CHECK POINT INFINITY

TOP FOUR WAYS TO INCREASE SECURITY RETURN ON INVESTMENT

The Cyber Security Return on Investment (ROI) Challenge

Organizations are under increasing pressure to rationalize IT infrastructure expenditures. Digital transformation requires major investments in applications, and firms would rather spend on application development then on the "plumbing" infrastructure necessary to run them. On the other hand, everyone understands the critical need for security. But while the demands made on security are increasing, security spending as a percentage of IT budgets is not.

The pressure on security budgets comes from many angles. Emerging threats, new application architectures, hybrid cloud and new regulations are just the most salient of a long list of things that all create more work and responsibilities. These factors are forcing CISOs to take a hard look at capital and expense budgets, to see how money can be used more efficiently.

As a pioneer in enterprise security, Check Point has long recognized the need to maximize ***both*** security efficacy, and the efficient use of resources. Check Point's Infinity Architecture balances these two challenging objectives. This document will describe how Infinity supports more efficient security investments, while also increasing security effectiveness.

Check Point Infinity Architecture

Check Point has always believed that effective and efficient security is only possible when deployed as a unified architecture. Check Point Infinity is the industry's only consolidated cyber security architecture that protects the business and IT infrastructure against Fifth Generation mega cyberattacks across all networks, endpoint, cloud and mobile. Infinity delivers:

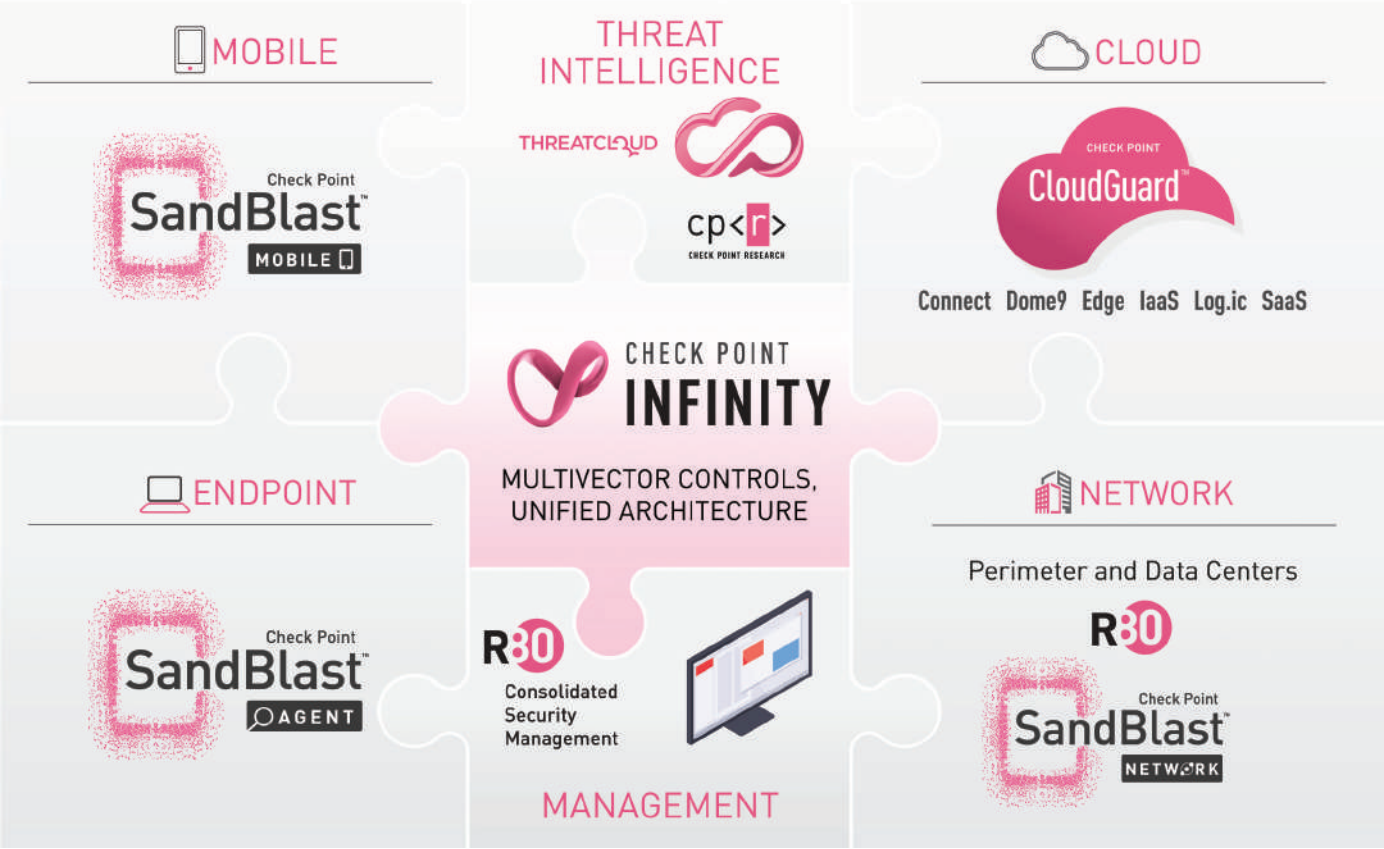
Advanced Threat Prevention: The industry's leading suite of protection capabilities, deployed across networks, cloud and mobile

Shared Threat Intelligence: Check Point ThreatCloud, which amalgamates and distributes threat intelligence and protection updates in real-time

Consolidated Management: A unified management interface that allows business-oriented risk policies to be operationalized into security protections, with APIs for integration with IT infrastructure and applications

Check Point
SOFTWARE TECHNOLOGIES LTD

WELCOME TO THE FUTURE
OF CYBER SECURITY



Check Point Infinity provides complete protection from known and zero-day attacks across every environment, including cloud and mobile. The simple, business-oriented management interface reduces complexity, making it easier to deliver security and compliance with constrained staff and budget. Infinity helps organizations deliver agile yet secure IT, which can adapt as business requirements change. Through advanced threat prevention, business-oriented policy management, and cloud-based threat intelligence, Infinity delivers a solid foundation for a sustainable, effective risk management strategy.

We will now examine the specific aspects of Infinity that drive financial efficiency and improved ROI.

Infinity: Driving Security Efficiency & Return on Investment

Four dimensions of the Infinity architecture drive down costs and improve ROI.

1 FEWER PRODUCTS TO DEPLOY AND MANAGE

The most obvious financial benefit of Infinity is that it consolidates many functions into fewer systems to be deployed. Historically, building security into IT infrastructure has been incredibly complex, due to the need to maintain application availability and performance while also providing security everywhere it's needed. The Infinity solution set consolidates many security functions into single systems that provide both scale and availability assurance. This results in simpler architectures, fewer points of failure, and less risk associated with upgrades and patches. It also simplifies procurement and training.

2 UNIFIED MANAGEMENT

The second key Infinity benefit is its unified management. At a high level, Infinity enables the creation and deployment of a unified policy across the architecture. The financial benefits are massive, because there are so many ways in which unified management drives down operational costs. These include:

Infinity Management Element	Financial Benefit
Single Management System	• Eliminates costs of deploying and maintaining parallel management infrastructures • Reduced training
Unified Policy	• Reduced staff time to create and manage security policies • Eliminates time wasted trying to determine actual policy resulting from multiple tools • Lower cost supports for hybrid cloud architectures
Task-Driven Administration	• Simpler policy creation – less than half the effort of competing products • Reduced risk of policy misconfiguration
Incident Response	• Consolidated event viewer and cyber attack dashboards reduce staff overhead for monitoring and incident response
Role Delegation	• Delegates policy management to relevant organizations, reducing unnecessary communication and coordination
Workflow	• Increase security effectiveness by reducing costly operator errors that can cause security breaches • Increases ability to stay in compliance by automating policy configuration and remediation • Simplifies risk and compliance reporting

Unified management also improves ROI indirectly through lower risk. Better policy management translates into lower risk of a security incident or data breach. This fact has been well documented. As an example, the annual Verizon Breach Reports highlight how most breaches are the result of basic control failures, including a failure to implement tight access and threat prevention policies. Given the high costs of data breaches, lowering the risk of such events has a significant ROI. While it can be argued that quantifying this benefit is challenging, this doesn't change the basic fact that lowering risk provides a further financial (and reputational) benefit in addition to the direct benefits noted above.

2019 Verizon Data Breach Report: https://enterprise.verizon.com/resources/reports/dbir/

3 THREATCLOUD THREAT INTELLIGENCE

ThreatCloud is Check Point's shared threat intelligence platform. It is the world's largest threat intelligence database, aggregating threat intelligence data from a broad array of sources, including 100 million gateways across the world. ThreatCloud processes 86 billion IoCs and emulates more than 4 million files per day, and thereby typically stops 7,000 zero-day attacks per day. ThreatCloud pushes threat prevention updates to all subscribing customer's Infinity deployments automatically, including firewalls, cloud, mobile and endpoint protections.

ThreatCloud improves security ROI in three ways. First, it lowers operational overhead, by automating threat prevention updates across the architecture, and decreasing reliance on multiple threat intelligence feeds and enforcement points. Second, it lowers the cost of incident response, by pushing threat prevention to enforcement points based on malware found in an organization's own environment. This "self-protecting" aspect of Infinity takes the pressure off IR teams when an incident occurs, allowing them to focus on recovery and less on trying to contain the outbreak.

Lastly, as with unified management, ThreatCloud decreases the likelihood of a significant data breach, potentially generating huge savings in reputational and financial impact to the overall business.

4 SIMPLIFIED INTEGRATIONS

Security doesn't exist in a vacuum; it must integrate with IT and cloud infrastructure. The lack of integrations across IT systems is frequently cited as a reason for poor risk management, and leads to attacks "falling through the cracks". Unfortunately these integrations can be challenging to build and maintain, especially given the limited programing staff generally available in the security team. Fortunately, because Infinity consolidates security functions, it acts as a single integration point for infrastructure, reporting, and incident response. This enables integrations that are simpler, and therefore easier and less expensive to build and maintain. This also reduces friction with other departments, as it is much easier for them to support the security integrations necessary to protect the business.

> "Check Point Security Compliance makes it easy for us to apply the best practices we need to meet our HIPAA requirements. It not only provides great protection, but it also demonstrates our commitment to security, which can make a huge difference if our organization is audited."
>
> *— Felix Castro, Director of IT, ICS*

"We cut the time we spend on managing security by 80% and, thanks to the simplicity of the Check Point solution, 90% of our daily IT security activities are now automated."

— Stefano Biava, IT Manager, Phoenix International

Infinity in Action: An Anatomy of an Attack

Better use of resources is always a good thing, except if it comes at the price of poor security. Fortunately this isn't the case with Infinity, as we will show in a real-world customer example. The organization in question is an international retail company with roughly 2,000 employees distributed in over 50 branches. Historically, the security team had constructed a "point-based" product approach: purchasing products from nine different vendors based on their perception of the current threat landscape and which technologies appeared to be "hot". The result was a patchwork of products that didn't talk to each other and was hard for the small security team to operationalize.

The consequences of these choices became apparent when the firm was successfully hit with an attack that leveraged a very common methodology:

- Day 1: Phishing emails were sent to a number of staff at their corporate Office365 accounts and even private gmail accounts. Most of these emails were caught by a network gateway, but one was opened on a mobile device by a remote employee, leading to a successful compromise of that device.
- Day 2: With full control over the mobile device of the employee, the hacker sent an email with an attachment containing zero-day malware to the entire mailing list of the employee. Since the email was sent from a corporate mailbox, the malicious attachment was successfully opened by dozens of employees, and infected their workstations.
- Day 3: The malware continued to spread throughout the network and infected hundreds of additional workstations; one of them was a workstation of an IT admin. Using this IT admin's compromised workstation, the attacker managed to obtain privileged access to a virtual machine in the public cloud that the customer database was stored on.
- Day 60: Data Breach was detected
- The firm suffered a $1.5M loss and significant reputational damage because of the attack.

Following this attack, the firm asked for a demonstration of Check Point Infinity. We were able to show how Infinity could have stopped the attack in the early stages of the cyber kill chain.

Specifically, advanced threat prevention for mobile devices would have detected the malicious file in advance and would have blocked the download, keeping the "Trojan Horse" malware off the mobile device of the employee. This would have prevented the hacker to attack the other employee workstations, stopping the attack from moving laterally in the network. Even if the hacker found a way to continue the attack, Infinity's automated protections would have stopped it once, after gaining Threat Cloud's instant alerts on the mobile attack, which included a File Hash and C&C server address.

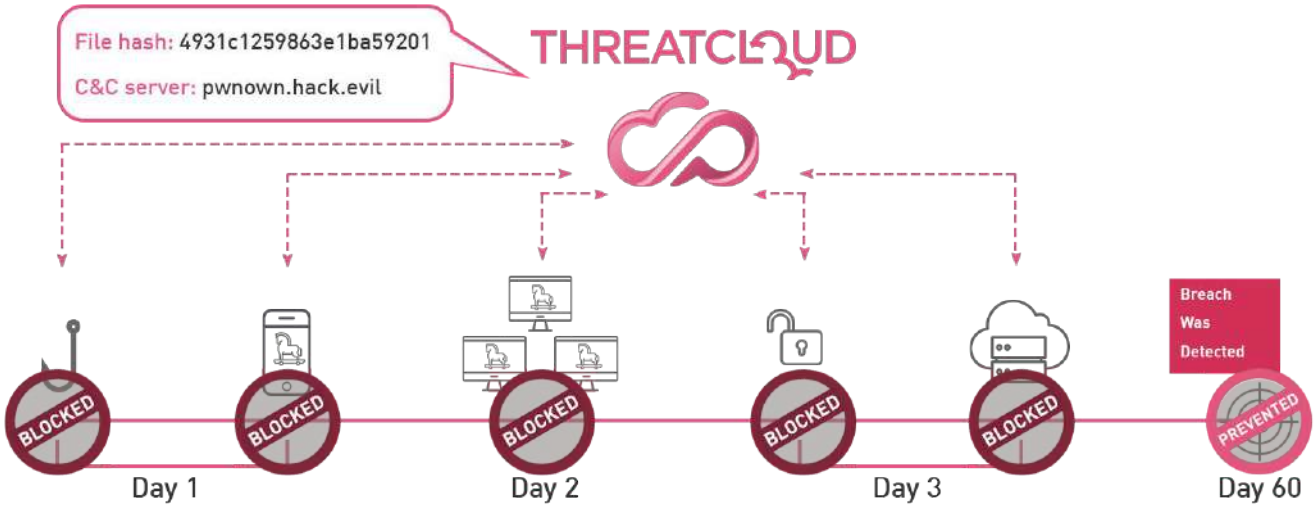
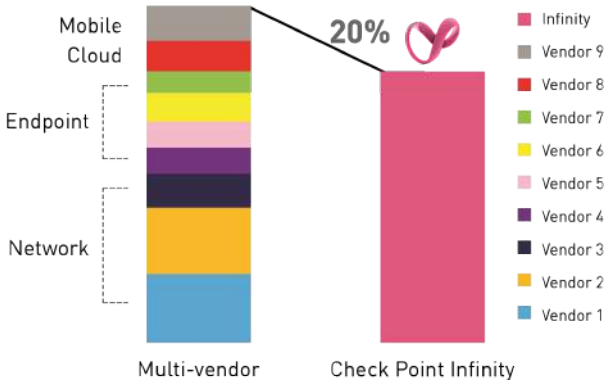


Figure 1: ThreatCloud is fundamental to disrupting the cyber kill-chain

The firm has subsequently replaced their multi-vendor product set with Check Point Infinity. They are now enjoying superior protection, and a 20% decrease in direct product costs. More importantly, they are able to operate the solution with much less staff time, since they have replaced nine consoles with only one.



Infinity lowered the firm's direct product costs by 20%.

Summary

While most organizations understand that IT security is complex and vitally important, they are also under pressure to control IT costs. However it is next to impossible to control costs when a wide variety of products and services need to be deployed, integrated, operated, and maintained. Check Point Infinity helps organizations of all sizes rationalize their security budgets and staffing by consolidating equipment, services, management and support into a single, operationally efficient framework that can more easily be integrated with the broader IT infrastructure and processes. Therefore, Infinity should be given strong consideration by any business seeking to improve ROI while not sacrificing on security or adherence to compliance regulations.

PREFER ANNUAL SUBSCRIPTIONS? CONSIDER INFINITY TOTAL PROTECTION.

Many organizations struggle to budget for security given the rapid pace of digital transformation and cloud adoption. Infinity Total Protection is a per-user, annual security subscription option that allows you to use as much Check Point security as you need, whenever you need it:

- Consume all Check Point solutions based on your requirements and timing
- Includes software, hardware, subscriptions and services
- 24x7 support and real-time security updates
- Single procurement and predictable spend

Ideal for organizations over 500 people, Total Protection is the only subscription offering available today that includes both network security hardware and software, with fully integrated endpoint, cloud and mobile protections and zero-day threat prevention, together with unified management and 24×7 premium support.

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