WHY CYBER SECURITY CONSOLIDATION MATTERS

A Survey of IT Security Stakeholders

Introduction

The flow of news stories about the latest cyber-attacks is relentless. Criminals and hackers never seem to rest, and are always ready to take advantage of any situation to try and compromise organizations' defenses for their own ends. In the Spring of 2020 alone, we saw a 30% increase in cyber-attacks that seek to exploit concerns about the Covid-19 pandemic, and our latest Security Report showed how the attack landscape grew and diversified through 2019 across enterprise networks, cloud deployments, endpoints, mobile and IoT devices.

With every new attack or vulnerability, the red flags start to wave. The usual reaction is for organizations to review and consider ramping-up security with new products, with the assumption that these will help to better protect their networks and data. But will they? Or does adding more solutions from different vendors simply add more complexity, and potentially undermine security?

To better understand this problem, Check Point commissioned Dimensional Research to survey 400 global security leaders to capture hard data on their attitudes towards tool consolidation. The key findings of this research confirmed:

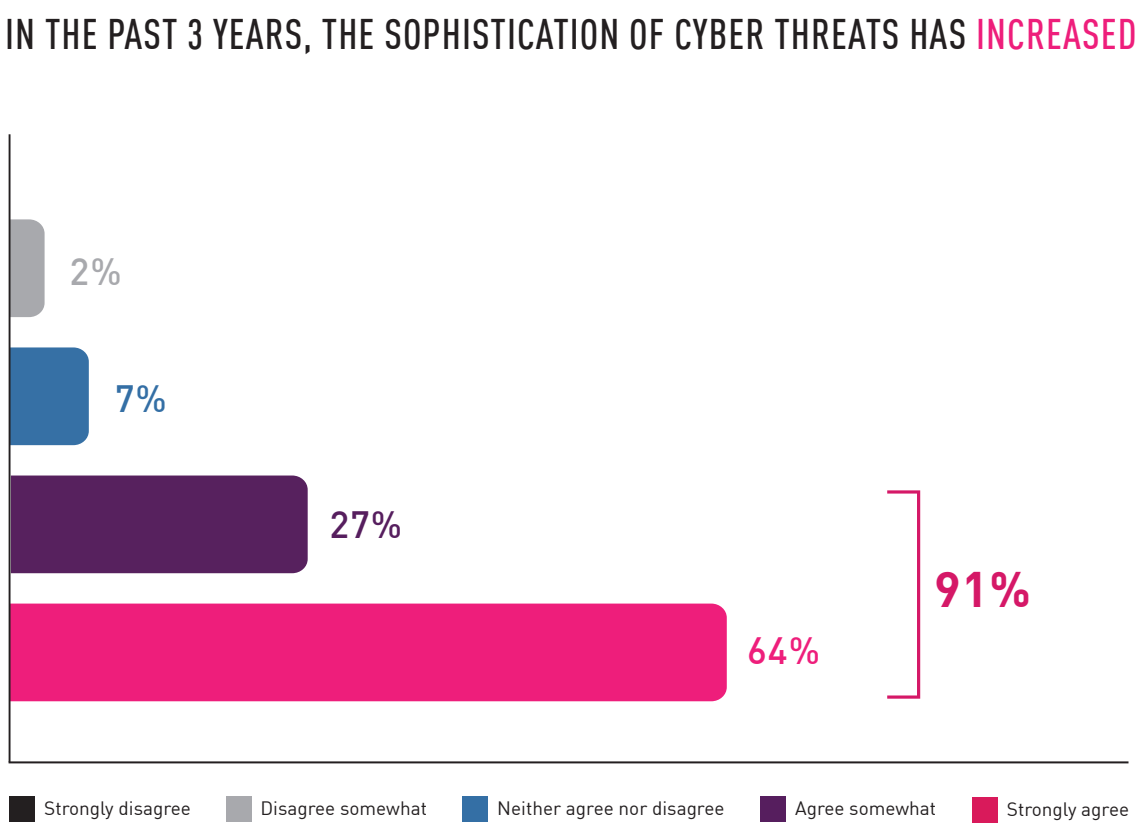
- **49%** of all organizations use between 6 and 40 point security products
- **27%** of larger organization use between 11 and 40 different vendors' products
- **98%** of organizations manage their security products with multiple consoles, creating visibility silos
- **79%** of security professionals say working with multiple vendors presents significant challenges
- **69%** agree that prioritizing vendor consolidation would lead to better security

"Does adding more products from different vendors simply add more complexity, and undermine security?"

The threat landscape is evolving… and getting worse

There isn't an attack surface that goes untouched. 27% of all organizations globally were impacted by cyber attacks involving mobile devices, according to Check Point Research. With 83% of enterprise workloads moving to the cloud, cyber criminals are increasingly attacking cloud providers. Check Point researchers have also seen ransomware attackers use a new, creative, double extortion tactic: prior to encrypting the victim's database the attackers extract large quantities of sensitive commercial information and threaten to publish it unless ransom is paid

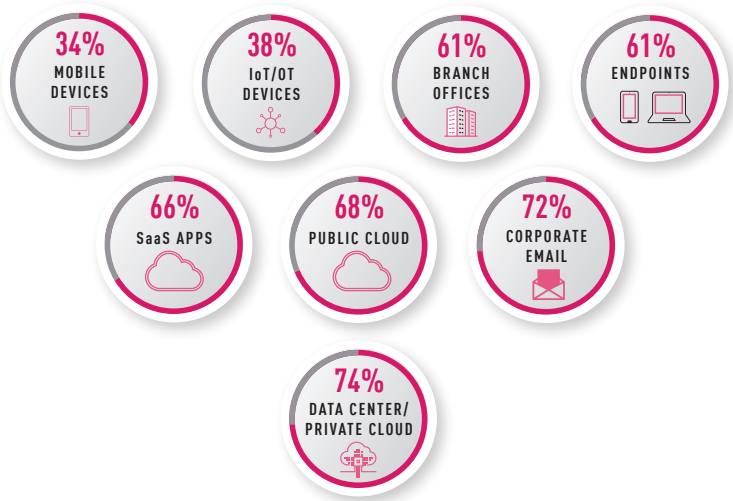
In Dimensional Research's survey 90% have seen increasingly sophisticated cyber threats during the past three years.



With more assets to secure, confidence in security goes down

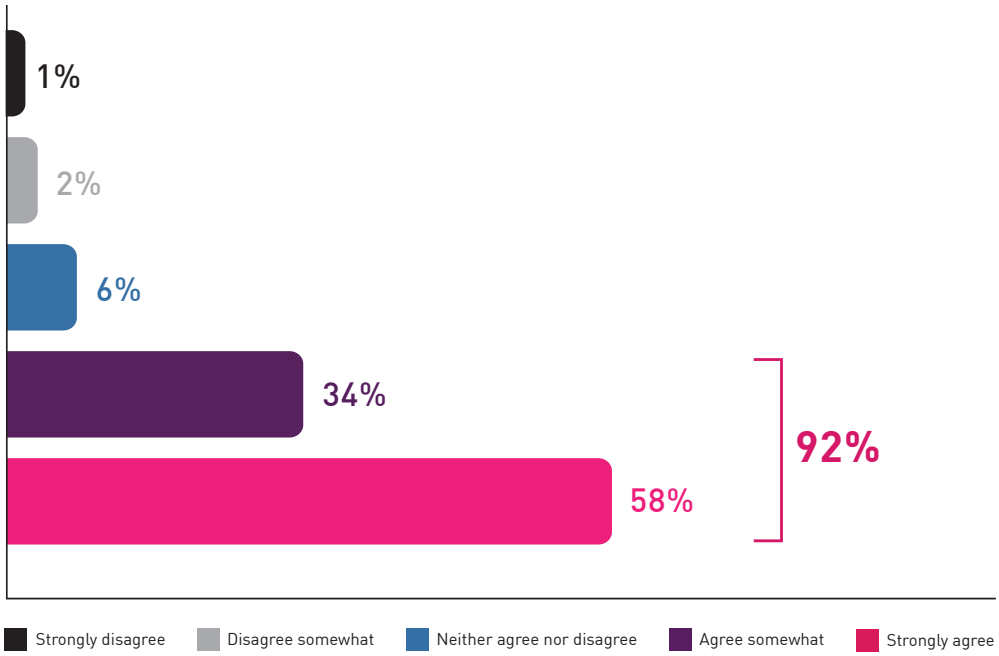
While cyber threats have become more sophisticated, security professionals are required to also protect a greater number of IT assets. Data centers, public clouds, corporate email, mobile and IoT devices, endpoints, SaaS apps, and branch offices must all be defended.

PERCENTAGE OF SECURITY PROFESSIONALS WHO ARE CONFIDENT IN THE SECURITY OF DIFFERENT IT ASSETS



92% of survey respondents said that securing all of their IT assets against all threats is challenging. But what is most remarkable is the low level of confidence held by these security professionals in securing various surfaces. Most security leaders lack confidence in the level of security provided for their organizations' mobile and IoT devices, with only 34% and 38% believing these devices are properly secured, revealing a considerable gap in organizations' security posture. That said, 72% are confident in their email security and 74% have faith in data center security.

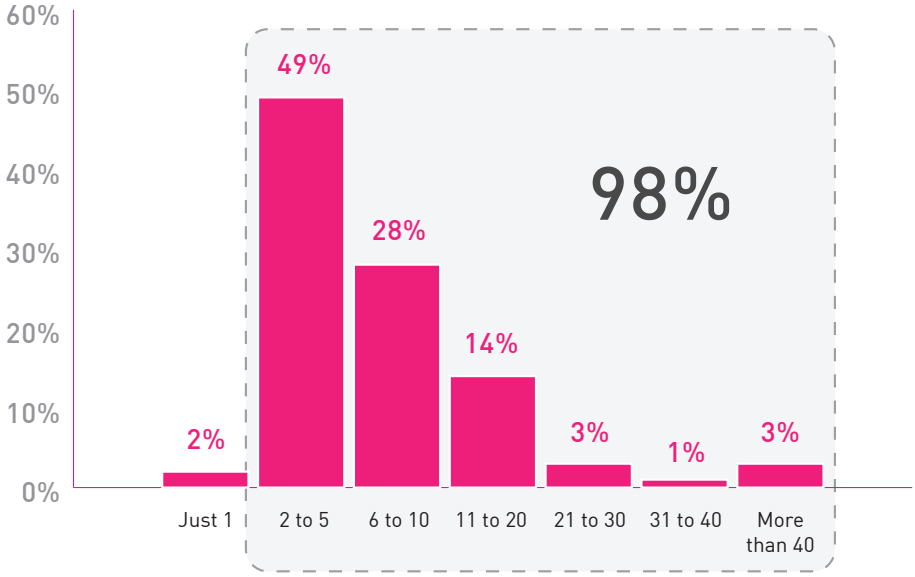
SECURING ALL IT ASSETS AGAINST ALL TYPES OF THREATS IS CHALLENGING



Nearly half of organizations deploy between six and 40 security solutions, adding to complexity

Virtually every organization in the survey used multiple security vendors, with 28% using between six and 10 different solutions, and 21% using between 11 and more than 40 different vendors.

HOW MANY SECURITY VENDORS DOES YOUR ORGANIZATION USE TO SECURE YOUR ENTIRE IT INFRASTRUCTURE?



However, larger organizations with 5,000 to 10,000 employees and those with 10,000 employees or more deploy far more solutions than their smaller company counterparts. Twenty-seven percent of companies of more than 5,000-10,000 employees use between 11 and 40 plus vendors; while 30% of companies with more than 10,000 employees used between 11 and 40 plus security vendors

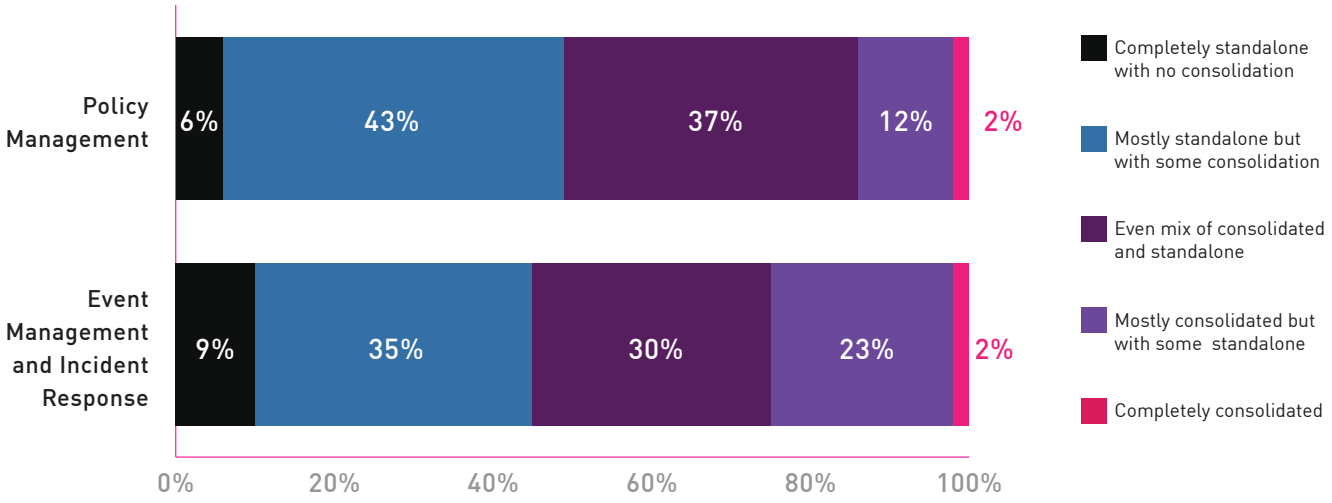
NUMBER OF SECURITY VENDORS FOR LARGER COMPANIES INCREASES

	Employees				
	All	500 - 1,000	1,000 - 5,000	5,000 - 10,000	More than 10,000
Just 1	2%	4%	4%	0%	0%
2 to 5	49%	66%	52%	41%	38%
6 to 10	28%	18%	28%	32%	33%
11 to 20	14%	11%	13%	11%	19%
21 to 30	3%	1%	1%	10%	2%
31 to 40	1%	0%	1%	3%	1%
More than 40	3%	0%	0%	3%	8%
11 vendors or more	21%	12%	15%	27%	30%

Multiple management consoles obscures visibility

The complexity of security operations is made worse by the fact that security teams are managing their cyber defenses from multiple consoles. The inability to get a holistic view of an organization's threat posture creates visibility silos, which complicates incident response. Of those surveyed, 98% manage security operations with multiple consoles. For 86% percent of organizations, policy management is accomplished mostly with standalone consoles, or a mix of consolidated and standalone consoles. For 74% of organizations, security events are managed with mostly standalone console, or a mix of consolidated and standalone consoles.

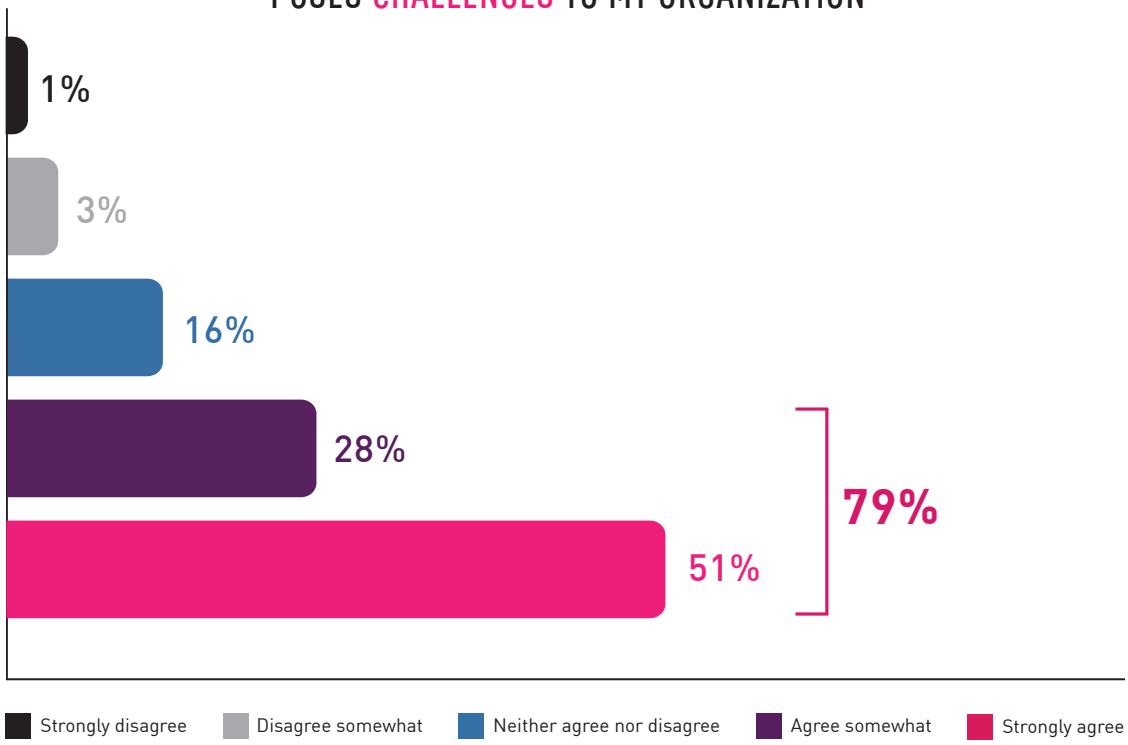
POLICY AND EVENT MANAGEMENT ARE USUALLY NOT CONSOLIDATED, OR PARTIALLY STANDALONE



Working with multiple security vendors causes challenges for organizations

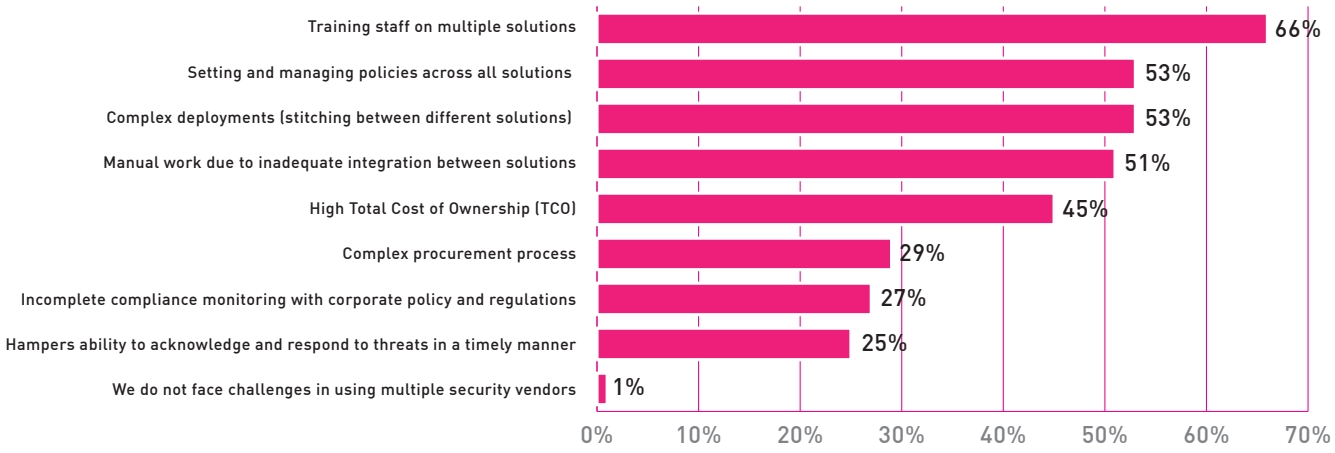
Using products from a dozen or more security vendors adds another layer of complexity for most organizations. Maintenance, version upgrades, contract renewals and other activities related to the care and feeding of a security solution all take valuable time and resources. 79% of survey respondents said that working with multiple vendors is challenging.

WORKING WITH MULTIPLE SECURITY VENDORS POSES CHALLENGES TO MY ORGANIZATION



99% of companies using solutions from multiple security vendors said it caused challenges to their organization. A majority of respondents cited training staff (66%), setting and managing policies (53%), complex deployments (53%) and manual work needed for inadequate integrations between solutions (51%) as their biggest challenges.

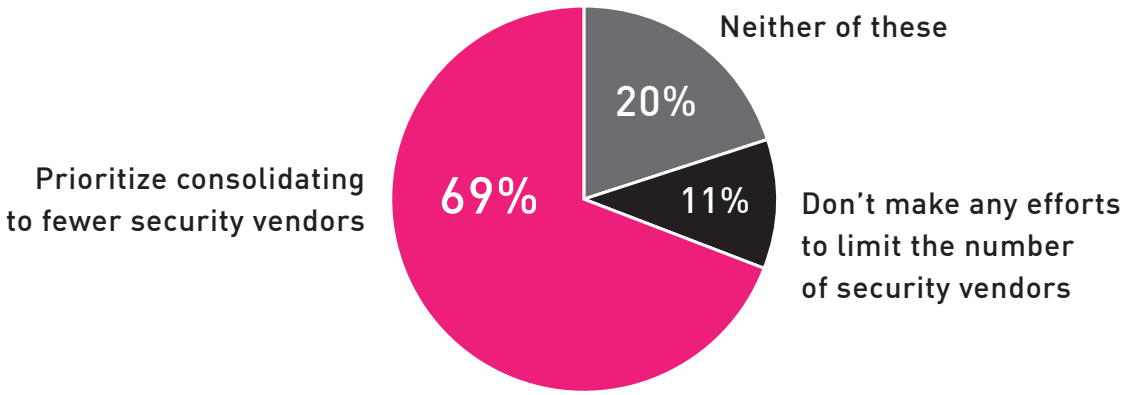
CHALLENGES POSED BY USING MULTIPLE SECURITY VENDORS



Why consolidation improves enterprise security

When asked what they believe would be the best approach for improving security in their organizations, 69% cited prioritizing consolidating to fewer security vendors.

STRONG AGREEMENT THAT VENDOR CONSOLIDATION WOULD IMPROVE SECURITY



Check Point Infinity: Begin the journey towards consolidation

Reducing the number of vendors not only simplifies having to monitor multiple management consoles, it allows for a higher level of security through superior integration, and fewer functional gaps between the protections each product delivers. It also significantly reduces the time, cost and resources of incident remediation processes.

> "It is not a daily increase, but a daily decrease. Hack away at the unessential. The closer to the source, the less wastage there is." *— Bruce Lee, Martial Artist*

If organizations move to a unified, consolidated security architecture such as Check Point Infinity that delivers protection across networks, cloud, endpoints and mobile, they improve their protection against threats, simplify security management, and boost efficiency. Infinity's single management centrally correlates a wide range of events across all network environments, cloud services and mobile infrastructures. Check Point's pre-emptive threat prevention technology blocks the most sophisticated attacks before they can inflict damage.

As legendary martial arts expert Bruce Lee said: "It is not a daily increase, but a daily decrease. Hack away at the unessential. The closer to the source, the less wastage there is." Consolidating security architectures enables organizations to remove the unessential, and make their defenses stronger and more agile against all forms of attack.

Next Steps

When asked what they believe would be the best approach for improving security in their organizations, 69% cited prioritizing consolidating to fewer security vendors.

- Read the white paper: *The Top Four Ways to Increase Security ROI*
- Watch the video about how Eurowind protects its critical energy infrastructure from attacks

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com