SiteLock

A SECTIGO® COMPANY

2024 SITELOCK ANNUAL WEBSITE SECURITY REPORT

TABLE OF CONTENTS

02

TABLE OF CONTENTS

03

04 The web doesn’t stand still and neither do the threats that target it.

In this shifting landscape, your website is more than just a storefront- it’s your brand’s frontline, your customer’s first touchpoint and a constant target for cybercriminals. That’s why security can no longer be treated as a background task. It’s a front-of-house priority. In 2024, SiteLock scanned over 14 million websites and processed more than 29 billion scans each month. What we observed reinforced a powerful truth: **Every breach is a brand breach.**

We saw attacks that didn’t just target infrastructure - they eroded brand value. Redirects hijacked customer journeys. Defacements damaged credibility. Malware that turned high-traffic sites into blacklisted domains. Each incident wasn’t just a technical failure - it was a customer lost, a brand diminished.
Cybercrime has evolved- trading smash-and-grab tactics for layered, persistent campaigns built to monetize, manipulate and remain invisible. In 2024, a single infection often meant multiple malware families working in tandem, each playing a role in a broader, coordinated breach. We saw the rise of AI-powered phishing kits, critical malware designed to embed deep within infrastructure and infections that escalated quietly over time. Bot traffic outpaced human visitors by more than 12 to 1, enabling relentless reconnaissance and automated exploitation at scale. CMS platforms especially WordPress and Joomla faced repeated compromises, largely through outdated and/or vulnerable plugins.

Put simply, today’s threats don’t give small businesses the luxury of lag. Cybercrime today isn’t just faster - it’s more relentless, more scalable and more accessible than ever, leaving SMBs with less room for error and even less time to respond. Yet amid the complexity, there’s a clear opportunity:

Security isn’t just a shield - it’s a signal of trust.
Clean, secure websites load faster. Rank higher. Convert better.
They reflect professionalism, strengthen customer loyalty and give SMBs a real edge - especially when competing against larger, better-resourced players.

This report is more than a postmortem on malware. It’s a blueprint for what’s next. Inside, you’ll find the key trends that defined 2024, along with practical recommendations built for small teams - insights to help you make informed decisions, prioritize effectively and stay resilient in a constantly shifting landscape.

At SiteLock, we’re not just here to protect websites. We’re here to protect what they stand for.
Because every alert prevented, every vulnerability patched, every infection blocked isn’t just a technical win - it’s a brand investment. And in today’s digital economy, trust is the currency that matters most.

Thank you for trusting SiteLock to protect your corner of the web.

The SiteLock Team

The 2024 SiteLock Annual Website Security Report is a deep analysis of threats targeting small and midsize business (SMB) websites. It explores malware behavior, CMS vulnerabilities, bot activity, alert volume and attacker economics helping SMBs understand not just what threats exist, but how they're evolving and where action is needed most.

Drawing from over **27 billion monthly scans** across a network of **14+ million sites**, the data reveals that cyberattacks in 2024 didn't just grow they matured. Powered by automation and scaled through AI, modern threats unfolded as multi-phase campaigns, designed to linger, layer and escalate. Critical and medium-severity malware made up the core of these infections, forming the backbone of today's breach patterns.

Bot traffic surged, outnumbering human visitors by more than 12 to 1, often used for constant probing and automated exploitation. CMS-based websites especially those running WordPress and Joomla, remained top targets due to plugin vulnerabilities and poor update hygiene.

Across the board, attackers are getting sharper. They're deploying reinfection-ready malware, weaponizing automation and exploiting weaknesses faster than ever. Whether you're a site owner, developer, or hosting provider, this report offers a clear lens into what's happening- and what you can do next. It's designed to help you anticipate risks, prioritize defenses and stay resilient in a threat landscape that never sits still.

Key findings include: Key Takeaways for 2024

567M
verified threats blocked per month
A volume increase over 2022 when adjusted for improved reporting precision

1.7M
infected files cleaned weekly
With infections frequently involving multiple malware strains

Bots dominated
with traffic exceeding human visitors by 12.6x
Scanning and exploiting at scale with little human intervention

Critical malware surged by 86%
Pointing to attacker escalation strategies that prioritize long-term site control

Medium and low-severity threats jumped 202% and 189% in prevalnce
Acting as the new "silent starters" in modern attacks

Site hygiene matters:
High-risk sites were 62x more likely to be infected
than low-risk ones

CMS-powered sites **were up to 31% more likely to be compromised**
than custom-coded websites

METHODOLOGY

06

The data presented in this report is derived from over 14 million active websites monitored through the SiteLock global threat detection platform between January and December 2024.
Data sources include automated website scanners, malware remediation logs, threat alerts triggered by our vulnerability detection systems and real-time telemetry from the SiteLock customer network.

Key scanning methods include:

- **SMART Scanning (Secure Malware Alert & Removal Tool):**
  Automates the detection and cleanup of malware files
- **Single-scan and multi-scan methods:**
  Used to inspect billions of files each month combining signature-based and heuristic analysis.

Weekly and monthly averages were calculated to normalize findings across varying scan frequencies and customer configurations.

Data Scope:

27B
files scanned monthly via multi-scan methods

2B
files scanned monthly via single-scan methods

1.7M
infected files cleaned per week on average

Adjustments in 2024 Methodology

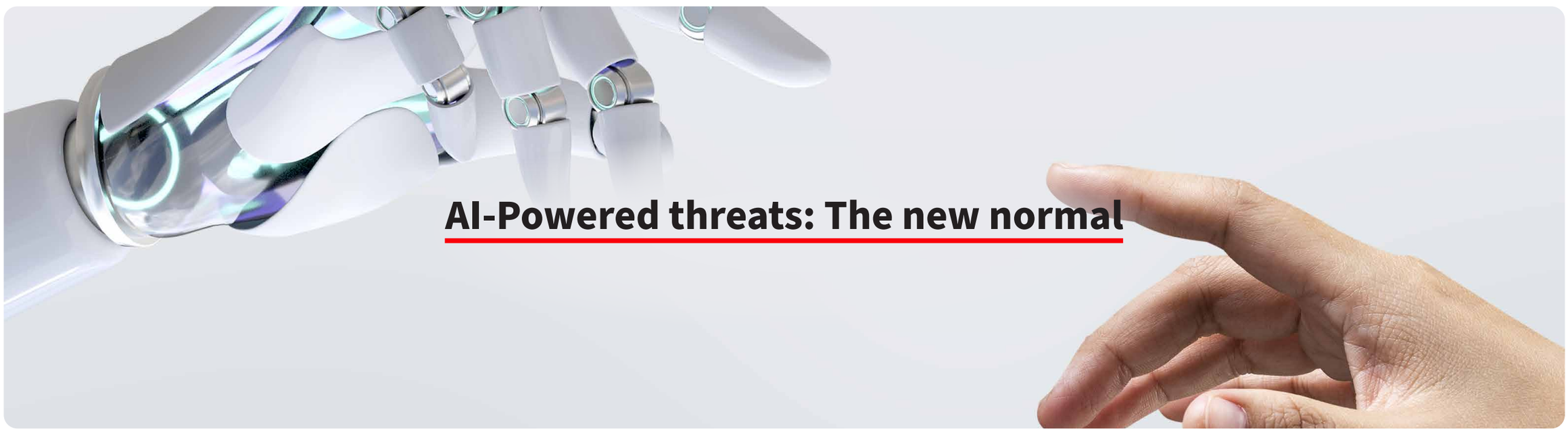
SiteLock refined its analytics approach to improve signal-to-noise clarity:

- **Blacklisting Data Removed:**
  Blacklisting data was removed from reporting due to Google SafeBrowsing API policy changes in early 2023.
- **Bot Traffic Exclusion in Threat Volume:**
  Beginning in 2023 and continuing into 2024, SiteLock **refined its firewall analytics methodology** excluding non-verified and ambiguous bot activity to focus solely on confirmed threats. This change impacts direct year-over-year comparisons to data collected prior to 2023.
- **“Threats blocked”** now refers strictly to confirmed malicious activity excluding ambiguous traffic patterns.
- **Alerting Enhancements:**
  In 2024, SiteLock expanded its vulnerability intelligence platform. High and critical alert counts are significantly higher than previous years due to the inclusion of new detection rules and broader platform coverage.

This report focuses exclusively on data observable through SiteLock's scanning and protection infrastructure. It does not account for websites not enrolled in active scanning.

THE BIG TRENDS SHAPING WEBSITE SECURITY

07



AI-Powered threats: The new normal

Artificial intelligence is now embedded across the modern attack lifecycle. Cybercriminals have fully embraced AI, dramatically elevating the sophistication and success rate of attacks. AI is now routinely used to craft highly realistic phishing emails and social media impersonations, making traditional defenses significantly less effective. Deepfake technology has enabled attackers to convincingly mimic voices and videos of trusted individuals, intensifying risks associated with social engineering.

Moreover, AI-driven malware has become more adaptive, capable of real-time mutation and evasion of traditional detection mechanisms. This shift underscores the importance of SMBs implementing advanced, proactive cybersecurity defenses to counteract these sophisticated threats.

Bots: The escalating arms race

Automated bot attacks continue to grow in both frequency and sophistication, with malicious bots accounting for **12.6 times more traffic** than human visitors in 2024 -a **28% increase year-over-year**. These bots scanned sites for vulnerabilities, executed brute-force login attempts and delivered payloads at scale. Many were capable of mimicking human behavior, bypassing traditional security filters.

This growing sophistication demands behavior-based threat detection, not just static blacklists

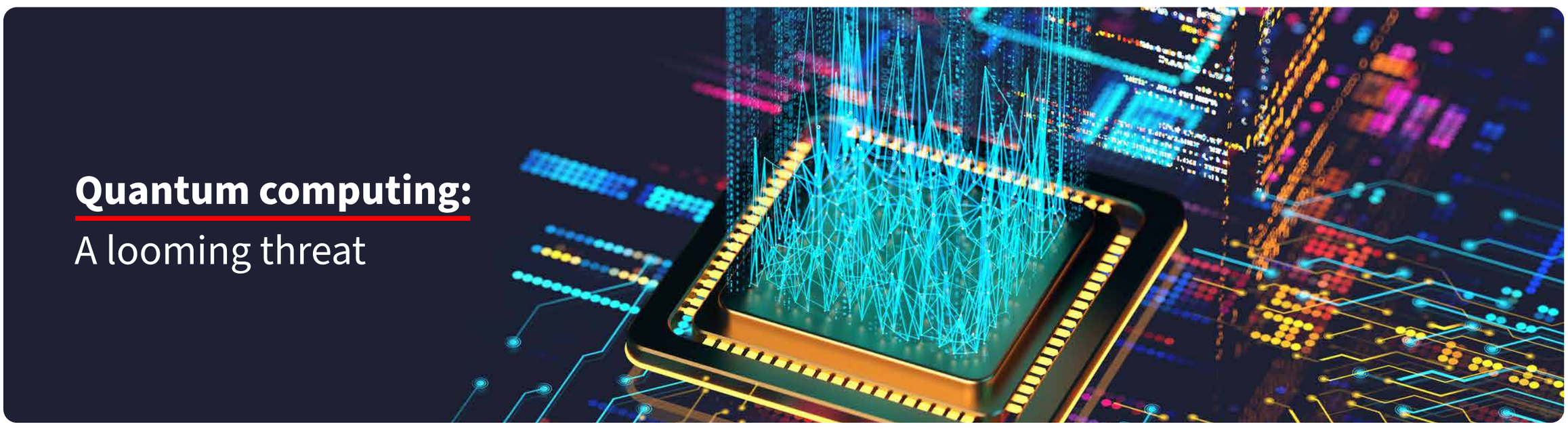
THE BIG TRENDS SHAPING WEBSITE SECURITY

08

The economics of cybercrime:

Lower barriers, higher risks

The barrier to entry for cybercrime is falling. Malware kits, AI tools and exploit packages are now widely available at low or no cost. This democratization of malicious tools means , cybercrime is increasingly attainable and SMBs face attacks not only from sophisticated cybercriminal organizations but also from amateur threat actors who can quickly deploy highly effective attacks. Consequently, the threat landscape is no longer dominated exclusively by professional cybercriminal networks. SMBs must therefore adopt broader cybersecurity awareness and implement layered defenses to remain resilient in this increasingly crowded and dangerous environment.



Quantum computing:

A looming threat

While still emerging, quantum computing presents potential future threats, primarily through the weakening of encryption standards that SMBs currently rely on to secure communications. Although direct threats from quantum computing remain limited as of late 2024, its future implications warrant careful monitoring by businesses that prioritize secure transactions and data privacy.

THREAT VOLUME & BOT ACTIVITY

09

On average, SMB websites faced 568 attacks per day in 2024

In 2024, SiteLock monitored an average of **567 million threats blocked per month** across its network of protected websites. While this figure reflects a **23% decrease from the 723 million/month reported in 2022**, the drop is not evidence of a safer landscape- it's the result of a shift in how threats are tracked and reported.

The updated reporting methodology was driven by key data pipeline changes:

- Removal of blacklist data following access restrictions introduced by Google's updated SafeBrowsing API.
- Recalibration of the Web Application Firewall (WAF) reporting to exclude low confidence "bad request" data and bot anomalies.

In effect, this reset the baseline narrowing the dataset to include only high-confidence, actionable threats. Threat reporting now reflects fewer false positives and cleaner telemetry, surfacing the most relevant signals tied to:

Verified exploit attempts | Unauthorized script injections | Suspicious shell activity

When the 2022 figure is recalculated using this updated methodology, it adjusts from 723 million to approximately 512 million threats blocked per month. By that comparison, the 567 million/month recorded in 2024 actually represents an 11% increase reinforcing that the threat landscape is not receding but intensifying.

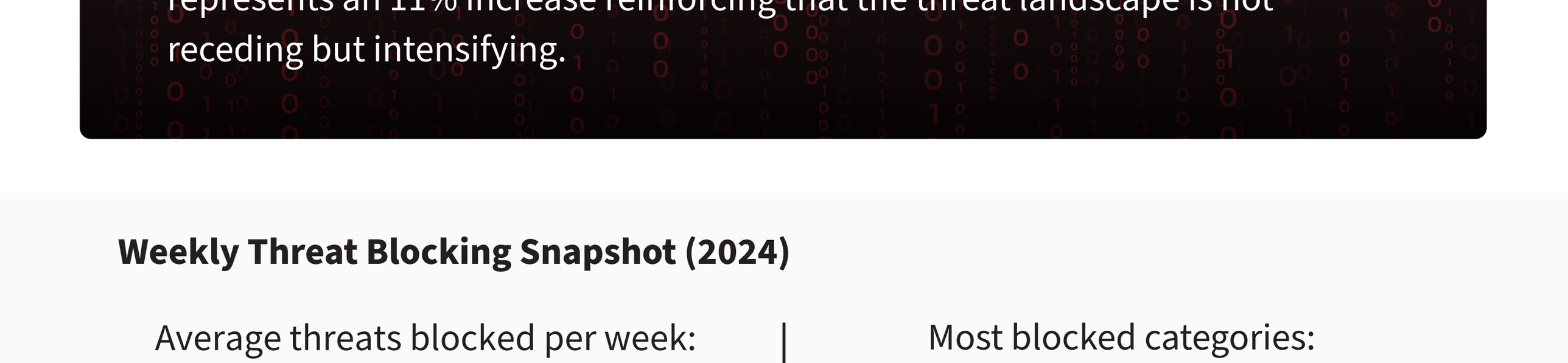
Weekly Threat Blocking Snapshot (2024)

Average threats blocked per week:

~131M

Most blocked categories:

Exploits | **Injections** | **Shell Scripts**



Key Takeaway:

Threat volume appeared lower in 2024, but that's due to improved reporting precision not diminished danger. Once adjusted, the threat volume remains critically high, underscoring the scale and persistence of attacks SMBs face daily.

Bot traffic trends: A surge that can't be ignored

Bot activity continued to dominate web traffic in 2024 with **websites receiving 12.6 times more bot visits than human traffic, up from 9.9x in 2023 -a 27% year-over-year increase.** This persistent rise makes bot activity as one of the most significant and often least visible threats facing SMB websites today.

Weekly snapshot of bot activity

Average bot visits per site:

4,914

Year-over-year growth:

15%

Bots & Risk: A Dangerous Correlation

While not all bot activity is malicious, the vast majority of elevated traffic on compromised or high-risk websites originated from known exploit frameworks and reconnaissance tools. These automated programs are designed to identify soft spots such as outdated software, exposed login panels and other common misconfigurations, making them a persistent threat vector for SMBs

Website Risks Amplified by Bot Behavior

Sites with high-risk scores are 62 times more likely to be infected than low-risk ones, often due to intensive targeting by malicious bots - illustrating how these bots don't just probe for vulnerabilities but actively seek out and exploit the easiest targets. Even after remediation, they often resurface to reinfect, turning minor gaps into long-term security liabilities for SMBs.

Why bot traffic matters for SMBs

- Scan for vulnerabilities in CMS platforms, plugins and themes
- Launch brute-force login and credential stuffing attacks
- Deliver malware payloads or trigger redirect scripts
- Scrape site content and degrade performance - hurting both SEO and user experience

This bot-led reconnaissance precedes most malware infections and for many SMBs, the visible compromise is just the final step in a long chain of automated targeting.

Business impact of unchecked bot activity

The cost of ignoring bot activity goes beyond security:

- **Infrastructure strain:** Bots inflate server load, driving up hosting and bandwidth costs
- **Performance degradation:** Slower page loads, higher bounce rates and reduced conversions
- **Analytics distortion:** SMBs lose insight into real user behavior
- **Reputation risk:** Spam redirects and SEO manipulation erode trust and visibility
- **Increased exposure:** Bots resurface after remediation, targeting lingering vulnerabilities
- **SEO penalties**

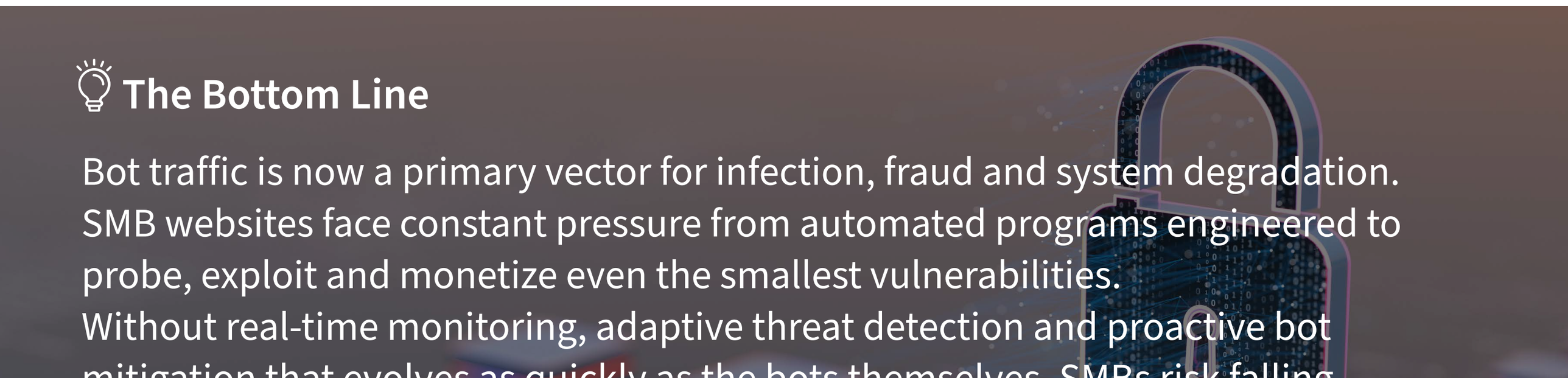
Malicious Automation Is Evolving

Although some bots are benign (e.g. search engine crawlers), the rise of AI-driven bots used for credential stuffing, form spam, scraping and exploitation has placed even basic web infrastructure under constant pressure.

Modern bots now:

- Mimic human behavior (scrolling, clicking, form fills)
- Bypass traditional defenses like CAPTCHA and IP rate-limiting
- Adapt on the fly, mutating attack methods in real time

This makes traditional security tools and filters insufficient- Static blacklists and basic filtering simply can’t keep pace with bots trained on real-world interaction patterns. Websites that fail to implement bot filtering, rate-limiting, or proactive scanning are more likely to experience repeated infections and data leakage over time.



The Bottom Line

Bot traffic is now a primary vector for infection, fraud and system degradation. SMB websites face constant pressure from automated programs engineered to probe, exploit and monetize even the smallest vulnerabilities.
Without real-time monitoring, adaptive threat detection and proactive bot mitigation that evolves as quickly as the bots themselves, SMBs risk falling victim to automated attacks - long before a single malware file is deployed.

Understanding Risk Tiers: Why Vulnerable Sites Get Hit Harder

Malicious bots don’t just inflate traffic - they amplify risk. In 2024, SiteLock’s telemetry showed a strong correlation between risk level and infection likelihood:

Risk-Level Breakdown (2024)

Risk Tier	YoY Infection Change	Relative Infection Likelihood
Low risk	**-41%**	**Baseline (1x)**
Medium risk	**-24%**	**Moderate**
High risk	**-39%**	**62x higher than low-risk**

What it Means:

Despite lower infection volumes across all tiers, **the relative risk for high-risk websites actually increased. A site deemed high-risk in 2024 was 62 times more likely to suffer an infection than a low-risk site** - a **3% rise** from 2023.

This points to two parallel trends:

- **Improved hygiene is reducing infections overall**, likely driven by better patching habits, CMS/plugin updates and more widespread use of website security tools.
- **Smarter targeting by attackers, focusing more aggressively on vulnerable targets.** The fact that high-risk sites are even more likely to be infected even as their absolute infection rates fall indicates that cybercriminals are becoming more deliberate and efficient, concentrating their efforts where defenses are weakest. Thus, even modest lapses in maintenance or configuration result in exponentially higher exposure.

Key Takeaway:

Risk reduction isn't just preventative- it’s protective at scale and investing in regular security assessments and remediation directly shrinks the attack surface. Proactive maintenance, CMS/plugin updates and regular vulnerability scans dramatically reduce the chances of attack regardless of traffic volume.

Infection rates & risk-level impact

In 2024, SiteLock observed persistent high malware activity across SMB websites.

Weekly Snapshot of Infection Activity

Infected sites per week (avg):	Infected files per week (avg):	Files cleaned per week (avg):
16,358	**1.7M**	**1.7M**
(+5% YoY)	*(+2% YoY)*	*(+5% YoY)*

These steady volumes reflect sustained exposure to vulnerabilities. Even as general awareness and hygiene practices improve, the data reinforces the importance of continuous monitoring and automated remediation to protect website integrity and prevent recurring compromise.

Dominant malware families observed in 2024

SiteLock identified a set of recurring malware families that shaped the threat landscape for SMBs in 2024. These families differ in structure and intent- ranging from control-enabling tools like backdoors and shell scripts to monetization-focused payloads such as redirect and spam injectors.

While each family carries unique capabilities, they were frequently deployed in combination, reflecting the **growing use of multi-stage, multi-function infections designed to maximize attacker foothold and operational flexibility**.

Top malware types detected

72% File Hacker

The most prevalent malware type in 2024, with an 8% year-over-year increase. Filehacker scripts are used to overwrite core site files or upload malicious executable scripts. Often the initial vector for broader infection, File Hacker payloads enable attackers to gain write access and deploy further malware.

49% Backdoors

Present in nearly half of all infected websites, up 7% from 2023. These stealth mechanisms provide persistent remote access even after cleanup or credential changes. Frequently embedded in plugin files or disguised as legitimate CMS components.

37% Eval Request Scripts

While still common, their prevalence declined slightly by 6% year-over-year. Lightweight, flexible payloads that execute external commands, fetch malicious content or inject spam redirects. Often nested inside plugin or theme files to avoid detection.

25% Shell Scripts

Server-level tools that grant attackers deep system control via command-line access. Frequently hidden inside image or configuration files and often deployed alongside backdoors and filehacker payloads.

19% Redirect Infections

Down 66% from 2023, though they remain a monetization vector. Used to silently redirect visitors to phishing sites, spam domains or malware-hosting URLs-commonly used in SEO spam campaigns.

17% FileManager

Web-based control panels used to upload, edit and delete files. Often disguised as legitimate admin tools.

12% Phishing Files 12% Defacements 5% SEO Spam

Secondary payloads that frequently coexist with higher-severity malware. While less common individually, their presence contributes to site reputation damage and regulatory risk.

Multi-Family Infections & Malware Severity: When One Threat Isn't the Whole Threat

Today's malware doesn't work alone. In 2024, SiteLock observed a sharp rise in infections involving multiple malware families operating in tandem, turning isolated compromises into layered, persistent attack chains.

Overlap is common: One Compromise, Many Payloads

Infections were rarely limited to a single malware type. **Compromised websites often hosted two or more distinct malware families simultaneously**, as attackers layered tactics to maximize damage, ensure persistence and maintain long-term control. This overlapping strategy is now a hallmark of modern website compromises - transforming what appears to be a single breach into an **evolving multi-stage threat** that is significantly harder to detect and eliminate.

Common malware combinations in 2024

Backdoors
Create persistent reinfection points that evade surface-level cleanups.

Redirects
Silently monetize traffic, damaging SEO and eroding customer trust.

Shell access and eval scripts
Dynamically download additional malware as needed providing attackers with pathways to escalate control over time.

Why attackers layer threats:

Multi-family infections are designed for endurance. By embedding multiple footholds, attackers increase dwell time and make cleanup significantly harder.
If even one component is missed, the infection can resurface days or weeks later restarting the attack cycle.

This layered approach gives attackers strategic flexibility:

They can shift payloads

Escalate privileges over time without needing to reinfiltrate the site.

Pivot monetization tactics

Websites lacking real-time monitoring or automated remediation are especially vulnerable to this type of recurring, shape-shifting attack as each missed trace becomes an open invitation for reinfection.

Key Takeaway:

Layered infections aren't just more destructive- they're also more durable. If even one piece is missed, attackers can return days or weeks later, restarting the infection chain.

Malware severity: Threat severity is no longer static

SiteLock classifies malware into four tiers based on behavior and business impact:

- **Low (Defacement):** Includes SEO spam, link injections and "Hacked by" messages that alter site appearance without further compromise.
- **Medium (Generic):** Common obfuscated scripts like JS-Generic, mailers, or cryptominers that execute malicious functions.
- **High (Visitor Attacks):** Redirects, phishing kits and downloaders targeting site visitors often monetized through traffic hijacking.
- **Critical (Command & Control):** The most dangerous tier, including shell scripts, filehackers, file managers and uploaders granting full and persistent attacker control over the website.

The Malware Severity Graph illustrates how infections can move across tiers - from minor nuisance to full compromise. A simple spam injection can escalate into a critical command-and-control breach over time without proper detection and remediation.

Threat Level	Threat type
Low (Defacement)	Comment SPAM, Link SPAM, Hacked By, SEO SPAM
Medium (Generic)	Cryptominer, Mailer, iFramer, JS-Generic
High (Visitor Attacks)	Injector, Phishing, Redirects, Download
Critical (Command and Control)	Filehackers, Shell Scripts, Uploaders, FileManagers

2024 Infection Landscape: Strategic Escalation, Not Just Volume

- Critical threats, despite being the least frequent by volume, still affected 30% of infected websites - an 86% increase in prevalence year-over-year
- High severity infections, which previously dominated, declined 45% in volume but still appeared in 62% of all infected sites, signaling continued risk to website visitors through redirect or phishing-type threats.
- **Medium severity threats became both the most widespread, seen in 73% of infected websites** - a 66% rise in volume and **a 202% jump in prevalence**.
- Low severity threats, surged as well now present in 66% of infections a 59% increase in volume and **a 189% rise in prevalence**.

What the data tells us

The drop in high-severity infections isn't a retreat- it's a recalibration. Attackers are no longer leading with obvious threats; they're escalating later, using stealthier malware to set the stage. Rather than launching attacks with high-severity payloads like phishing kits or redirect scripts, they're moving earlier in the kill chain: using stealthier, lower-severity malware to gain a foothold, maintain access and set the stage for escalation.

This shift explains several key patterns:

Critical infections
surged by 86%
signaling an uptick in deeper, more damaging compromises despite affecting fewer sites (30%) overall

High-severity malware still appeared in
62% of infections
but it's no longer the attacker's starting point - it's part of a larger, more layered sequence.

Medium and low-severity threats
exploded in prevalence
these threats are increasingly used as scaffolding: they embed quietly, evade detection and pave the way for full-scale takeovers.

Medium and low-severity threats
exploded in prevalence
laying the groundwork for deeper compromise

18

Key Takeaway:

Attackers are evolving their playbook. They're starting quiet and finishing loud, building layered infections that escalate over time. Modern infections rarely stop at the surface. Multi-stage and multi-family by design, they’re built to persist and escalate. That’s why even lower-tier infections can be the opening move in a much larger breach - making early detection and comprehensive remediation essential to stopping an attack before it spirals.

Why It Matters for SMBs

Malware infections have direct and long-lasting consequences and their impact goes far beyond cleanup:

- **SEO penalties** from spam links and blacklisting
- **Loss of trust** when customers encounter phishing, redirects or spam content
- **Revenue loss** from downtime, remediation costs and brand damage

And each reinfection compounds the cost - in dollars, downtime and customer confidence.

CMS RISKS & VULNERABILITIES

19

Content Management Systems (CMS) power millions of websites globally and provide the foundation for many SMBs to scale quickly. But they also represent some of the most exploited environments by attackers.
In 2024, CMS-based sites, especially those using **WordPress, Joomla and Drupal** continued to show significantly higher exposure to both vulnerabilities and infections compared to custom-coded (non-CMS) websites.

CMS vs. Non-CMS: Comparative Risk

SiteLock's 2024 analysis confirmed a sharp divide in risk levels.

CMS-powered websites continued to show significantly higher vulnerability exposure compared to custom-coded (non-CMS) sites:

WordPress and Joomla sites were 25% more likely to have vulnerabilities than non-CMS websites.

Drupal sites were 31% more likely to have vulnerabilities than non-CMS websites.

In contrast, **infection rates for non-CMS websites dropped 52% year-over-year**, reflecting stronger baselines or improved security practices among custom-coded websites.

This disparity carried over into infection rates as well.

Drupal sites were **3.88x more likely** to be infected (+77% YoY)

WordPress sites were **3.27x more likely** to be infected (+78% YoY)

Joomla sites were **1.80x more likely** to be infected (+65% YoY)

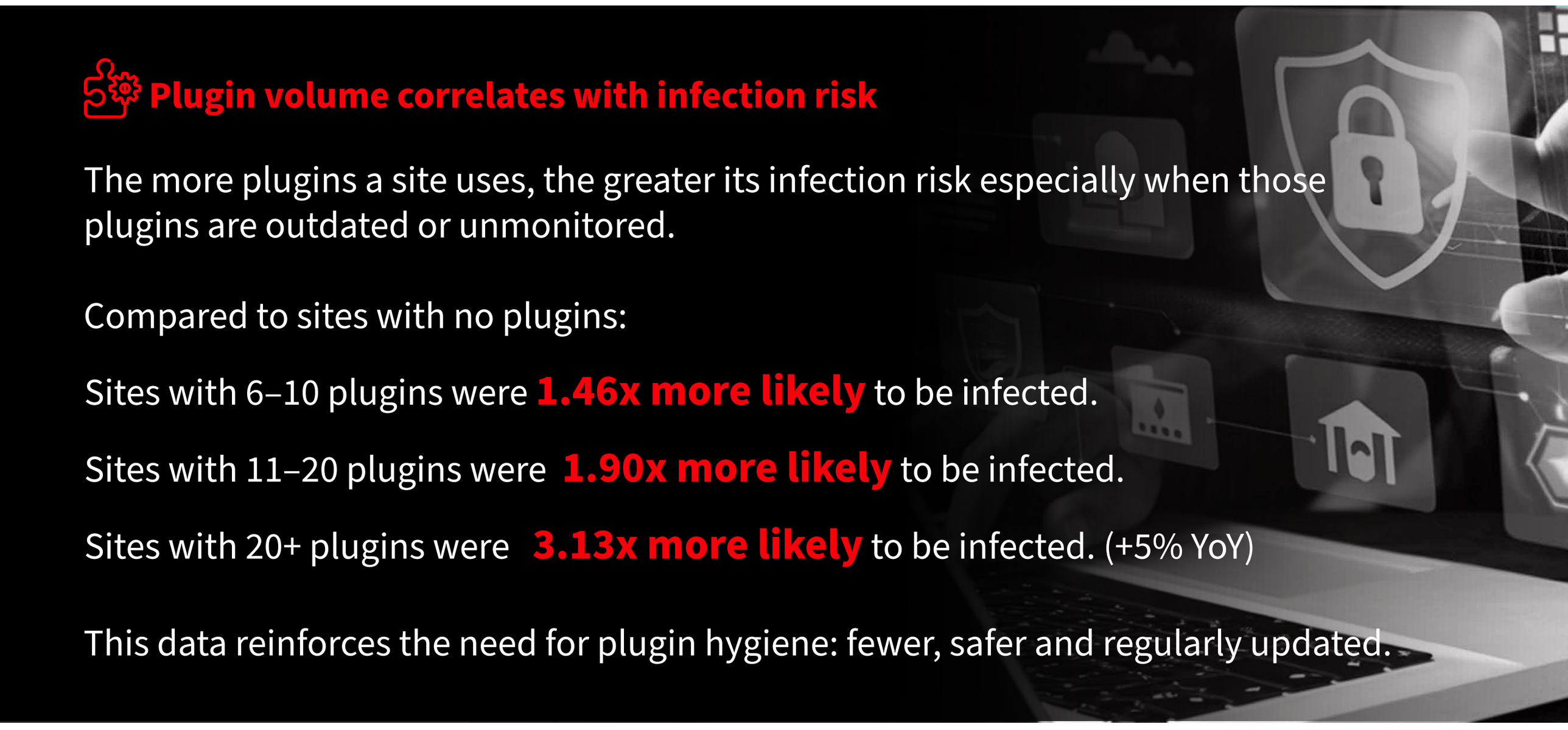
These trends highlight a troubling correlation: Popular CMS platforms offer flexibility and scalability but also introduce risk through complexity and third-party dependency.

The plugin problem: A recurring weakness

Much of this risk comes down to plugins - outdated or poorly maintained plugins remain one of the leading causes of CMS infections. While plugins enable rich functionality, they also represent a sprawling and often under-maintained attack surface.

Attackers commonly exploit:

- **Known vulnerabilities** in popular plugins and themes
- **Unpatched versions** of high-installation plugins with large user bases
- **Weak permission models** that allow hidden script injections



Plugin volume correlates with infection risk

The more plugins a site uses, the greater its infection risk especially when those plugins are outdated or unmonitored.

Compared to sites with no plugins:

Sites with 6–10 plugins were **1.46x more likely** to be infected.

Sites with 11–20 plugins were **1.90x more likely** to be infected.

Sites with 20+ plugins were **3.13x more likely** to be infected. (+5% YoY)

This data reinforces the need for plugin hygiene: fewer, safer and regularly updated.

CMS platforms give SMBs speed and flexibility but if security hygiene doesn't keep pace with customization, that flexibility can spiral into exposure.

Notable Plugin Exploits in 2024

Plugin	Vulnerability Type	Impact
Elementor ≤ v3.18.1	Remote code execution via unrestricted file uploads	Widely exploited
Yoast SEO ≤ v21.0	Stored XSS impacting 13M+ sites	SEO injection risk
UpdraftPlus ≤ v1.23.3	CSRF leading to XSS	Admin compromise

These examples underscore how a single unpatched plugin can expose millions of websites to full compromise.

The CMS risk formula: scale × complexity

Unlike custom sites, CMS environments are built on large ecosystems of modular components -core software, plugins, themes -many of which are managed by different authors. This complexity makes it harder for website owners to:

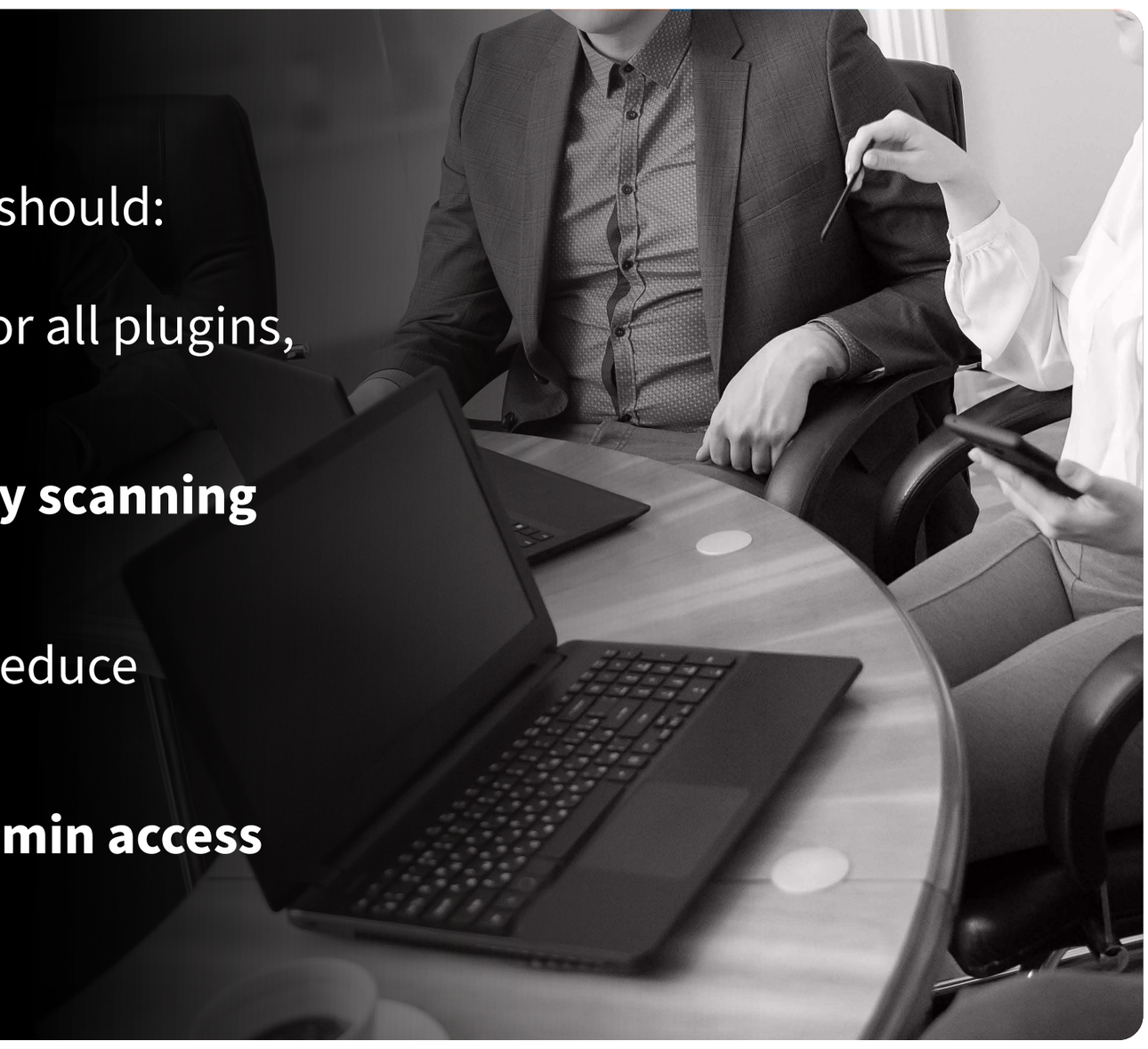
- Keep every component consistently updated
- Validate the security of third-party code
- Detect obfuscated or hidden malware in core directories

Even well-maintained sites can fall victim if any part of the stack becomes vulnerable - amplifying the risk for SMBs with limited IT resources.

What SMBs Should Do

To reduce CMS-specific risks, SMBs should:

- **Prioritize regular updates** for all plugins, themes and CMS cores
- **Use automated vulnerability scanning** to flag outdated components
- **Remove unused plugins** to reduce exposure
- Monitor for **unauthorized admin access or suspicious file changes**



Platform Alerts: Keeping Customers Ahead of Threats

In 2024, SiteLock continued to enhance its platform alerting capabilities to keep customers better informed and equipped to act before threats escalate. These alerts served as early warning signals, enabling faster remediation and shorter risk windows.

Alert volume & SMB impact

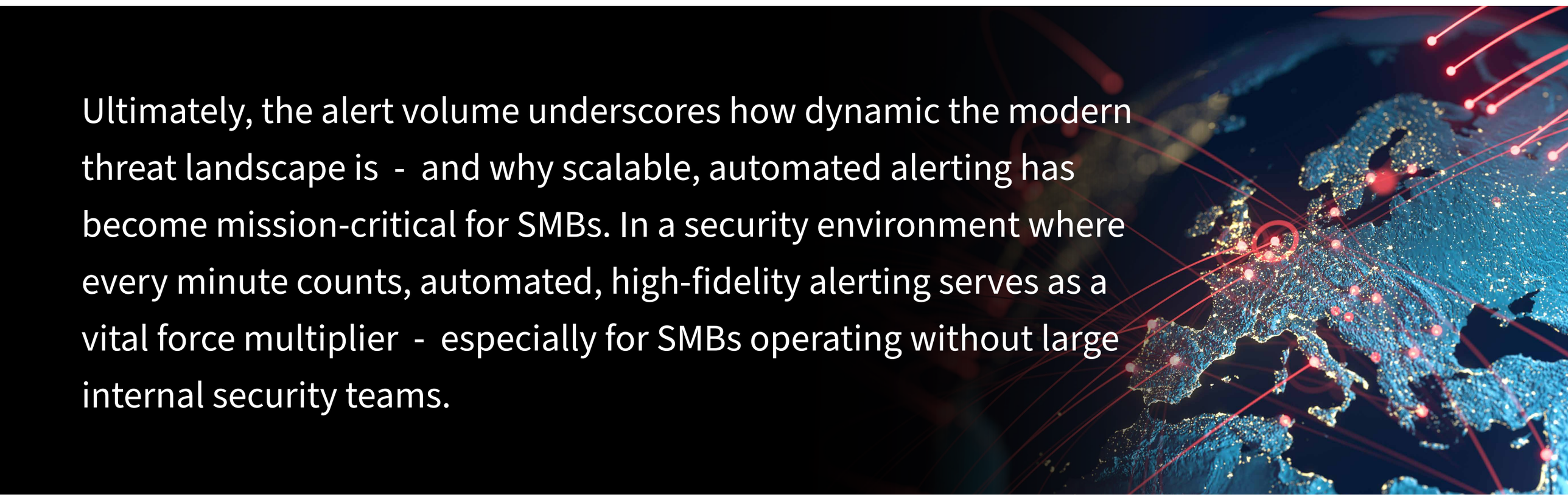
1.1M high and critical alerts were sent to customers in 2024 -marking **a 123% increase year-over-year**

SiteLock averaged **92,413 alerts per month**, providing website owners the timely intelligence needed to stay ahead of emerging threats

What the alerts data tells us

This surge in alerts reflects not just rising threat complexity, but also major gains in detection accuracy, telemetry speed and prioritization logic across the SiteLock platform. SMBs are now equipped with more precise, actionable intelligence that enables them to:

- Catch early signs of compromise
- Reduce threat “dwell time”
- Prioritize urgent remediation over lower-severity hygiene tasks
- Focus resources where they’ll have the greatest impact



Ultimately, the alert volume underscores how dynamic the modern threat landscape is - and why scalable, automated alerting has become mission-critical for SMBs. In a security environment where every minute counts, automated, high-fidelity alerting serves as a vital force multiplier - especially for SMBs operating without large internal security teams.

Platform Enhancements

To support faster and more effective responses, SiteLock introduced key alerting upgrades in 2024:

Expanded vulnerability database
with faster update cycles

Refined alert thresholds
to reduce noise and highlight what truly matters

Better prioritization logic
to surface critical issues faster

Streamlined interface
for reviewing, filtering and acting on alerts

These upgrades helped reduce alert fatigue while boosting the effectiveness of customer remediation workflows.

From reactive to proactive: The value of timely alerts

SiteLock's real-time alerting system is helping SMBs shift from reactive cleanup to proactive risk mitigation.

With timely, actionable insights, businesses can:

- Reduce the window of exposure before attackers strike
- Respond to vulnerabilities before they became entry points
- Patch high-risk plugins faster
- Strengthen site hygiene by addressing root causes
- Improve overall website hygiene

Cheap Tools, Expensive Consequences

Cybercrime has become disturbingly efficient. Today, attackers can launch high-impact campaigns using low-cost, widely available malware kits, AI tools and automated exploit frameworks - often with little technical skill. The return on investment for attackers is enormous: a successful phishing kit might cost just $50, but a single compromised SMB website can yield thousands in stolen data, SEO manipula, or ransomware payouts.

Meanwhile, the cost to victims is steep. For SMBs, each breach can mean thousands in downtime, cleanup and lost revenue - not to mention damage to customer trust and brand reputation. It's a high-stakes mismatch: while threat actors scale with automation and near-zero cost, SMBs face rising risk and limited security resources.

Attackers' High-ROI Business

Today's cybercriminals operate like high-margin startups - with low overhead and massive return-on-investment. A single vulnerable site can be monetized in multiple ways from data theft and redirect spam to cryptojacking and ransomware.

- Malware kits and exploit frameworks are widely available for $20–$100, often requiring no technical skill to deploy.
  - Infostealer-as-a-Service goes for as little as $12/month, allowing even low-skilled actors to siphon sensitive data at scale.
- Phishing kits and AI-powered spoofing tools can be deployed in minutes and can yield thousands per campaign.
- Ransomware groups like Conti have siphoned $80M+ from victims highlighting the scale and profitability of this underground economy.

Bottom line: Attackers face low barriers to entry and high returns - making cybercrime one of the most profitable and scalable illicit businesses in the world.

SMBs Pay the Price - Exponentially

For small and mid-sized businesses, the financial stakes are devastating. Unlike attackers, who can fail fast and cheap, SMBs face catastrophic consequences from even a single breach.

- The average cost of a website malware attack ranges from $5,000 to $20,000[1], depending on downtime and cleanup complexity.
- Breach response costs in 2024 ranged from $120,000 to $1.24 million per incident[2] - a staggering burden for most SMBs.
- 60% of SMBs go out of business within 6 months of a severe cyberattack[3].
- Each hour of downtime can cost hundreds - or even thousands - in lost revenue, especially for ecommerce businesses.

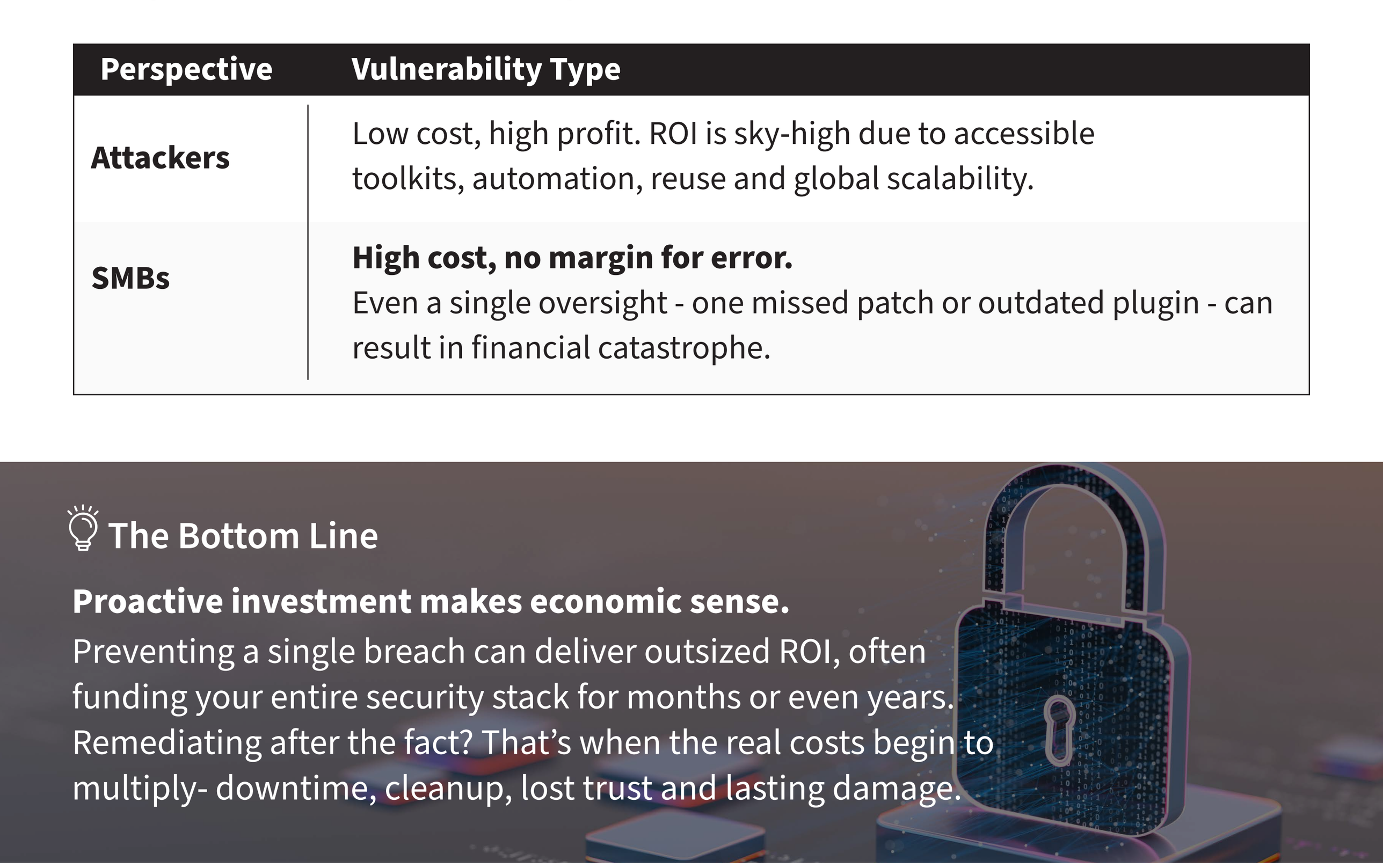
Globally, cybercrime is projected to soar to nearly $19.7 trillion by 2030[4] - that's more than the GDP of China and nearly twice the size of the U.S. economy - highlighting how cyber threats have become an economic superpower of their own.

The Economics Driving Escalation

Cybercrime is a numbers game and the odds are stacked against SMBs.
Attackers only need one weak link. Their playbook is built for scale: cheap toolkits, infinite reuse and global reach mean they can fail often and still profit wildly.
SMBs don't get that luxury.

They have to win every time - patch every plugin, monitor every alert, defend every endpoint - without enterprise-grade resources or round-the-clock teams. One slip, one delay, one missed update can cost them everything.
It's high-reward for attackers and high-risk for everyone else.

Perspective	Vulnerability Type
Attackers	Low cost, high profit. ROI is sky-high due to accessible toolkits, automation, reuse and global scalability.
SMBs	**High cost, no margin for error.** Even a single oversight - one missed patch or outdated plugin - can result in financial catastrophe.



The Bottom Line

Proactive investment makes economic sense.
Preventing a single breach can deliver outsized ROI, often funding your entire security stack for months or even years. Remediating after the fact? That's when the real costs begin to multiply- downtime, cleanup, lost trust and lasting damage.

[1]What is the Average Cost of Cyber Security Services? A Complete Price Guide, BinaryIT
[2]Verizon's 2024 Data Breach Investigations Report
[3]National Cybersecurity Institute
[4]Proxyrack Global Cybercrime Report 2025

AI, Automation & the Quantum Horizon

The threat landscape is evolving faster than ever. What was once considered advanced is now automated and attackers are now weaponizing intelligence at scale. For SMBs, this surge in automation and AI-driven tactics translates into higher risk - and fewer resources to keep up.

AI, Automation in the Attack Chain

Artificial intelligence is now a primary tool in the modern cybercriminal's arsenal. In 2024, SiteLock observed:

- **AI-generated phishing campaigns** that mimicked trusted sources with alarming realism - amplified by deepfakes and automated responses that simulate human interaction
- **Machine-learning- powered payloads** that adapt in real time, mutating and dynamically generating variants to bypass detection
- **Automated reconnaissance and credential stuffing** campaigns scaled to levels manual attackers could simply never achieve

According to third-party data:

AI-generated phishing attacks **increased by 30% in 2024,** with small businesses identified as the primary targets.

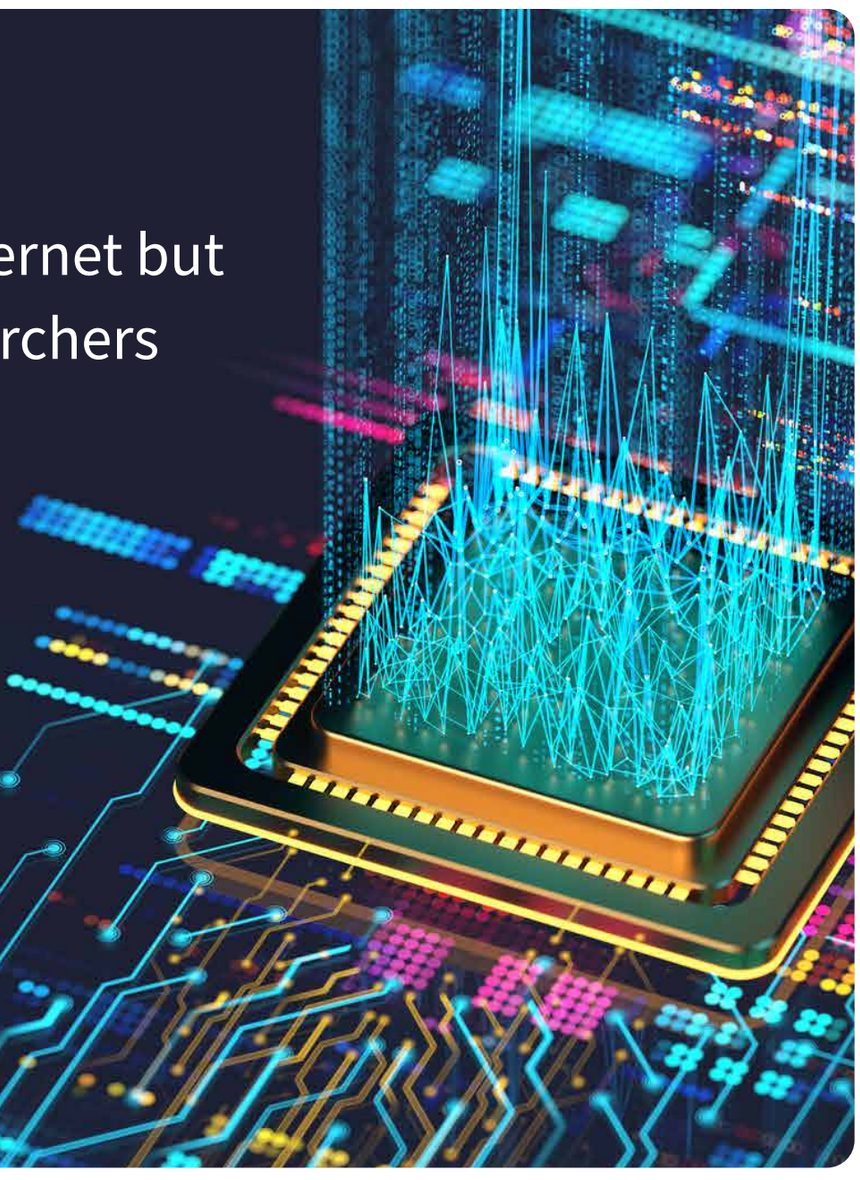
Adversarial AI and poisoned models are being actively used to mislead or exploit machine learning systems embedded in modern platforms.

The outcome? Faster infection cycles, broader reach and more convincing impersonation -putting trust and user behavior at the center of risk.

The Quantum Question

While quantum computing hasn't yet broken the internet but the clock is ticking. By late 2024, cybersecurity researchers began issuing early warnings:

- **Post-quantum risk is growing:** Encryption once considered unbreakable may become obsolete exposing stored data even if it's secure today.
- **SMBs reliant on standard encryption (HTTPS, TLS)** may need to prepare for post-quantum migration earlier than expected.



While not yet directly linked to malware campaigns:

Quantum breakthroughs already pose a long-term risk to data confidentiality.

Encryption-dependent protections from secure session handling to certificate-based access - could be undermined once practical quantum decryption becomes viable.

Think of quantum as climate change for security - slow-moving, but existential if ignored.

What This Means for SMBs

Malware infections have direct and long-lasting consequences and their impact goes far beyond cleanup:

- **Defensive lag is lethal:** Automation has outpaced manual defenses and if your response time is measured in hours or days, you're already behind.
- **Humans are now the soft spot:** AI-powered threats now don't just target systems - they impersonate people. Social engineering has become AI's playground: automated, scalable and disturbingly personal.
- **Readiness must be layered and proactive:** Behavioral analysis, automated response and zero-trust thinking aren't just buzzwords - they're survival tools.

Cyberattacks in 2024 weren’t just more frequent- they were more calculated. Malware is no longer just a blunt instrument; it’s part of an increasingly professionalized, automated business model. For threat actors, malware is a product. Infections are scalable. Compromise is just a delivery method.
Speed is now a critical advantage - attackers can identify and exploit vulnerabilities in hours, not days. Cybercrime has become industrialized, with threat actors operating in “as-a-service” ecosystems that mirror legitimate enterprises, complete with support, subscriptions, and performance guarantees.

For small businesses, this shift is especially dangerous. Every unpatched plugin, outdated CMS core, or delayed response becomes a high-stakes liability. SMBs are under siege from adversaries who not only wield cutting-edge AI tools, but also operate with the scale, coordination, and resources of large organizations -making defense disproportionately harder.
And when your website is your storefront -the face of your brand and the heart of your customer experience- a security failure doesn’t just disrupt operations. It undermines trust, and that’s far harder to recover.

Recommendations for SMBs

The future of cybercrime is fast, automated and constantly evolving. Small businesses don’t need enterprise budgets to build enterprise-grade defenses. What they do need is a smart, focused strategy that keeps up with how threats actually operate today.

Here’s how to shift from reacting to preventing:

Stay Ahead of AI-Powered Threats

- **Train your team** to spot AI-generated phishing emails, deepfakes and spoofed communication.
- **Establish authentication processes** to verify unusual or sensitive requests.

Stop Bots at the Door

- **Implement bot management** solutions that filter known malicious traffic.
- **Use behavioral detection** to catch evasive bots that mimic human actions.
- **Monitor** for repeated failed logins, scraping behavior and suspicious IPs.
- **Block or rate-limit** traffic from suspicious IPs or user agents.

FINAL THOUGHTS

29

Fortify Your CMS (Before It Becomes a Backdoor)

Update early, update often: Regularly update your CMS, plugins and themes-set reminders or use tools with auto-update.

Audit your stack: Remove unused or outdated components that expand your attack surface.

Verify plugin integrity before installing - popularity doesn't equal safety.

Use file change monitoring to catch silent infections early.

Build a Hygiene Habit

Use an automated website security solution to monitor continuously and stay protected.

Schedule regular scans to detect early indicators of compromise.

Enable real-time alerts and automated remediation. Threats today are multi-stage-if you wait, they growauto-update.

Don't overlook low-severity threats: These are often the opening move in a deeper compromise. Catching them early means avoiding a cascade.

Back up your content regularly: Because prevention is great, but recovery is critical.

Regularly review past alerts to spot recurring weak points.

Botom line:

Security isn't about locking everything down - it's about being prepared when (not if) someone tries the door. **The goal isn't perfection - it's persistence.**
Small, consistent actions can shrink your risk dramatically and protect your future.

SiteLock

A SECTIGO® COMPANY

GET IN TOUCH

sales@sitelock.com

(877) 846 6639

+1 (415) 390 2500 *(International)*