CyberTalk.org

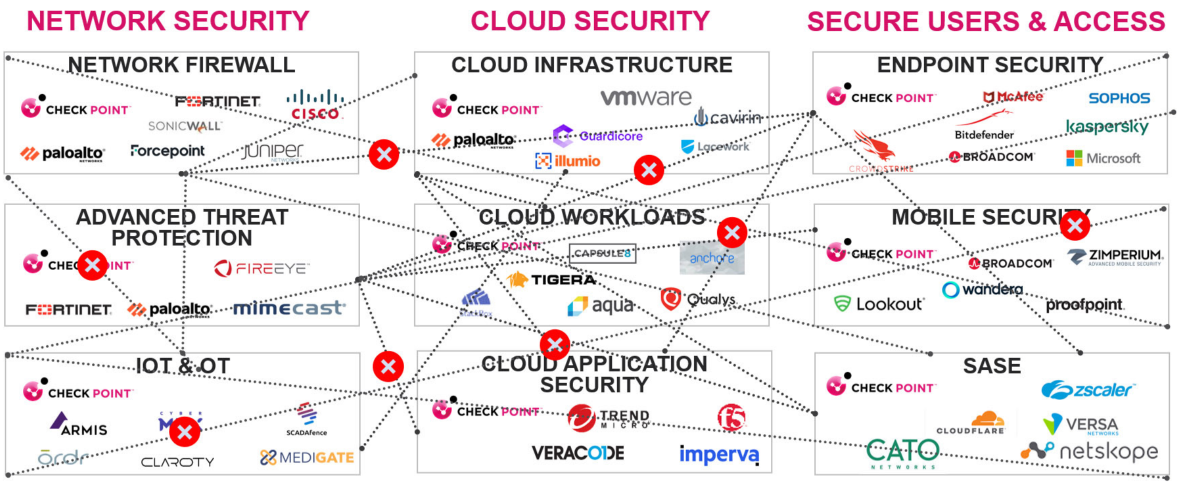
What CISOs Can Expect from a Consolidated Cyber Security Architecture

Multiple Headwinds: Complex Tool Sprawl, Lack of Integrated Stack, Malicious Cyberattacks, and a Worrisome Economic Outlook

As CISOs look forward to a new year, the role may become even more complicated. A perfect storm could await security leaders. The pandemic created legions of remote workforces. A threat landscape worsens with attackers leveraging previously unseen sophisticated cyberattacks. A shortage of skilled talent is estimated at 3.5 million open cyber security positions.[1] Despite a sixty-nine percent increase in cyber security spending from 2021 to 2022, an ESG study[2] says the budgets needed to protect organizations are insufficient. And with a skittish economy, the headwinds CISOs face are many and strong.

On the brighter side, security leaders say executives are paying more attention to cyber security. The frequent news cycle of one data breach after another is impossible to ignore. How much and where CISOs invest in their cyber security though, depends on many factors such as weighing the daily deluge of risks, projects, compliance and audit requirements, executive directives, large-scale projects slimmed down, staff expertise and capabilities, and more.

A Best of Breed Stack: What It Might Look Like



As a result, organizations have gravitated over the years to a patchwork of best-of-breed solutions. Organizations can have as few as a dozen solutions upwards of forty or fifty or more products from various vendors to address specific security requirements. An organization's users, resources, and data are everywhere. On-premises data center, the cloud, laptops, and IoT devices. The piecemeal sprawl comes with a major complication, the tools are either difficult or impossible to integrate. In a thread-bare budget, spending resources to stitch products together has been out of reach for many.

In this paper, we offer a viable option for the best-of-breed mindset, which is consolidated cyber security.

[1] "A New Approach is Needed to Close the Cybersecurity Talent Gap," by Rami Sass, Forbes, November 14, 2022

[2] "2022 cybersecurity spending trends: Where are organizations investing?" by Drew Robb, Infosec, September 7, 2022

Consolidated Cyber Security: An Integrated Stack Approach

Gartner has defined the Cybersecurity Mesh Architecture (CSMA) as a top strategic trend to help organizations move toward a more scalable and interoperable approach to security. CSMA aims at simplifying and improving corporate cybersecurity by providing a framework for discrete security solutions to collaborate on common goals.

Being able to consolidate and integrate your security technology stack via a single console used to be an illusion. However, today it has become a viable option for CISOs to consider. Here are the top-line benefits you can expect:

- A single console with all tools talk, share intelligence, and respond automatically to prevent all threats
- Far less repetitive administrative tasks that improve job satisfaction and staff morale
- Easier and faster incident forensics on all alerts, and not subsets
- Cost less to purchase, maintain, and renew. Stack costs are typically 20 percent less than the point product approach.
- Enhanced support is from one vendor rather than many, reducing the time and raising the thoroughness of incident investigations
- Development and testing are made easier to support with a limited number of tools
- Savings on training, and recruiting, plus easier to scale up, down, or migrate

> A recent 2022 survey by Gartner reports that 75 percent of organizations are pursuing security vendor consolidation, up from 29 percent in 2020.[3] Concerns about operational complexity and a need to strengthen risk mitigation are key drivers for change.

An ESG survey found that the top reasons to consolidate security vendors were to improve operational efficiencies (65%), gain tighter integration of security controls (60%), and improve threat detection (51%).

Check Point Infinity: A Consolidated Security Architecture

Organizational requirements are continually changing such as corporate applications and data shifting to the Cloud, initiating digital transformation projects, enabling significantly more remote workers, and adding new devices to the network every day. Protecting your organization from new, sophisticated cyberattacks has never been more challenging in respect to the diversity of business and technological changes.

[3] "Most organizations looking to consolidate security vendors in ^{2022}," by Steve Zurier, SC Media, September ^{13}, ^{2022}

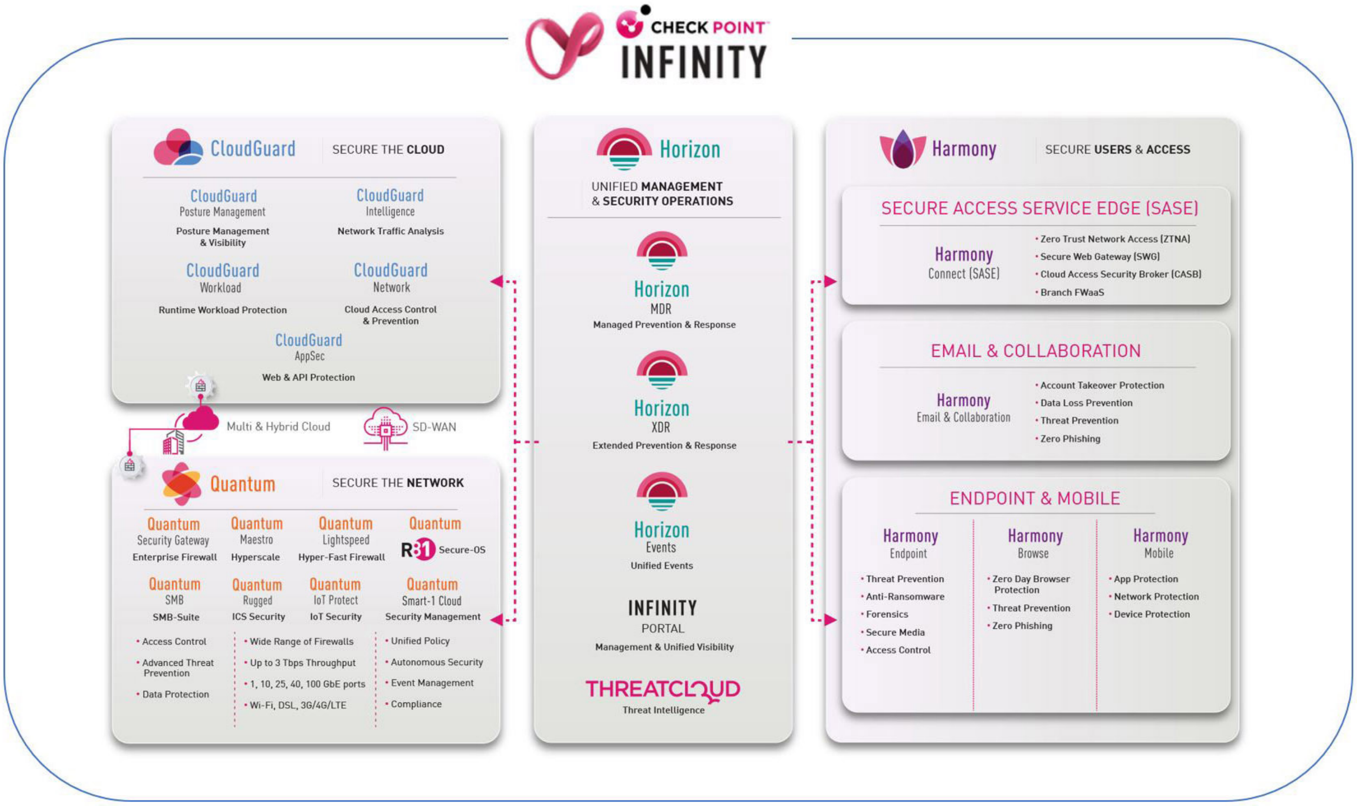
[4] "Top Strategic Technology Trends for 2022: Cybersecurity Mesh, by Felix Gaehtgens, et al, Gartner, October 18, 2021

Check Point Infinity is the first modern, consolidated, cyber security architecture built to prevent sophisticated Fifth Generation attacks across networks, cloud deployments, endpoints, mobile, and IoT devices. Infinity offers cyber security peace of mind as it enables organizations to solve security gaps, reduce risk, and lower the total cost of ownership. By focusing on threat prevention and leveraging globally shared intelligence on known and unknown cyberthreats, the Infinity Enterprise License Agreement (ELA) offers a complete, preventative, and efficient security solution for your entire landscape.

Here are the benefits you can receive with the Infinity ELA consolidated architecture:

- Most advanced real-time threat prevention against the latest generation of cyberattacks
- All inclusive: hardware, software, subscriptions, and 24x7 support
- Single procurement and predictable spend
- Real-time security updates via ThreatCloud
- Unified management from a single pane of glass

The graphic below is the layout of the Check Point Infinity cyber security architecture.



Learn more about how consolidation can move you from tactical to strategic security with improved protection and lower costs. Check out this Check Point Infinity page. Optionally, get a CISO perspective on consolidated security with this webinar, *Defining the Modern Cyber Security Architecture*.