INDUSFACE™

STATE OF APPLICATION SECURITY

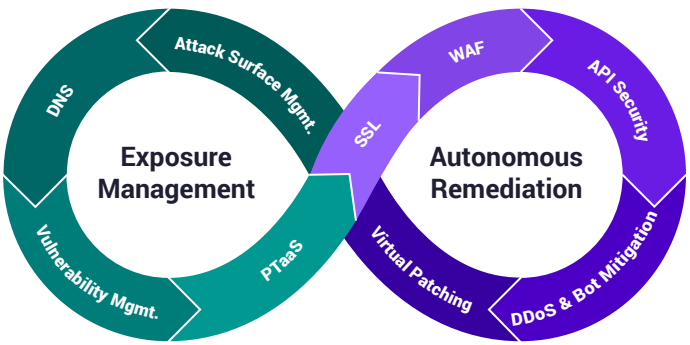
SMBs | Q1 2025

INDEX

APPTRANA

AI-POWERED APP SECURITY.

HUMAN-VERIFIED ACCURACY.



START YOUR FREE TRIAL NOW

ABOUT INDUSFACE

Indusface is a leading application security SaaS company, securing over 5,000 customers across 95 countries with its award-winning platform. Funded by institutional investors, it has been a category leader in Gartner Peer Insights™ for the past three years.

The industry's only AI-powered, all-in-one AppSec platform helps businesses discover, detect, remediate, and protect web applications and APIs at internet scale, backed by a 100% uptime guarantee.

TRUSTED BY 5000+ CUSTOMERS ACROSS 95 COUNTRIES

Customer's Choice for
3 Years in a Row

Highest Rated Cloud WAAP

100% Recommendation

4.9 Stars of 5

FORRESTER®
Q4 Report 2024
The Web Application Firewall Solutions Landscape

Gartner
Market Guide 2023
Cloud Web Application and API Protection (WAAP)

S&P Global
Market Intelligence
451 Research
Technology Data, Research, & Advisory

EXECUTIVE SUMMARY

894
Million
Total attacks on SMBs in Q1 2025

2.24
Million
Average attacks per SMB site — **153% higher** than enterprises

71%
Increase in attacks compared to Q1 2024

763
Million
DDoS attacks — making up 85% of all attacks

97 out of 100
SMB sites were hit by bots — with **1/3rd** of attacks from bad bots

12x
more attacks on each API host compared to websites

70x
higher DDoS attacks on APIs vs websites

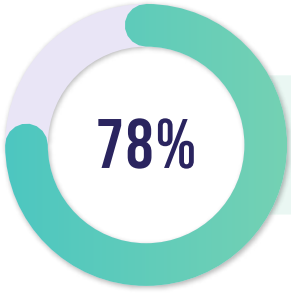
78%
of SMBs are concerned that a could put them out of business

OVERVIEW:

Small and mid-sized businesses (SMBs) are the economic backbone of the global economy. They make up over 90% of all businesses, employ more than half of the global workforce, and contribute approximately 45% to global GDP. From retail and healthcare to SaaS, eCommerce, and finance, SMBs form the foundation of the country's innovation and resilience.

But while their impact is large, their defenses are often limited.

The **State of Application Security for SMBs - Q1 2025** report analyzes a sample of over **400 SMB** sites and compares attack trends from **Q1 2024** with those from **Q1 2025.** The data reveals a sharp increase in targeted cyberattacks, particularly at the application layer, where customer-facing web apps and APIs are increasingly exploited. **894 million attacks** were witnessed in Q1 2025, with an **average of 2.24 million attacks per website,** marking a **71% increase** compared to Q1 2024. Alarmingly, attacks per SMB site were **153% higher** compared to enterprises. As SMBs grow more digital, attackers have shifted their focus from network perimeters to application endpoints that offer higher value and lower resistance.



of SMBs are concerned that a Cyber Attack Could Put Their Organizations Out of Business[1].

Despite growing awareness, most SMBs continue to rely on outdated, siloed, or resource-heavy security tools, leaving them exposed to threats like credential-stuffing bots, API scraping, business logic abuse, and application-layer DDoS.

This report analyzes how the application threat landscape evolved over the past year, why SMBs are uniquely at risk, and how a modern, scalable approach to AppSec can help close the protection gap. It also outlines how MSPs and fully managed security providers are positioned to help SMBs address these challenges—through integrated, automated, and fully managed solutions.

1. INTRODUCTION: THE RISING TIDE OF THREATS ON SMBS

The cyber threat landscape is evolving fast, and SMBs are increasingly in the crosshairs. In Q1 2025 alone, over **894 million attacks** were witnessed across SMBs, with each site witnessing an average of **2.24 million attacks.** Attacks per SMB site were **153% higher than enterprises.**

Key Attack Trends:

DDOS

763 million DDoS attacks were observed in Q1 2025, contributing to **85% of overall attacks.** SMBs experienced **19x higher** DDoS attacks compared to enterprises and an **80% increase** compared to Q1 2024.

APIs

Attack activity on APIs rose by **4x** in Q1 2025 compared to Q1 2024, and DDoS on APIs spiked by **11x.** Compared to websites, **each API host witnessed 12x higher overall attacks.** Custom rules and positive security policies helped block over **1.2 million attacks per API.**

VULNERABILITIES

Attacks on website vulnerabilities grew by **264%,** while attacks on **API vulnerabilities surged by 100x.**

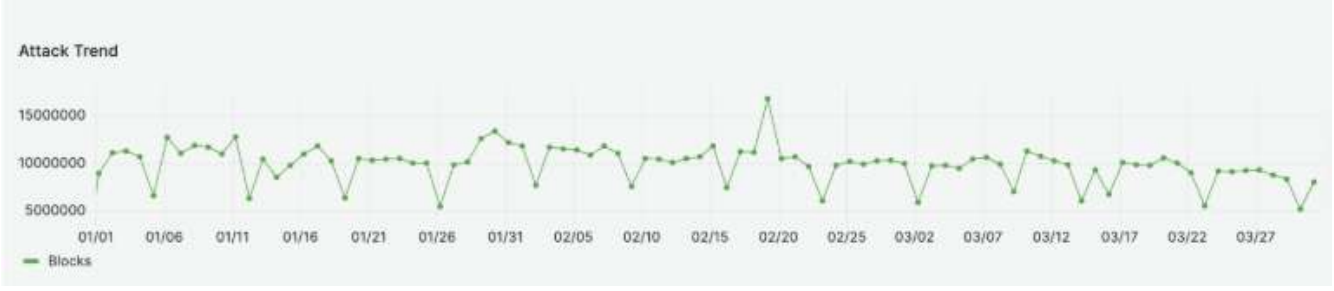
BOTS

5.75 million bot attacks were observed, with **97 out of 100 sites** affected. Notably, **1/3rd of bot attacks** originated from bad bots.

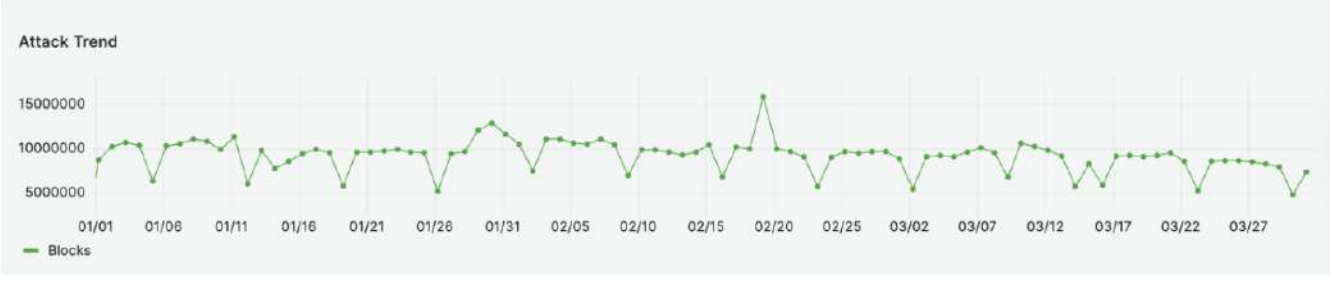
Ashish Tandon
Founder & CEO, Indusface

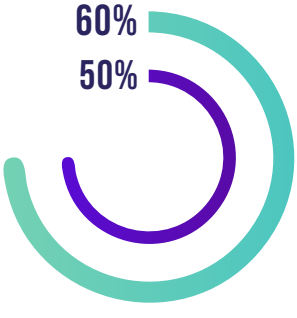
"Cybercriminals are constantly evolving their tactics, leveraging different attack vectors based on industry, application type, and company size. APIs, for example, face 12x attacks per host when compared to web apps."

Here's the overall attack trend witnessed in Q1 2025:



API attack trend Q1 2025:





of SMBs report feeling inadequately prepared for cyber threats[2].

of breaches impacting SMBs were tied to application vulnerabilities[3].

2. WHY SMBS ARE MORE VULNERABLE

Several structural and operational realities make SMBs easier targets:

SMALL TEAMS, BIG ATTACK SURFACES

Most SMBs have fewer than five IT/security staff managing dozens of web apps, APIs, and cloud services.

FRAGMENTED TOOLS

A mix of open-source scanners, basic WAFs, and manual processes results in poor visibility and delayed response.

COMPLIANCE COMPLEXITY

Regulated industries like finance, healthcare, and eCommerce face growing audit pressure but lack automation.

SLOW REMEDIATION

Over **30% of critical vulnerabilities remain unpatched for 180+ days** due to limited staff and prioritization gaps.

3. THE SHIFT IN ATTACK TACTICS

Over the past year, attackers have adopted methods that are faster, more evasive, and easier to execute—even for less experienced actors.

The rise of Large Language Models (LLMs) and AI tools like ChatGPT, DeepSeek, and others has significantly lowered the barrier to entry for launching cyberattacks. With these tools, even novice attackers can craft payloads, scan for vulnerabilities, and automate exploit chains—leading to a noticeable spike in application-layer threats targeting SMBs.

Here are some noticeable trends:

DDOS IS NOW THE #1 ATTACK VECTOR FOR SMBS

SMB websites and applications face significantly more DDoS attacks than enterprises—**763 million in Q1 2025 alone,** contributing to **85% of total attack volume.** These attacks quietly degrade services and often go undetected by network-based tools. Most SMBs lack 24/7 monitoring, and security duties often fall on overstretched IT or DevOps teams.

APIS ARE EXPOSED AND UNDER-PROTECTED

With more SMBs relying on APIs for mobile apps, partner access, payment, eCommerce, and more, attackers are targeting them for data scraping and logic abuse. Many SMBs lack API documentation and discovery processes, leaving shadow APIs and endpoints unmonitored and vulnerable. Each API host witnessed **12x more total attacks, and 70x higher DDoS attacks compared to websites.**

VULNERABILITIES ARE RISING AND REMAIN UNPATCHED

SMBs have 4x more open critical/high vulnerabilities than enterprises. Limited staff and alert fatigue delay patching, increasing the risk of exploitation, especially when known flaws remain open for weeks or longer. Vulnerability-based attacks on website vulnerabilities grew by 264%, whereas attacks on API vulnerabilities spiked by 100x, underscoring the urgent need for proactive protection.

BOTS ARE MORE EVASIVE AND HARDER TO STOP

Bots now mimic human behavior—emulating mouse movement, bypassing CAPTCHAs with AI, rotating IPs, and blending into normal traffic. These human-like bots are widely available and harder to detect with traditional tools, making them one of the most persistent threats facing SMBs.

INDUSFACE offers a fully managed AppSec platform that is very affordable, even for SMBs. This helps SMBs with DDoS & bot monitoring/mitigation, provides continuous vulnerability scanning, and remediates open vulnerabilities within 72 hours. As vulnerabilities grow and attacks become more sophisticated, the need for robust protection becomes more critical than ever to ensure SMBs can maintain secure and uninterrupted operations.

4. SECURING SMBS IN AN EVOLVING THREAT LANDSCAPE

As cybersecurity risks continue to escalate, small businesses are increasingly becoming prime targets for attacks. With limited resources and outdated security measures, many SMBs find themselves exposed to evolving threats that outpace traditional defenses.

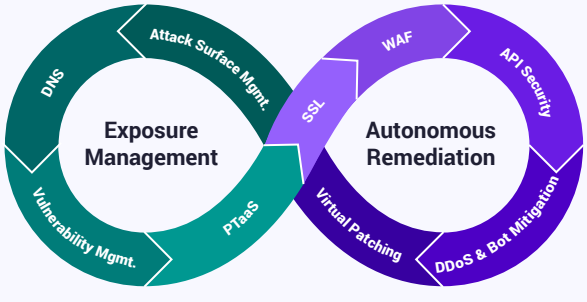
Issues like data loss, regulatory fines, service disruptions, customer churn, and brand damage can hit SMBs disproportionately hard compared to enterprises. The financial and reputational burden often falls squarely on a small team, with little room to recover.

Trusted partners - whether MSPs, MSSPs, or end-to-end security platform vendors like **INDUSFACE,** play a vital role in bridging this gap. By offering fully managed, all-in-one application and API security platforms, they allow SMBs to simplify their defenses without compromising on effectiveness.

Here's how:

- Always-on AI-powered protection for websites, APIs, and applications
- DDoS and zero-Day mitigation that adapts to behavioral attack patterns along with 24/7 SOC monitoring
- Autonomous remediation that patches open vulnerabilities fast, and doesn't bombard the security teams with just alerts & false positives
- Built-in compliance reporting for SOC2, PCI DSS, HITRUST, and more

AI-Powered, Continuous Compliance for Web Apps and APIs



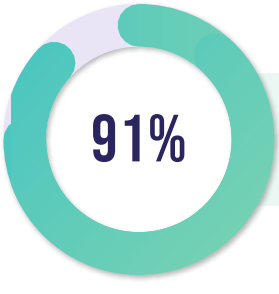
No false positives. No open vulnerabilities. AI-powered WAAP with human verification ensures every app and API is protected against all known threats—remediated within 72 hours, an industry only capability.

Ashish Tandon
Founder & CEO, Indusface

"Security teams can stay ahead by investing in all-in-one, AI-powered AppSec platforms that adapt quickly to these evolving threats. However, even with AI, manual oversight is essential to prevent AI hallucinations and ensure uninterrupted business operations. This balanced approach that combines the agility of AI with human expertise helps us protect business critical applications of 5000+ global customers"

Instead of juggling fragmented point solutions, SMBs can bridge the gap by turning to trusted partners—MSPs, MSSPs, or unified security platform providers. With fully managed, all-in-one solutions, these partners help SMBs stay secure and compliant, without adding complexity.

- Access expert-driven and verified protection instantly
- Reduce risk and liability
- Accelerate compliance and audit readiness
- Eliminate the burden of managing multiple tools



of SMBs said they would switch to a provider offering proactive security and compliance support[4].

SMBs need outcomes, not alerts. They need protection that scales with them, not against them. And they need it now—through trusted partners who bring security, compliance, and peace of mind as a service.

Venkatesh Sundar
Founder & President – Indusface

"Small doesn't mean safe. In fact, SMBs are often seen as low-hanging fruit due to their limited resources and slower patch cycles"

References:

1. **Microsoft:** https://techcommunity.microsoft.com/blog/microsoft-_365blog/new-smb-security-innovations-from-microsoft-inspire-2023/3876477

2. **VikingCloud's 2025 SMB Threat Landscape Report:** https://www.vikingcloud.com/resources/viking-clouds-2025-smb-threat-landscape-report-small--and-medium-sized-businesses-big-cybersecurity-risks

3. **Sectigo:** https://www.sectigo.com/resource-library/-study-finds-50-of-smbs-have-experienced-a-website-breach-and-40-are-being-attacked-monthly

4. **ConnectWise:** https://www.connectwise.com/company/press/releases/2020-van-son-bourne-smb-research-release

INDUSFACE™

DALLAS | BENGALURU | VADODARA | MUMBAI | NEW DELHI

Indusface is a leading application security SaaS company, securing over 5,000 customers across 95 countries with its award-winning platform. Funded by institutional investors, it has been a category leader in Gartner Peer Insights™ for the past three years.

The industry's only AI-powered, all-in-one AppSec platform helps businesses discover, detect, remediate, and protect web applications and APIs at internet scale, backed by a 100% uptime guarantee.

Contact Us: +1 866 458 3058 | +91 265 6133021

Email - sales@indusface.com | Website - www.indusface.com