SPONSORED BY

CHECK POINT™

What to Look for in a Consolidated Security Platform

The Pros and Cons: A Buyer's Guide

SC Media CRA | Business Intelligence

© 2024 CyberRisk Alliance

ebook
An SC Media publication

The pros and cons (a buyer's guide)

Protecting the modern organization shouldn't be done piecemeal. A consolidated security platform from a single vendor that incorporates network security, endpoint protection, cloud security, automated detection and response, threat intelligence, AI and zero trust provides a comprehensive, harmonious solution to security needs. ***Paul Wagenseil*** *explains what to look for and how to connect with the right platform.*

OUR EXPERTS:

Aviv Abramovich
Head of Security Services Product Management, Check Point

Dave Gronner
Product Marketing Manager, Check Point

John McClure
CISO & SVP, Enterprise Infrastructure & Cloud, Sinclair Inc.

Carl Lee
Information Security Manager - Cyber Defense Ops at APi Group

Cybersecurity has become far too complicated for most organizations to manage efficiently by using dozens of intertwined vendor solutions. The proliferation of environments, platforms and tools makes it costly and difficult for security staffers to manage different interfaces and separate true threats from alert noise.

Organizations can solve this problem by consolidating their tools and vendors into an umbrella platform that lets them manage cybersecurity across all their assets from a single interface. Such consolidated security platforms streamline operations, dampen alert overload, reduce costs, and let organizations more securely protect their networks, endpoints, mobile devices, and cloud instances.

"If it's from a single vendor, then you're actually improving your efficiency, because there are a lot fewer skills that you need in your security team to manage all these different [tools]," says Aviv Abramovich, Head of Security Services Product Management at Check Point.

Information overload

In past years, an organization's cybersecurity would need to protect the on-premises network and endpoints, and maybe an off-site backup or data center. Different tools handled different aspects of cybersecurity, but you could comfortably manage them all because you'd probably have no more than six or eight tools in total.

Today, cybersecurity looks completely different. Many or most of your employees are working from home. Assets run on third-party clouds and in-house applications are delivered from the cloud.

© 2024 CyberRisk Alliance

User identity has replaced the network perimeter as the first line of defense. Privately owned laptops and smartphones constantly join your in-house wireless network, while company-owned devices must be protected as users take them home or on the road.

Protecting your company, your resources, your properties and your users is no longer a simple affair. As Dave Gronner, Product Marketing Manager at Check Point, puts it, "You're solving a problem that's 10 times more complicated than you were trying to solve only a few years ago."

Tool overload

With these changes in network topology and use cases, the number of cybersecurity tools has exploded.

- Your firewall can no longer secure only the building network. You need new firewalls to protect your web-based applications, cloud instances, and remote devices.
- Antivirus software has morphed into endpoint protection, and from there to extended detection and response (XDR) that patrols the entire network and automatically initiates mitigation when threats are detected.
- Flat files of usernames and passwords have grown into robust cloud-based identity and access management (IAM) systems that automatically verify, provision and deprovision staffers and machines.
- Automation is widespread, extending from anomaly detection to security orchestration and response (SOAR) systems that handle much of the mitigation.
- Cloud-native security tools have arisen to protect a vastly different networking environment: cloud access security brokers (CASBs), cloud web application firewalls (WAFs), cloud-native application protection platforms (CNAPPs), cloud security posture management (CSPM) and cloud workload protection platforms (CWPP).
- Remote-networking security models like secure access service edge (SASE) and security service edge (SSE) leverage the cloud with their firewall-as-a-service (FWaaS), zero-trust network access (ZTNA), secure web gateways (SWGs) and software-defined wide area networks (SD-WANs).
- Modern security teams must monitor numerous data feeds and alerts—threat intelligence, security incident and event management (SIEM), anomaly-detection and compliance-management tools, as well as firewalls.
- As a result, recruiting and managing the right staff of skilled security analysts and admins is much harder with a fragmented and mixed set of security systems to operate.

> *"If you don't see that whole end-to-end event, you're only dealing with the symptoms. If you have the visibility end-to-end, you have much better security."*
>
> — Aviv Abramovich | *Head of Security Services Product Management, Check Point*

Unpacking it all

It's no wonder that organizations use more security tools than they can handle, and that security teams may feel overwhelmed. An Oracle/KPMG survey of 750 organizations found that 78% of respondents reported using more than 50 discrete cybersecurity products, and 43% reported using more than 100.

Many of these tools come from different vendors. In general, the larger the company, the greater the number of cybersecurity vendors it has.

A Check Point survey found that "27% of companies of more than 5,000-10,000 employees used between 11 and 40 plus vendors, while 30% of companies with more than 10,000 employees used between 11 and 40 plus security vendors."

Ninety-eight percent of respondents said their companies used multiple consoles to manage security operations, while 79% called working with multiple security vendors a challenge.

Most importantly, "when asked what they believe would be the best approach for improving security in their organizations, 69% [of respondents] prioritized consolidating to fewer security vendors."

There's evidence that such a shift is already taking place. Gartner found in 2022 that 57% of 418 organizations surveyed were working with 10 or fewer cybersecurity vendors, especially regarding SASE and XDR.

Gartner found that improved risk posture, not cost, was the primary driver for vendor consolidation. Seventy-five percent of the organizations surveyed by Gartner wanted to consolidate their number of cybersecurity vendors.

Vendor consolidation: Benefits

There are clear security and cost advantages to be gained by reducing the number of vendors, including:

- A smaller set of APIs to interact with other services, including ticketing systems and orchestration and automation tools
- Tighter security integration overall
- More threat visibility across all domains
- Greater effectiveness of internal policies
- More consistent threat-intelligence distribution
- Fewer and more consistent updates and patches
- Reduced skill-set requirements for security staff
- Lower risk of misconfiguration and non-compliance
- Streamlined costs relating to tech support, staff training, and 24/7/365 managed services
- Fewer contracts or service agreements to manage
- More streamlined budgeting, making it easier to track overall spending and evaluate return on investment

© 2024 CyberRisk Alliance

> *"You can save a lot of money and increase your operational effectiveness by having fewer tools to work with."*
>
> — Carl Lee | *Information Security Manager - Cyber Defense Operations, APi Group*

Enter the consolidated security platform

One way to simplify your cybersecurity management and better secure your organization is to use an umbrella platform that unifies all or most of your tools and sources them from just a few vendors, or even a single vendor.

"If you can combine them down to a few different tools that work really well, it's easier to manage and I think there's cost savings in it," says Carl Lee, Information Security Manager - Cyber Defense Operations at APi Group. "You can save a lot of money and increase your operational effectiveness by having fewer tools to work with. From an automation standpoint, it's less pivoting that your analysts must do to find information."

Consolidated/Unified Security Platform

On-prem network

- Data center
- Enterprise core/ perimeter
- Manufacturing/industrial
- Remote users
- IoT, SD-WAN

Cloud

- Public & private cloud
- Network/workloads/ apps
- Code-to-cloud
- Firewall-as-a-service

Workspace

- End points
- Internet & corporate access
- Email & web
- SaaS apps
- Mobile devices

Security Operations, Unified Management & Services

- Extended Prevention & Response (XDR)
- Security Policy Management
- Real-time Threat Intelligence
- AI Copilot/Advisor tools
- 24/7/365 Managed SOC and Security Services

Industry Frameworks

- Zero Trust Security
- Cybersecurity Mesh
- Hybrid Mesh Firewall
- NIST (US)
- ENISA (Europe)

Consolidated security platform components: A checklist

Ideally, a consolidated security platform will include as many of the following components as possible:

- ☑ Advanced threat prevention against phishing, ransomware, and other forms of malware
- ☑ AI compute infrastructure protection
- ☑ Artificial intelligence or machine learning (AI/ML) to detect anomalies and attacks a human might miss
- ☑ AI "copilot" to assist with real-time administrative and operational tasks
- ☑ Automated and AI-based anomaly detection and response
- ☑ Centralized management for SecOps with security policy, threat analysis, visibility, detection/response
- ☑ Cloud protections, including a cloud access security broker (CASB), cloud security posture management (CSPM), and CNAPP (cloud native application protection platform)
- ☑ Compliance reporting and management
- ☑ Content disarm and reconstruction (CDR) to neutralize potential zero-day attacks
- ☑ Data-loss prevention (DLP)
- ☑ DNS protection
- ☑ DDoS protection
- ☑ Email security
- ☑ Endpoint protection
- ☑ Exposure management
- ☑ Extended detection and response (XDR) and managed offering (24/7/365)
- ☑ Firewall as a service (FWaaS)
- ☑ Generative AI application protection
- ☑ Global threat-intelligence feeds and automated real-time response
- ☑ HTTPS/TLS/SSL inspection (securing encrypted traffic)
- ☑ Industrial Control Systems / Operational Technology & SCADA infrastructure security
- ☑ Identity and access management (IAM)
- ☑ Intrusion detection/prevention systems (IDS/IPS)
- ☑ IoT and embedded device security
- ☑ Layer 1-7 security / deep packet inspection
- ☑ Mobile device security
- ☑ Multi-tenancy management for MSSPs and enterprises
- ☑ Network security covering on-premises, cloud, and remote resources and users, including data centers and branch offices
- ☑ Privileged access management (PAM)
- ☑ Point-to-point VPN
- ☑ Pre-Quantum Cryptography (PQC) to defend against quantum computer-based decryption
- ☑ Remote-access VPN with granular application-level controls for zero trust policies
- ☑ SaaS application protection, including for free "shadow SaaS" apps downloaded and used by employees
- ☑ Secure web gateway (SWG) and other components of secure access service edge (SASE) or security service edge (SSE) models
- ☑ Security incident and event management (SIEM) or security orchestration and automated response (SOAR) tools
- ☑ Security virtualization with a unified approach for physical firewalls and virtual systems
- ☑ System resilience including firewall clustering, load sharing, n+1 redundancy
- ☑ Unified firewall interface to protect all assets (aka hybrid-mesh firewall)
- ☑ Web and browser security / secure enterprise browser
- ☑ Zero-trust network access (ZTNA), whether as part of SASE/SSE or on its own

Knowing what you need most

A consolidated platform might not include all these tools, as different vendors have their own strengths and weaknesses. The platform vendor may integrate with third-party solutions to provide best-of-breed tools to their customers.

"There are companies that are very good at managing identities," says Check Point's Abramovich. "You would use them as an identity [provider]. And you would use, let's say, Check Point for network security. You probably want to use separate vendors for security and networking. Security needs to protect the network, and the network just wants to connect everywhere as best as it can."

The consolidated security platform should conform with the zero-trust security model. Zero trust assumes that a network has already been penetrated, challenges all network users to continuously verify themselves, monitors all user behavior and limits each user's access and privileges to only that necessary to perform their assigned tasks.

"A modern unified platform needs to be built around the zero-trust concept," Abramovich says. "Fewer privileges, always verify, continuous verification and awareness and visibility — if you don't have these specific capabilities, your platform will be missing some really important components and capabilities."

Of course, that depends on how far along the implementing organization is on its zero-trust journey. Many organizations still depend, wholly or partly, on the older perimeter-based model.

"I think we can definitely move you much further along with a zero-trust model if you want to implement it," Abramovich adds.

Three consolidated security platform essentials

To Abramovich, regardless of the specific tools a unified threat platform might have, the platform should deliver three essentials. The first is **protection**.

"You have to protect your physical networks, whether they're your perimeter networks or your physical data centers," he says.

"Then you have to protect your cloud infrastructure," he adds. "Every cloud has an orchestration system. Your security system needs to have integration with those tools [and] a unified platform can do that really well in a cloud system."

Protection needs to be enforced everywhere, not just in the cloud or in the on-prem network, but on mobile and remote devices as well, Abramovich says.

"Anywhere you can access data, anywhere you can send data to, anywhere you host data or save data, that's where you have to make sure that you have a way to reach or protect that particular asset," he adds.

The second is **visibility**.

"How do you see what's going on in your environment?" Abramovich asks. "You have to look at the whole story, what the user is doing on their laptop, how they logged in, how their laptop is secured, to how they accessed the data, what have they done with the data, what have they uploaded or downloaded, and where they sent it to."

If you can't monitor and manage that whole end-to-end event, you're only dealing with the symptoms, he adds. If you have visibility end-to-end, you have much better security.

The third aspect is **correlation of intelligence among the various tools**.

"At the end of the day, your security is only as effective as the intelligence that powers it," Abramovich says. "The better and more rich and more deep your intelligence is, the better your security decisions will be."

The quick correlation of intelligence among the different tools is a huge gain, he points out.

"If my network security sandboxes a file, and determines that the file is malicious, it needs to tell all the other domains whether they're endpoints or cloud," Abramovich says.

Such integration between different tools is one of the primary advantages of a consolidated-security approach, he adds — not just in terms of communication, but also staff skills and demands. If it takes 10 different vendors to do all these things, Abramovich says, your team must be really skillful with 10 different vendor solutions.

John McClure, CISO & SVP, Enterprise Infrastructure & Cloud at Sinclair, Inc., echoes that sentiment. Not only would a consolidated security platform reduce the number of contracts to manage and possibly boost buying power, but the reduction in training time, ability to find experienced personnel and the ease of future integration are all pluses.

"Being able to find somebody who's worked on a single platform is significantly easier in terms of talent," says McClure. "The talent piece is there, the integration piece is there, as well as the simplification in terms of use, and the less friction when I'm looking on to bring on additional pieces of the unified platform."

The artificial-intelligence angle

AI will play an increasingly important role in consolidated security platforms, Abramovich says, just as it will aid cybersecurity in general. Chief among the advantages of AI are pattern recognition and anomaly detection.

"AI will be more accurate to identify the things that are really malicious versus the one that might look like it or look just abnormal, but they're actually not malicious," Abramovich says.

But AI will also learn from what it detects and develop its own conclusions.

"What AI is doing is generating its own intelligence from the intelligence that already exists," he says. "The importance of using AI is to create more intelligence to help you do things better."

On a less analytical side, Check Point has also introduced what it calls Infinity Copilot, an AI-based assistant that can help security-operations teams and administrators understand where shadow policies or overlapping/conflicting policies may exist and propose remedies.

Copilot and similar AI assistants can provide guidance and suggestions for improvement, create proposed policies, plus troubleshoot issues for quick ticket resolution. AI assistants will also increase team productivity and relieve the daily stresses that staffers face, especially those associated with the unknowns of complex security policies.

"We are now also able to use AI not only for better threat prevention, but also for security administrative tasks," Abramovich says. "We have an AI assistant that you can ask to do all sorts of things. You can actually write to it in human language."

Downsides of using a single vendor

Of course, there may also be disadvantages in getting most of your security tools from a single source or just a few sources. The key is to determine what is best for your organization.

"There is a little bit of security defense-in-depth of having a diversified vendor stack, not having all of your eggs in one basket," says APi Group's Lee. "If you have an outage or have an issue, it can affect the whole organization."

To McClure, there's the danger of betting on the wrong company.

"This space moves quickly," he says. "You see acquisitions happen, and things you've really invested in heavily are no longer getting invested in the same way after an acquisition. Or you're seeing a company that's on a skyrocket trajectory, and all of a sudden, it looks like they're not going to get past a certain stage of maturation."

Like Abramovich, McClure points out that some companies have specific core competencies and will likely out-perform newer entrants to that space, even if the newcomers are large and well-funded.

"I don't think necessarily that a big company couldn't do it," he says, "but I just don't think their R&D and their intellectual property and the way that they've cut their teeth and really gained trust in the community is going to be there for all this stuff they try to add on later."

Lee says his organization tries to unify tools and vendors as much as possible.

"When we force diversity, it's because it's a unique offering," he says. "There's always pressure from a budget standpoint to say, 'Do we have an existing tool that can solve this?' before we go and look for something else that's unique."

This leads to the question of vendor lock-in. But to Abramovich, that's an unlikely scenario. He says Infinity, Check Point's own consolidated security platform, lets you plug in tools from other vendors if you'd prefer.

"Vendor lock-in happens when you don't have a good alternative," says Abramovich. "We don't expect that a customer will adopt everything from us, or that they have to adopt everything from Check Point in order to achieve better security."

"I don't force you to run Check Point on your endpoint or your cloud," he adds. "I recommend it. It's better if you do it — you'll have a better experience and better security as a result. But if you choose to use other vendors, we will work with them together in the same way."

Abramovich adds that it's not always realistic to expect the best-of-breed for every aspect of cybersecurity. Sometimes the advantages of smooth integration and proper management override those concerns, especially if the "second best" is more than good enough.

”"In most cases, " he says, "the reality is you're short on staff, you have budget constraints, you have timeline constraints, and you just need to be more efficient."

Or, as Lee puts it, "if it's 90% effective and you're able to cover that 10% through process or whatever else, is it worth the user pain and the disruption of the business and re-educating people and all these things to get that extra 10%? Probably not."

Checklist: How to shop for a consolidated security platform

Now that we've explored the anatomy and purpose of unified security platforms, here is a checklist to follow when it's time to determine what you need (or don't need) and how to zero in on the right vendor:

☑ Assess your assets, risks, and needs

Inventory all your assets, be they in data centers, on-prem, in the cloud, or remote. For each one, figure out the likelihood of compromise, and the potential impact of compromise. "I would start by baselining where is your security posture today," says Abramovich.

☑ Don't throw out what's working and might be repurposed

Maybe there's something that you've already paid for that's doing almost everything you need it to do. "If you have great endpoint security, don't change it," says Abramovich. "Don't replace it. Don't start there. Start where things need fixing."

☑ Create a wish list

Do you want a hybrid-mesh firewall to put all your on-prem, cloud and web-application firewalls, as well as a firewall-as-a-service, into a single interface? Do you want the platform to include an AI-powered administrative assistant?

"If you were looking at seven different vendors [you're using now] and you're thinking about going to one vendor," says Lee, "let's take all seven and in each of those categories, ask 'What are my key use cases? What are my requirements? What are my must-haves?'"

☑ Lay out a roadmap, and a budget, and set goals

using known performance indicators so that you can review everything a year or two down the road. "Have a plan on how you want to migrate — what controls, what KPIs you're going to measure," says Abramovich.

☑ Talk to vendors to see what they can offer you

Lee recommends asking for RFPs for each tool, and also to define your important requirements to make sure that you get at least 90% of what you need.

☑ Make a shortlist of vendors

and then find out how long each has been in business and what kind of product innovations it is planning. "I would make sure the company has been around for a little while," says McClure. "In the cyber world, that doesn't mean 20 years — maybe they're a five- or six-year-old company — but that they have some lasting power."

☑ Talk to other organizations

especially those in the same field as yours, to see what kind of experiences they've had using some of the solutions on your shortlist. "I want to know who's using it, I want to know what their experience has been, I want to know what they came from and what they went to, what were their use cases?" says Lee. "What did they do for an RFP, who did they evaluate against?"

Once you've determined your needs and found the right vendor, it's time to invest and deploy. To that end, **take advantage of professional vendor services** that can assist you in your migration.

"The benefit of using a partner or professional services is you're talking to teams and individuals that have already traveled the journey," says Abramovich. "They've done it before. They know what to do and what not to do."

CyberRisk Alliance (CRA) is a business intelligence company serving the high growth, rapidly evolving cybersecurity community with a diversified portfolio of services that inform, educate, build community, and inspire an efficient marketplace. Our trusted information leverages a unique network of journalists, analysts and influencers, policymakers, and practitioners. CRA's brands include SC Media, Security Weekly, ChannelE2E, MSSP Alert, InfoSec World, Identiverse, Cybersecurity Collaboration Forum, its research unit CRA Business Intelligence, the peer-to-peer CISO membership network, Cybersecurity Collaborative, the Official Cyber Security Summit, TECHEXPO Top Secret, and now LaunchTech Communications. To learn more, visit CyberRiskAlliance.com.

SPONSORED BY

Check Point Software Technologies is a global leader in cyber security solutions, dedicated to protecting corporate enterprises and governments worldwide. For over 30 years, our mission has been to secure the digital world for everyone, everywhere. From pioneering stateful firewalls to our AI-powered, cloud-delivered security solutions, we are committed to safeguarding organizations with an industry-leading 99.8% prevention rate. Through our Check Point Infinity Platform, we provide cutting-edge solutions to defend against the most sophisticated cyber attacks. Our portfolio includes Check Point Harmony to secure the workforce, CloudGuard to secure the cloud, and Quantum to secure the network.

MASTHEAD

EDITORIAL

SVP OF AUDIENCE CONTENT STRATEGY

Bill Brenner | bill.brenner@cyberriskalliance.com

SALES

CHIEF REVENUE OFFICER

Dave Kaye | dave.kaye@cyberriskalliance.com

DIRECTOR, STRATEGIC ACCOUNTS

Michele Guido | michele.guido@cyberriskalliance.com

© 2024 CyberRisk Alliance