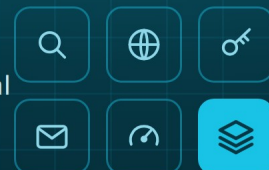


The Hidden Cost of a Fragmented Security Stack

Why SMB and mid-market organizations pay more, and see less, when external security is split across five tools.



EXECUTIVE SUMMARY

Most SMB and mid-market organizations don't buy external security as one thing. They buy it piece by piece: a vulnerability scanner, an attack surface management tool, a dark web monitoring service, an email health tool and a security rating. Each comes from a different vendor, with its own contract, its own console and its own renewal date.

We priced that stack using the cheapest published option in each category. **Even at that floor, it costs \$20,006 a year.** At the top of the market ranges, it reaches \$107,500. Neither number counts the time it takes to run five tools, or the penetration test that none of them delivers. This paper shows where the money and hours go, and makes the case for consolidating onto one platform.

5


tools, contracts, logins and renewals to cover one external attack surface

\$20,006


per year for those five tools, at the cheapest published prices we found

182


hours a year to log in, get oriented and keep the tools running

0


of those five tools deliver a penetration test

Meet Dana

Dana is the IT director at a 400-person precision parts manufacturer. Her team is two people. She owns everything from the ERP system to the plant-floor network to the laptops in sales. Security is part of her job, not all of it.

Her industry is under pressure. Manufacturing has been the most attacked industry for five years running, with 27.7% of all attacks IBM X-Force observed in 2025.¹ Exploiting a vulnerability is now the most common way into a breach, and it is the entry point in 38% of manufacturing breaches.² Her cyber insurer wants proof of external testing. Her biggest customer sends a security questionnaire every year. So over three budget cycles, Dana bought what each gap seemed to call for. Five tools later, this is her Monday.

Monday, 8:00 a.m. in Dana's office

ILLUSTRATIVE


8:00
Vulnerability scanner

Login + MFA. 212 open findings, ranked by CVSS score.


8:12
Attack surface tool

New login. Two new subdomains. Does the scanner see them?


8:21
Dark web monitor

Third password. 14 exposed employee credentials. Which still work?


8:30
Email health

DMARC failures from a sender nobody recognizes.


8:37
Security rating

Score down 6 points. The CEO will ask why.


8:45
Spreadsheet

Copy it all across to work out what overlaps.

8:45 a.m. Nothing fixed yet.

Five consoles, five severity scales, no shared view of the perimeter.

5

LOGINS

5

MFA PROMPTS

45

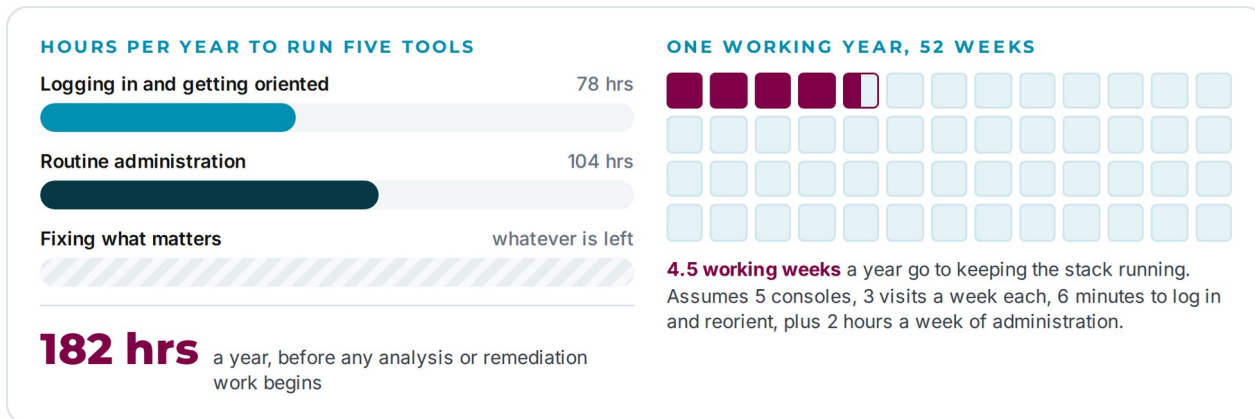
MINUTES

By 8:45, Dana has logged in five times, approved five MFA prompts and read five dashboards that each rank risk differently. The tools don't share an asset inventory, so she can't tell whether the new subdomains are the servers the scanner flagged, or whether the exposed passwords belong to accounts that still exist. She opens a spreadsheet to stitch it together. Nothing has been fixed.

The hours nobody budgets for

Research published in Harvard Business Review found that workers switch between applications nearly 1,200 times a day and spend just under four hours a week getting reoriented afterward, about 9% of their working year.³ Security consoles are a concentrated version of the same problem. Each has its own login, its own vocabulary and its own way of scoring risk.

We modeled Dana's week conservatively. Five consoles, three visits a week each, six minutes per visit to log in and get oriented: 78 hours a year. Add two hours a week of routine administration, such as licenses, scan schedules, false positives and reports, and the total reaches **182 hours, or four and a half working weeks a year**, before she analyzes or fixes anything. At a \$60,000 base salary that is about \$5,250 of time, and more once benefits are included.



What five tools cost, at the floor

To keep the numbers beyond dispute, we priced each category at the cheapest published option we could find for a real, paid product, not a typical deal.⁴ Those floor prices fit a small footprint: one scanner, up to 100 internet-facing assets, two email domains and fewer than 250 employee accounts. Larger organizations will pay more. The bars show the full market range from our research, and brand-name platforms in each category can push the total past \$100,000.



The costs that never appear on an invoice

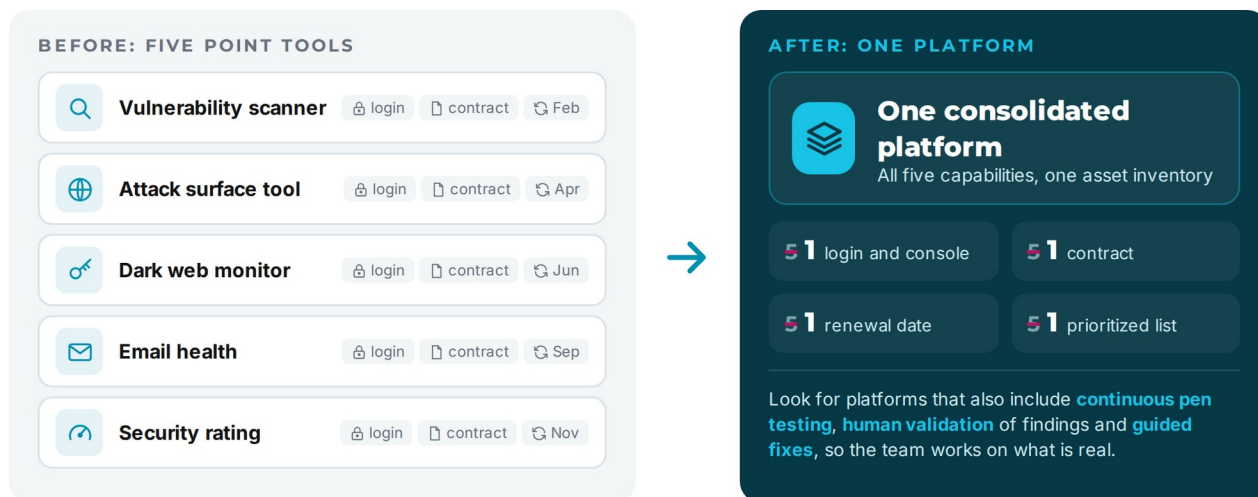
- **Five buying cycles.** Five security reviews, five negotiations and five renewal dates, each pulling attention from the work.
- **No shared picture.** Each tool sees a different version of the perimeter. Correlating them is manual, so it happens late or not at all.
- **Findings without proof.** Scanners report what might be vulnerable, not what an attacker can actually use. When teams can't separate real risk from noise, fixes stall. Only 26% of critical vulnerabilities were fully remediated in 2025, and the median time to fix rose to 43 days.²

- **Still no pen test.** None of the five tools produces a penetration test, which insurers, auditors and customers increasingly expect. A single annual external test typically adds \$5,000 to \$15,000.⁴

The case for consolidation

Consolidation isn't about fewer logos on an invoice. It is about one view of the perimeter, one list of what matters and more hours spent fixing. When you evaluate a consolidated platform, look for five things:

1. **All five capabilities in one console**, working from one asset inventory.
2. **Validation**, so findings are confirmed as exploitable before they reach your team.
3. **Penetration testing built in**, with a report auditors and insurers can use.
4. **Remediation guidance and retesting**, so fixes are confirmed, not assumed.
5. **Subscription terms with a low-risk exit.**



That is the model behind LUMA Perimeter. It combines external vulnerability scanning, attack surface management, dark web and credential monitoring, email health and security scoring with continuous external penetration testing and human validation, on one platform and one contract, at roughly the cost of one annual pen test. For Dana, Monday morning becomes **one login and one prioritized list of validated findings, with the fix attached**.

About Parabellyx

Parabellyx delivers enterprise-grade security testing, built for SMB and mid-market organizations. Founded in 2018 by offensive security experts and headquartered in Toronto, Canada and Denver, USA, we have delivered hundreds of security assessments. Our LUMA platform pairs automation with certified ethical hackers to test continuously: **LUMA Perimeter** for the external attack surface, **LUMA Internal** for the network inside, and **LUMA PTaaS** for on-demand, human-led penetration testing. We work directly and through channel partners across North America, the UK, the Caribbean and MENA. Learn more at parabellyx.com.

SOURCES AND METHODOLOGY

1. IBM X-Force Threat Intelligence Index 2026, as reported by Manufacturing Dive, Feb 26, 2026. 2. Verizon 2026 Data Breach Investigations Report, executive summary.
3. R. N. Murty, S. Dadlani and R. B. Das, "How Much Time and Energy Do We Waste Toggling Between Applications?", Harvard Business Review, Aug 2022 (137 users, three Fortune 500 companies).
4. Annual USD list prices checked Oct 2026: tenable.com/buy (Nessus Professional), halosecurity.com/start (EASM from \$399/month), dmarcian.com/pricing (Basic, billed annually), help.upguard.com (Breach Risk, 100 to 999 employees). SpyCloud from the Texas DIR government price list. Market ranges and pen test pricing from Parabellyx, The Cost of the Fragmented Security Stack, internal market research, Jul 2026.
- Time model is a Parabellyx estimate using the assumptions stated above, costed at base salary only. Dana and her Monday are illustrative.