CHECK POINT™

YOU DESERVE THE BEST SECURITY

TOP 4 ELEMENTS OF A CYBER SECURITY PLATFORM

Introduction

In today's rapidly evolving threat landscape, adopting a proactive, intelligence-based cyber security platform is essential. Key challenges include maintaining robust security, visibility, efficiency, ROI, and managing digital transformation.

A cyber security platform can address these issues through AI-powered threat intelligence, a zero trust approach, consolidation, and cloud security capabilities. Advanced tools reduce the risk of cyber attacks, ensuring your organization remains safe, agile, and prepared for the future.

Why Innovation

You've already seen that traditional security approaches aren't enough to contend with today's emerging threats. With an attack surface that seems to stretch beyond the horizon, the shortage of 3.4 million cyber security workers, and increasing compliance complexity, among other challenges, you might find yourself rethinking how to approach security.

Can you operate at the velocity of digital disruption? By evaluating new tools and technologies, and by embracing innovation, you'll be able to align cyber security with business objectives. You'll be able to enable new business opportunities at speed and scale.

> "Change makes you vulnerable — even change for the better. Pursuing a strategy that connects innovative security solutions to business enablement involves an element of risk. But not as much risk as failing to take action."
>
> Cindi Carter, Field CISO, Check Point

Cyber Security in Action

Put cyber security into action. Explore the top 4 elements of a cyber security platform, including AI-powered threat intelligence, zero trust, a consolidated cyber security architecture and unified cloud-native security.

1. AI-Powered Threat Intelligence

AI-based threat intelligence can offer significant value. At present, nearly 50% of enterprises are already using a combination of artificial intelligence and machine learning tools to improve cyber security outcomes, and 92% of organizations plan to adopt these types of tools in the future.[1]

Advanced algorithms permit AI-based threat intelligence solutions to observe, analyze and alert you to threats in real-time. Unparalleled in every way, you'll receive essential information that can optimize and inform decision-making. You'll be able to proactively prevent attacks.

When it comes to efficiency, AI-supported cyber security programs can automate time consuming and monotonous tasks; from monitoring logs, to scanning for vulnerabilities, to patching systems. In turn, security teams can focus their attention on more strategic activities.

AI also enables automated threat response. An organization can configure AI-based tools so that they can independently respond to security incidents. For instance, in the event that AI detects a potential attack, it can automatically block the attack, quarantine a device as needed, and alert the security team. This cuts down on response times, prevents large-scale incidents, and enables security teams to tackle tougher problems.

Further, AI can help analysts cycle through a **fast, data-driven and comprehensive incident response**. It can automate workflow and remediation. It can also enable SOC teams to review and refine incident response processes on a continuous basis.

2. A Zero Trust Approach

Across the industry, security professionals are shifting to a zero trust approach, which assumes that every user or device on a network is a potential threat. A zero trust approach sanctions the verification of each individuals' identity and device ahead of granting resource access. As you'll see below, implementing zero trust based on a single consolidated architecture can provide organizations with numerous benefits.

[1] How Artificial Intelligence is Revolutionizing Cyber Security, Cyber Talk, March 27, 2023

In general, zero trust can result in improved visibility. In a traditional perimeter-focused security architecture, an organization's security solutions are concentrated at the network perimeter. Although this reduces the number of external threats that can affect the organization, it also means that the organization has limited visibility into what's happening within that network perimeter.

The zero trust security model moves the security boundary. Because every access request must be approved or denied, the organization has more meaningful visibility into the actions being performed within its network.

Zero Trust can also limit insider threats. To that effect, zero trust reduces the possibility of malicious insiders. With a zero trust architecture, every user, device and application must be authenticated and authorized ahead of receiving access to network systems or resources. In addition, zero trust employs continuous monitoring and analytics in order to catch any behaviors that could be indicative of an insider threat.

Zero Trust also limits the possibility of malicious insider action by segmenting the network into smaller, more manageable elements that make it challenging for a hacker to maneuver laterally across the network. The hacker would need to compromise multiple network segments and overcome additional access controls to infiltrate an enterprise.

In general, zero trust offers a more refined, defined and proactive approach to cyber security, preventing acutely negative fallout from incidents.

Depending on the approach taken, zero trust can also help **streamline cyber security management.** If you implement zero trust using disparate technologies, you might find coverage gaps that hackers could easily and stealthily exploit. Our experts recommend pursuing a holistic and practical approach to zero trust implementation through the use of a consolidated cyber security architecture.

With a consolidated cyber security architecture supporting your zero trust implementation (or evolution) you can execute against 100% of zero trust security principles, you can manage your tools more efficiently and better protect your organization from zero day attacks. In addition, zero trust plus cyber security consolidation means that you can have a single vendor partner with you throughout every step of your transformation journey.

3. Consolidated Cyber Security Architecture

Beyond the previously noted advantages of a consolidated cyber security architecture, cyber security consolidation can enhance overall efficiency, lead to cost optimization, and increase resilience.

When it comes to efficiency, consolidated security architecture **directly impacts the number of hours that your team spends securing your enterprise.** When organizations employ a consolidated security architecture, there's a 50% reduction in staffing needs.[2]

> "As businesses look to remove cost and complexity from the entire digital and security stack, consolidation will become a "real" priority."
>
> Deryck Mitchelson, Former CISO of NHS Scotland and Field CISO, Check Point[3]

In terms of direct ROI, statistics indicate that point solutions take an average of 40 days to identify cyber attacks. This costs organizations an average of $667,500 in remediation costs. In contrast, consolidated solutions identify attacks in an average of two days, with an average total cost of $6,800 in remediation.

"As businesses look to remove cost and complexity from the entire digital and security stack, consolidation will become a "real" priority," says former CISO of NHS Scotland and Field CISO for Check Point, Deryck Mitchelson.[3]

One of the most powerful advantages that a consolidated cyber security solution can confer consists of **end-to-end cyber security resilience**. You want the best chance of adapting to adverse conditions, withstanding an incident, recovering from potential disaster, and resuming business as usual.

The best consolidation tools prevent advanced threats, respond to widespread attacks and broadly enhance an organizations' cyber security controls. Select solutions can also seamlessly integrate with third-parties to achieve optimal outcomes.

4. Cloud Security Capabilities, Enabling Digital Transformation

Organizations are transitioning from traditional data centers to what are next-generation data centers — the cloud. Rising cloud complexity and cloud sprawl means that organizations must focus on keeping cloud networks, data and applications safe. In addition, the constantly evolving nature of the cloud reinforces the need for superb cloud security.

---

[2] What is a Consolidated Cyber Security Architecture? Check Point

[3] 4 CISO Perspectives on the Future of Cyber Security, Cyber Talk, December 22, 2022

> The rate of cloud security change feels 100X faster than the rate of change for on-premises security. As a result, your security team is likely in constant fear of a cloud-based attack or threat.

Leverage next-generation cloud security to accelerate your cloud-based digital transformation objectives. **Effective cloud security can enable your organization to digitally transform** in a way that advances enterprise agility, furthers innovation and that helps you capture new value.

A unified and agile deployment model allows your business to gain control, governance and observability across your cloud environment. A single vulnerability or unconfigured resource, left unchecked, can result in a breach.

Obtain the best cloud protection by applying a solution that includes automation capabilities. Select or shift to a could security solution that offers automated vulnerability scanning, automated continuous monitoring and automated patch management. If you're not automated, you're always going to be behind. You're going to lose the battle because everything around you is automated.

Organizations are moving to the cloud in order to create new value — in order to move faster; in order to create more capabilities, more applications, and more functionality in a more efficient way. Your security needs to support the creation of new value for your business, for your partners and for your customers.

Unified cloud-native security for your workload and networks can provide a powerful package of competitive business advantages, especially when integrated with dynamic threat intelligence platforms.

To keep pace with modern threats, you need next-generation, innovative and **digitally transformative cloud security.**

Security in Business Enablement

It is time for a new security paradigm. By implementing advanced technologies, like AI-based threat intelligence platforms, zero trust combined with consolidated infrastructure, and unified cloud-native security, an organization can effectively address some of the most taxing and treacherous issues within cyber security today; from visibility, to compliance, to complexity.

When these concerns are effectively and proactively managed by technological solutions, you can concentrate on higher-level issues. By applying a "Security in Action" approach, you can take on a more strategic role in your organization, driving greater value and protecting against threats at the same time.

What are you waiting for?

After all, hackers are continually evolving their strategies, and investigating the latest tools. It makes sense, you should too. It's time to take action.

Taking Action: AI-powered, Cloud-delivered Cyber Security

Translate your cyber security strategy into action. Check Point's Infinity Platform embodies the fundamental principles described in this guide. It leverages cutting-edge artificial intelligence to provide real-time threat prevention across all attack vectors, protecting networks, cloud and work-spaces from sophisticated cyber attacks.

Instead of relying on multiple, non-integrated point solutions from different vendors, Infinity unifies all cyber security capabilities from a single pane of glass, simultaneously reducing management complexity and lowering total operating costs. By implementing Check Point Infinity, you're going beyond advanced cyber security – you're empowering your organization with the industry's most innovative, comprehensive and future-proof solution available on the market today.

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
100 Oracle Parkway, Suite 800, Redwood City, CA 94065 | Tel: 1-800-429-4391

www.checkpoint.com