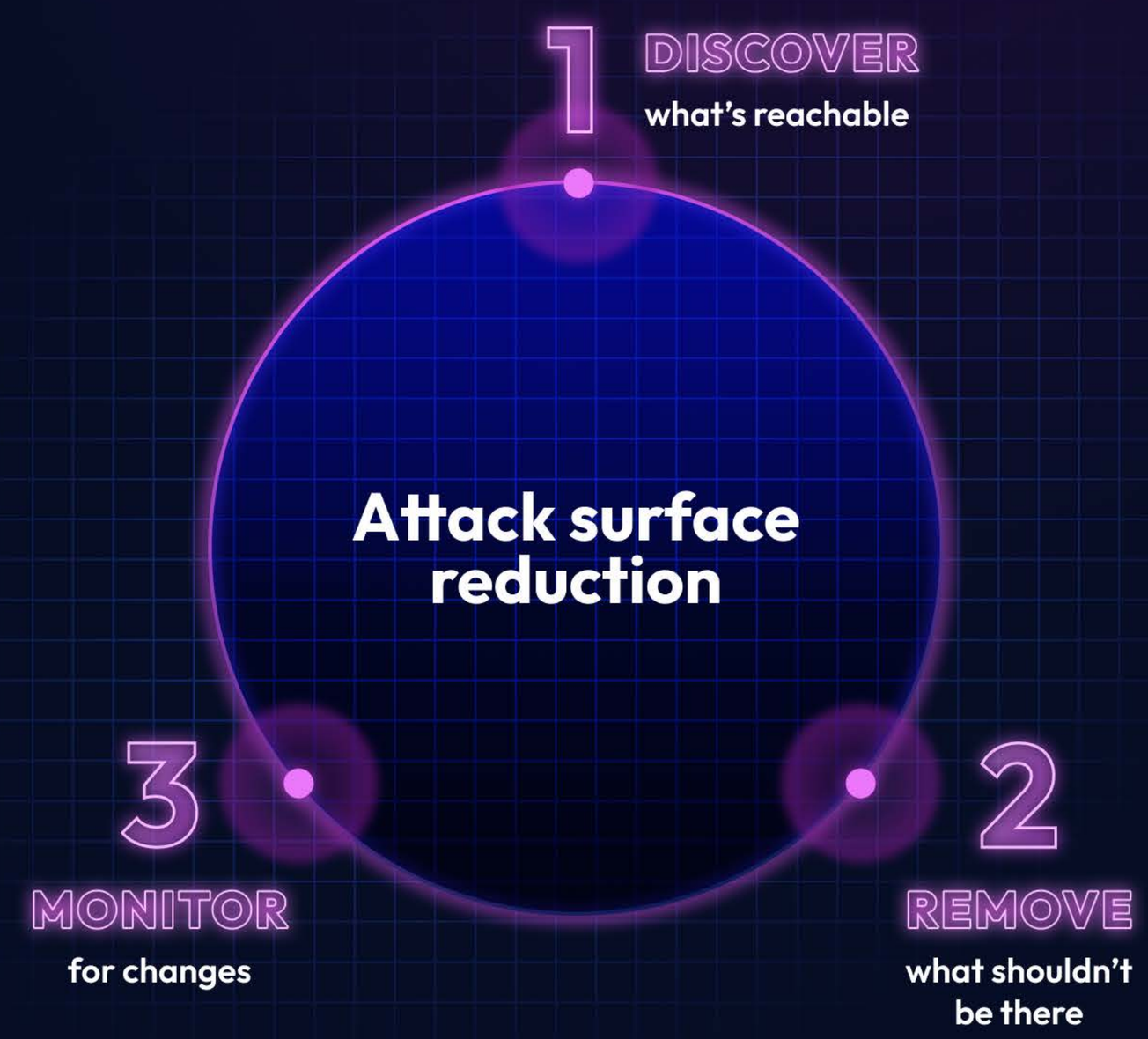
One of the sharpest contrasts is Banks (11 days) vs. Financial Services (24 days). Despite operating in the same broad sector, banks remediate more than twice as fast. This could be driven by heavier regulatory pressure.

Removing exposure before it becomes a problem

Vulnerability management and attack surface reduction go hand in hand—but while most teams focus on patching what's vulnerable, fewer are asking whether it should be exposed at all.

AI is compressing the time between vulnerability disclosure and exploitation. But if the affected service doesn't need to be—and isn't—reachable from the internet, the window of risk is significantly reduced.

Attack surface management exists to solve exactly this problem: reducing what's exposed before it can be exploited.



About Intruder

Intruder's exposure management platform helps lean security teams stop breaches before they start by proactively uncovering attack surface weaknesses. Since 2015, the platform has helped customers take more than 133,000 exposures off the internet.

Designed to cut through the noise and complexity, Intruder makes it easy to discover exposed assets, detect misconfigs, prioritize real risks, streamline security workflows, stay compliant and mobilize teams to fix issues fast.

By unifying attack surface management, cloud security, AI pentesting, and continuous vulnerability management in one intuitive platform, Intruder makes it easy to secure your entire infrastructure—from apps and APIs to cloud accounts and employee devices.

Founded by Chris Wallis, a former ethical hacker turned corporate blue teamer, Intruder was selected for GCHQ's Cyber Accelerator and is now protecting over 3,000 companies worldwide.

Start a free trial or book a call with one of our experts at intruder.io

Read our reviews on G2.com

Appendix: Perimeter size by industry

Average number of internet-exposed network services per asset, by industry, to show attack surface size. Includes all ports and services, not just those deemed an attack surface risk.