Check Point
SOFTWARE TECHNOLOGIES LTD

REDUCING YOUR CYBER RISK WITH A CONSOLIDATED ARCHITECTURE

Introduction

When point solutions first emerged on the market, IT professionals purchased products designed to address specific security problems. However, cyber attacks have evolved in volume and sophistication since the inception of point solutions, and this approach is no longer feasible, nor good enough. Although point solutions can cover the security basics, a consolidated architecture provides complete visibility, superior threat intelligence and uniquely powerful management tools. This paper discusses how these core capabilities can help you reduce your risk, optimize for efficiency and take your business to new heights.

> The average security team juggles 57 different security tools on behalf of their organization.[1]

With expanding attack vectors, including cloud, mobile, SaaS and IoT, now is the time to reconsider your cyber security strategy.

[1] "Why Poor Visibility is Hampering Cybersecurity," Help Net Security, June 24th, 2019

Visibility

For the most expansive and in-depth security insights into your network, visibility via an easy-to-comprehend security dashboard is imperative.

A security solution that provides clear insights enables you to effectively manage your risk and your time. When security products speak in different languages and report in different metrics, teams must devote extensive time to comparing trends. Piecing together disparate bits of information to identify suspicious activity is inefficient, and it can also result in missed clues. When security products cannot communicate with one another, clearly seeing the organization's day-to-day security posture becomes nearly impossible, valuable talent is poorly managed, and security slips can occur.

Owning security products that cannot communicate with one another, and where metrics aren't visible in a single location, may mean that your security team needs to manually enter data into different platforms. Not only does this create the monotonous task of rekeying information, it also exposes organizations to data entry errors. With an integrated, dashboard-based solution, data only needs to be entered once, cutting down on the risk of employee errors, which strengthens your cybersecurity posture.

> With expanding attack vectors, including cloud, mobile, SaaS and IoT, now is the time to reconsider your cyber security strategy.

A good security dashboard will offer real-time event monitoring that gives you 360° visibility into your network.

Enhanced Threat Intelligence

Using a dashboard to apply and monitor threat intelligence tools –such as automation, multiple feeds, and actionable insights- accelerates identification and remediation efforts. Threat intelligence tools can help you achieve more than you thought possible.

Automation

For better threat intelligence, deploy automated threat intelligence (TI). Rather than the haphazard compilation of insights at irregular intervals that you obtain through manual processes, automated threat intelligence drives consistency, and lends a new level of maturity to your IT security architecture. With consistently monitored and measured security analytics, you can see threats before they lead to long-term consequences.

Automated security tools also augment response times. The volume of information due for analysis is vast, and without AI based tools, it is too vast for most teams to contend with. The majority of the data that exists in the world was created in the past few years, meaning that this problem of information overload is relatively new. When new challenges arise, the tools for resolving them must keep pace.

Multiple Feeds

Another advantage of modern, automated threat intelligence includes the ability to rapidly process information from a variety of sources, simultaneously.

Access to multiple threat-intelligence streams gives you an increased volume of data to work with, which, in turn, better informs the actions that you need to take. As Gartner notes, "...to be more effective and proactive, there is the need for a more active...exchange of threat intelligence data."[2]

Modern cyber security threat intelligence platforms can process information from file emulations, external security analyses, anti-malware engines and more. Although the high volume of threat information can be overwhelming, this issue is easily addressed with customized targeting tools that can help you hone in on specific types of insights.

Actionable Insights

Organizations need as much information as possible in order to effectively analyze risk, and to choose the best course of action. When you can obtain a clear picture of the threat landscape, both externally and inside of your organization, you can optimize your decision making. Actionable insights are a game changer, and can keep your organization more secure than ever before.

Enhanced threat intelligence can transform your approach to security, allowing you to see who or what is on your system, which in turn enables better decision-making, resulting in a stronger cyber security posture.

When you can obtain a clear picture of the threat landscape, both externally and inside of your organization, you can optimize your decision making

[2] "Competitive Landscape — Threat Intelligence Services," page 7, Gartner, October 2014

Powerful Management Tools

A consolidated cyber security architecture offers simplified management, greater efficiency and cost savings.

Simplified Management

According to a Forrester survey of global decision makers, 54% reported that their existing tech architecture is too complex to manage.[3] With a high volume of security platforms, centralized management is essential. Rather than spending time untangling which of your many platforms need attention or how to address a problem, a centralized management system does the work for you.

For example, in an organization that relies on point solutions, two point solutions with overlapping functions may each recognize a threat, but classify it differently. Given the conflicting intelligence, security personnel will have to deliberate on what procedures to follow. Prolonging threat response times is known to increase chances of attack damage. With a unified management approach to cyber security, you have reliable data points that enable you to take immediate action. Centralized management means less operational friction, and more time for higher-level priorities.

Troubleshooting

There's a lot to do, and your IT team likely lacks the bandwidth to spend hours, days or weeks resolving interoperability issues across a variety of providers. Calling help centers and reaching staff who not only have knowledge of their own product, but also of those produced by other companies, can be a time-consuming task. A centralized system operating via a single, overarching platform makes troubleshooting a breeze. Because the provider supports the entire operating system, the support staff can answer questions easily, and quickly resolve issues.

Cost Savings

You'll likely see lower overall costs with a consolidated security solution. An abundance of point solutions means that you may have similar tools that provide overlapping functions, meaning that you're paying for the same tool multiple times over. With a single vendor, you can be sure that you're not paying for anything that you do not need. You'll also save on labor and installation fees.

In terms of direct ROI, statistics show that point solutions take an average of 40 days to identify attacks, costing organizations an average of $667,500 in remediation costs. In contrast, consolidated

[3] "Improve Business Agility Through Platform Consolidation," Forrester, June 2018

solutions identify attacks in an average of two days, with an average total cost of $6,800 in remediation. It goes without saying; a consolidated solution is the better deal.[4]

Unified threat management offers unparalleled benefits. For fast-paced organizations, powerful management tools simplify your day-to-day tasks, and help you get the most out of your resources.

In Conclusion

Many organizations are making the transition to a consolidated security solution. Two-thirds of organizations are actively trimming the number of vendors that they work with.[5] Bringing all of your protections and functions under a single umbrella does more than minimize your risk; it results in business enablement that benefits you, your team, and your organization at-large.

For more information on how a single, consolidated architecture can enrich your organization, please visit the Check Point Infinity webpage, or reach out to your local Check Point representative.

A Case in Point

Tecnun University of Navarra wanted powerful, consolidated security tools, and to meet their needs, they selected Check Point as a vendor. “The ability to combine all the security features we need in a single product for protection and management was decisive.”

“We can now view traffic and have access to information we didn’t have before, for both internal and external activity, meaning we can react quicker and make decisions on the spot.”

“Moreover, the security management console allows our IT department to define the desired service and security level for each group (students, teachers and support staff) and categorize what they have access to and how they can access it,” said Enrique Reina, Head of IT at the University of Navarra’s Technology Campus, in San Sebastian.

[4] “Rethinking the Cyber-Consolidation Paradigm,” Check Point Software Technologies

[5] “The Cybersecurity Technology Consolidation Conundrum,” CSO Magazine, Jon Oltsik, May 26th, 2019

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