Forrester Report Copy Prepared Exclusively For Christine Wan With Splunk Inc. Distribution and reproduction are prohibited.
For more information, see the Terms Of Use Policy and Ways To Share Research.

TRENDS REPORT

Understand The Benefits And Drawbacks Of Cybersecurity's Platform Push

Look, It's A Security Suite! No, It's A Security Portfolio! No, It's A Security Platform!

June 24, 2025

By Jeff Pollard, Jess Burn with Joseph Blankenship, Liam Holloway, Michael Belden

FORRESTER®

Summary

Security platforms grew, literally, out of the concurrent need for increased tech integration and reduced spend, creating a market of security titans amidst a still teeming pool of startups and standalone point solutions. But security platforms aren't created or defined equally. Security and risk professionals can use this report and Forrester's security platforms definition to draw distinctions between security vendors and their platform approaches and make decisions related to security tools and tech consolidation.

© 2025 Forrester Research, Inc. All trademarks are property of their respective owners.
For more information, see the Citation Policy, contact citations@forrester.com, or call +1 866-367-7378.

Forrester Report Copy Prepared Exclusively For Christine Wan With Splunk Inc. Distribution and reproduction are prohibited.
For more information, see the Terms Of Use Policy and Ways To Share Research.

Security Platforms Promise A Cure For Point Solution Ills

Over the last five years, security vendors across domains amassed a breadth of capabilities and expanded market share through M&A activity. They are now taking their body of offerings to market as security platforms, and the timing is right. Security leaders are feeling financial pressure from CFOs and boards and suffering chronic practitioner skill shortages, making security tech consolidation to platforms an appealing endeavor and a potential solution to solve problems like:

- **Too many vendors.** The cybersecurity tech and services market continues to grow with just over 4,000 vendors in this space as tracked by industry watchers and over $175 billion in projected revenue for 2025, not including governance, risk, and compliance (GRC) and privacy tools, according to our soon-to-be-released Forrester Cybersecurity Forecast, 2025 to 2028. The presence of multiple security vendors in an enterprise is often the end product of years of point solution purchases to solve the problem of the day, leading to redundancies in capabilities and cost. "As you go through and you see you've got all these different products, you realize I bought feature AB and C from one vendor and then CD and E from another, so I just double-paid for feature C," says a security leader at Palo Alto Networks.
- **Too many technologies.** Of the scores of vendors in the market, most have the same origin story: a founder with a technology and a dream. They do one thing well, get funding for it and a set of customers who value it, and then either get acquired, go public, or go under. But, facing budget and skill constraints, security leaders who once may have signed on as an early adopter of a technology from a startup may wait until that technology is added as a capability in a current vendor's platform. Of this approach, the CISO at a leading healthcare intelligence organization says, "Platforms are expanding into areas where I have specific tools. Let's take a look and see where our gaps are, where we have overlap, and can we get rid of one or two of them?"
- **Too much complexity.** Forrester's Security Survey, 2024, found that 23% of security decision-makers cited IT environment complexity as one of their biggest information security challenges in the next 12 months. With pledges of greater visibility and risk management for security leaders and greater operational efficiency for practitioners, platform providers go to market on reducing complexity and are gaining footholds in enterprises as boards and execs push for cost and tech consolidation. Karthikeyan Vaidyalingam, global head of cloud and AI security

© 2025 Forrester Research, Inc. All trademarks are property of their respective owners.
For more information, see the Citation Policy, contact citations@forrester.com, or call +1 866-367-7378.

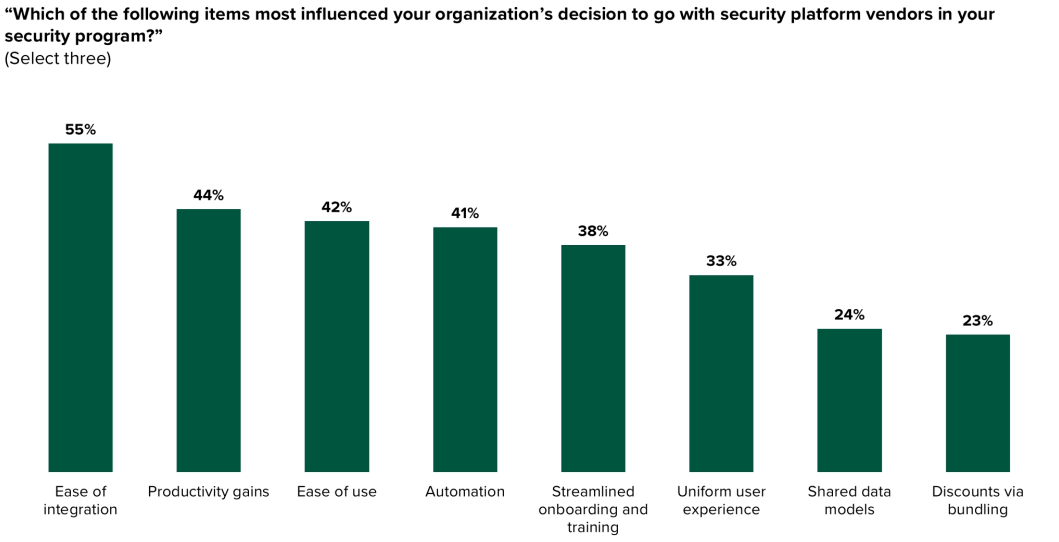
Forrester Report Copy Prepared Exclusively For Christine Wan With Splunk Inc. Distribution and reproduction are prohibited.
For more information, see the Terms Of Use Policy and Ways To Share Research.

at a leading global insurance and financial services company, echoes this sentiment: "Everyone is starting to rethink their security spend, so we are in the process of looking at how we can consolidate some of these tools, get rid of some of these tools, or replace capabilities wherever possible."

- **Too few integrations.** A plethora of point products that don't share data or telemetry means a corresponding number of logins and consoles and the potential for an exponential number of alerts, bogging down security practitioners and limiting visibility. When asked what potential benefits were most influential in their organization's decision to invest in a security platform, 55% of IT and technology decision-makers in Forrester's Q4 Tech Pulse Survey, 2024, cited ease of integration (see Figure 1). This tracks with MetLife's experience, according to Rashmita Das, principal cybersecurity architect for cyber platforms: "Individually, all these vendors that provide different technology could also be a platform. You can imagine how much integration is required between four vendors. If integrations don't exist, then I have to spend development time in custom-building those systems."

Figure 1

Organizations' Rationale For Implementing Security Platforms



Base: 150 IT/technology decision-makers
Source: Forrester's Q4 Tech Pulse Survey, 2024

© Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

© 2025 Forrester Research, Inc. All trademarks are property of their respective owners.
For more information, see the Citation Policy, contact citations@forrester.com, or call +1 866-367-7378.

Forrester Report Copy Prepared Exclusively For Christine Wan With Splunk Inc. Distribution and reproduction are prohibited.
For more information, see the Terms Of Use Policy and Ways To Share Research.

Set Realistic Security Platform Expectations

For security and risk pros, platforms will not disappear. In fact, we expect adoption of platforms to increase for no other reason than the inescapable nature of platform messaging from security vendors — which requires a definition of security platforms. Forrester defines security platforms as follows:

Security platforms combine multiple security controls from a single vendor in one unified user interface with a single underlying data model for all relevant data from each control. Security platforms enable outcomes including ease of deployment, use, and integration, resulting in productivity gains for users. Third-party integrations via marketplaces and extensions should enhance security platforms beyond the vendors' own products. In addition, platforms present financial advantages through the discounting and bundling of multiple security controls in one purchase.

Demand Deliberate Platform Design

CISOs have long heard about the mythical "single pane of glass" (SPOG) promised by vendors. The cyclical reemergence of "SPOG" has happened frequently enough that security teams could almost set a clock by it. But today's security platforms are much closer to making this promise a reality for the first time. While it's relatively easy to market a platform, it's hard to build one. Platforms must meet specific expectations to fulfill their promises. Security platforms must be:

- **Built with one user interface across all solutions.** Historically, if single sign-on and iframes existed across vendor UIs, the vendor counted that as a "single user interface." But today's platforms go well beyond that. These interfaces come to life from the beginning with a design paradigm that applies to any current — and future — platform features. This allows vendors to emphasize analyst experience (AX) for platform users. "That's where a platform adds value," says Das at MetLife, "when my analysts don't have to do the manual legwork and don't need to get out of the platform. Everything is in one place."
- **Developed for a single underlying data model.** Security leaders know all about collecting and storing security data. What they may not realize is that vendors also suffer from their own data model problems. Legacy products are built one way, innovation efforts are built another way, and technology acquisitions each treat the underlying data differently. This results in a hodge-podge of fields, values, categories, and transformations to make data usable from one product to another. In a true platform approach, vendors are tackling this problem with one extensible data model that is flexible enough to accommodate different data types without

© 2025 Forrester Research, Inc. All trademarks are property of their respective owners.
For more information, see the Citation Policy, contact citations@forrester.com, or call +1 866-367-7378.

Forrester Report Copy Prepared Exclusively For Christine Wan With Splunk Inc. Distribution and reproduction are prohibited.
For more information, see the Terms Of Use Policy and Ways To Share Research.

the Band-Aid fixes that were necessary in years past. Network, endpoint, application, cloud, and identity data all have different characteristics but remain usable across all pieces of the platform.

- **Designed to enable third-party integrations via marketplaces.** Make no mistake, a key goal for a platform vendor is to incent security leaders to buy as much as possible from the platform vendor. While this is true, platforms also need to work with third-party solutions to maximize their relevance — and value. Few, if any, environments are homogeneous, and many security leaders are loath to lock in with a single vendor for their entire security stack. "For the adoption of a platform, you have to be able to support the existing ecosystem and the current investments that customers have made," comments Kris Anderson, director of product management at Trend Micro. This "meet the customer where they are" approach is accomplished via marketplaces, where vendors can enable and upsell additional integrations to third-party products and services. This benefits customers with easy deployments and preprogrammed integrations of other tools.

Push For Specific Platform Payoffs

The benefits of security platforms — true security platforms, not just product suites — outweigh the risks for security leaders. Product suites are just collections of products or capabilities sold by the same vendor. They may have some points of integration (like reporting or common UI elements) but don't offer much more than the ability to buy multiple capabilities from a single vendor. Security leaders need to understand exactly what gains platforms should bring (see Figure 2). Product suites do not possess these characteristics, while platforms will:

- **Shift the integration burden to the platform provider.** The integration work of making multiple products talk to each other is done — behind the scenes by the platform provider, not by your team — when you buy a platform. There are no expensive consulting engagements to build middleware just to make a single vendor's products work with each other. This results in faster time to value, eases deployments, and removes visibility gaps between solutions. "As a security analyst, one of the most important things to make the right security decision is context," says a chief product and services officer at a global cybersecurity solutions provider. "If you don't have the right context, you may not make the right security decision. So if you're looking product by product by product by product, you missed some of that context. And that's where the platform adds value."
- **Simplify automation.** Creating automated workflows between solutions requires specific skills: knowledge of APIs, scripting and/or programming skills,

© 2025 Forrester Research, Inc. All trademarks are property of their respective owners.
For more information, see the Citation Policy, contact citations@forrester.com, or call +1 866-367-7378.

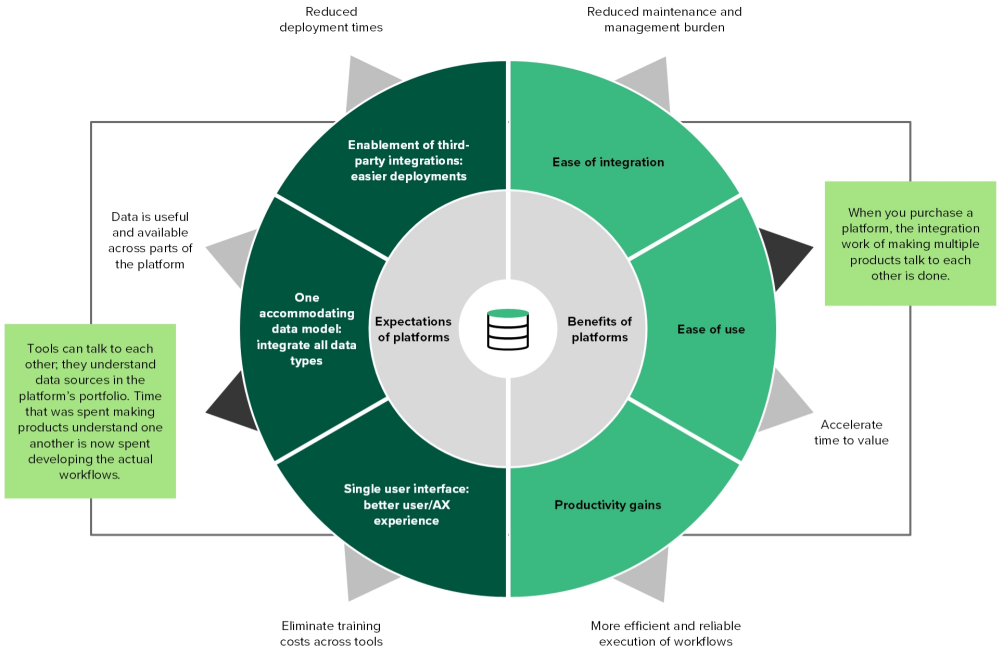
Forrester Report Copy Prepared Exclusively For Christine Wan With Splunk Inc. Distribution and reproduction are prohibited.
For more information, see the Terms Of Use Policy and Ways To Share Research.

documentation of the solutions, and (the least available of all) time to do the work. To be more effective and efficient, security teams should automate tasks and remove time-consuming, manual actions people perform often. Doing this with standalone, multivendor security tools may require the use of a third-party security orchestration, automation, and response (SOAR) solution to make the tools talk to each other. In a platform approach, automation is made easier because the tools already talk to one another and they understand data from other data sources in the platform provider's portfolio. Time that was spent making products understand each other is now spent developing actual workflows.

- **Deliver productivity gains.** The prior two gains ultimately result in an additional benefit: increased efficiency and throughput for security team members. This is the true all-encompassing result of a true platform. A true platform enables security teams to work faster, better, and more accurately. Vaidyalingam agrees: "We can build investigations much more efficiently, and the time it actually takes to identify the source of an attack path and also the different indicators of compromise and the indicators of lateral movement — we can actually get to that easier."

Figure 2

Expectations And Benefits Of Security Platforms



© Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

© 2025 Forrester Research, Inc. All trademarks are property of their respective owners.
For more information, see the Citation Policy, contact citations@forrester.com, or call +1 866-367-7378.

Forrester Report Copy Prepared Exclusively For Christine Wan With Splunk Inc. Distribution and reproduction are prohibited.
For more information, see the Terms Of Use Policy and Ways To Share Research.

Beware The Platform Siren Song, Lest You Wind Up On The Rocks

Platforms can deliver real benefits for security teams. Security leaders, however, should avoid rushing headlong into platform adoption, primarily because buzzwords exist in cybersecurity marketing and "platform" is one that security leaders hear often. Calling something a platform does not make it one, so when it lacks integrations, shared data models, and clear efficiency gains then you'll recognize it for what is: an opportunity to stamp your buzzword bingo card. Be aware that security vendors are developing platforms to entice investors just as much as customers, because this ensures consistent revenue growth through cross-sell within the vendor's own platform. Terms like average revenue per unit (ARPU) and statistics that showcase the quantity of customers with three, four, or more modules from a single provider are things investors seek out and reward handsomely. Security leaders evaluating security platforms should:

- **Keep one hand on their wallet when vendors come proselytizing for platforms.** Like carnival barkers, security vendors lure an unsuspecting public into their tent and let them leave only after squeezing a few more dollars from them (see Figure 3). As the vendor adds more tools, platform sales continue to grow. At face value, this is a positive thing for investors and customers: More people using more solutions indicates that those customers must be happy. For investors it shows that revenue will continue to go up and the vendor is successfully cross-selling. The head of cybersecurity services at a leading managed detection and response (MDR) provider adds, "I think that is largely led by industry: the normal parts of doing business — trying to create revenue, trying to create differentiation, trying to keep shareholders happy, trying to map to existing demands from clients." For security leaders, this comes with an important caveat: The entry-point price is the lowest amount you'll ever pay that vendor if you like the platform.
- **Anticipate that subtracting vendors does** not **equate to fewer tools.** Perhaps the most dangerous myth that propagates when discussing security platforms is that fewer vendors equal fewer tools. Platforms consolidate individual tools into a better, more useful package, but your net number of security tools and the expertise those tools require often remain the same. Your team still needs knowledge of endpoint, network, cloud, identity, and application security solutions regardless of how well bundled those products are. A CISO at a leading healthcare intelligence organization says: "There should be the same process within each module for getting information. It shouldn't be so different that the team has to

© 2025 Forrester Research, Inc. All trademarks are property of their respective owners.
For more information, see the Citation Policy, contact citations@forrester.com, or call +1 866-367-7378.

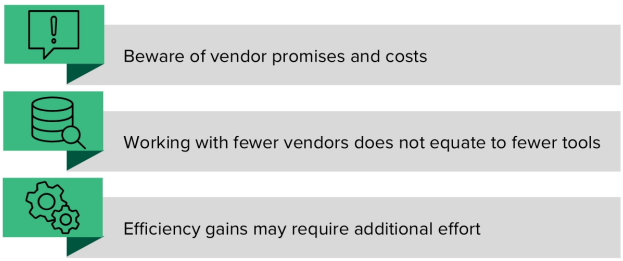
Forrester Report Copy Prepared Exclusively For Christine Wan With Splunk Inc. Distribution and reproduction are prohibited.
For more information, see the Terms Of Use Policy and Ways To Share Research.

relearn every time they go into something. Most security departments don't have the depth of skill sets for each individual tool. There have to be some synergies you're trying to create." Any agreement you sign must include onboarding, training, and support, as going with a single vendor does not make these items unnecessary.

- **Expect higher efficiency but not without putting in some additional effort.** Unless technology integrations, user interface issues, or data access gaps cause inefficiencies in your security processes today, it's unlikely security platforms will create efficiency gains for you. Bottlenecks related to poorly designed processes, missing automation, slow approval requirements, change control problems, and other internal blockers will still exist and platforms do not address any of those issues — nor do they solve cultural or political issues.
- **Uplevel your analysis to pick the right platform.** If you go all in with a platform and it turns out well, then your organization will reap rewards. When that happens, the vendor you select will continue investing in each component of the platform, expand more capabilities, and satisfy additional use cases. In the best cases, your platform partner will do that before you know you need them to. It's when that doesn't happen that things go wildly wrong. Extricating yourself from a single partner you rely on becomes expensive, time consuming, and, worst of all, politically problematic if you went out on a limb to select your current platform. Ensure your cybersecurity roadmap and your platform vendor's roadmap overlap in the right ways. Check out the vendor's history on mergers and acquisitions to provide insight into how future M&A might go. Keep tabs on the individual markets the platform encapsulates so that you can create a quick exit strategy if needed.

Figure 3

Three Reasons To Be Skeptical When Choosing A Security Platform



© Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

© 2025 Forrester Research, Inc. All trademarks are property of their respective owners.
For more information, see the Citation Policy, contact citations@forrester.com, or call +1 866-367-7378.

Forrester Report Copy Prepared Exclusively For Christine Wan With Splunk Inc. Distribution and reproduction are prohibited.
For more information, see the Terms Of Use Policy and Ways To Share Research.

Supplemental Material

Companies We Interviewed For This Report

We would like to thank the individuals from the following companies who generously gave their time during the research for this report.

A global cybersecurity solutions provider

A leading healthcare intelligence organization

A leading global insurance and financial services company

A leading MDR provider

MetLife

Palo Alto Networks

Trend Micro

© 2025 Forrester Research, Inc. All trademarks are property of their respective owners.
For more information, see the Citation Policy, contact citations@forrester.com, or call +1 866-367-7378.

Forrester Report Copy Prepared Exclusively For Christine Wan With Splunk Inc. Distribution and reproduction are prohibited.
For more information, see the Terms Of Use Policy and Ways To Share Research.

FORRESTER®

We help business and technology leaders use customer obsession to accelerate growth.

FORRESTER.COM

Obsessed With Customer Obsession

At Forrester, customer obsession is at the core of everything we do. We're on your side and by your side to help you become more customer obsessed.

Research

Accelerate your impact on the market with a proven path to growth.

- Customer and market dynamics
- Curated tools and frameworks
- Objective advice
- Hands-on guidance

Learn more.

Consulting

Implement modern strategies that align and empower teams.

- In-depth strategic projects
- Webinars, speeches, and workshops
- Custom content

Learn more.

Events

Develop fresh perspectives, draw inspiration from leaders, and network with peers.

- Thought leadership, frameworks, and models
- One-on-ones with peers and analysts
- In-person and virtual experiences

Learn more.

Contact Us

Contact Forrester at www.forrester.com/contactus. For information on hard-copy or electronic reprints, please contact your Account Team or reprints@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
Tel: +1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

© 2025 Forrester Research, Inc. All trademarks are property of their respective owners.
For more information, see the Citation Policy, contact citations@forrester.com, or call +1 866-367-7378.