Check Point
SOFTWARE TECHNOLOGIES LTD

CHECK POINT INFINITY ARCHITECTURE

THE CYBER SECURITY ARCHITECTURE OF THE FUTURE

GEN V

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Virtually all IT Security organizations seek to improve their ability to mitigate risk at a reasonable, sustainable investment level. Three challenges make this extremely difficult:

1. The 5th generation of cyberattacks – aggressive, rapidly evolving multi-vectored mega attacks (such as WannaCry, NotPetya and others) that inflict major damage on businesses and their reputation
2. The organization's dynamic, evolving set of data, applications and infrastructure that need to be protected (mobile, cloud/SaaS, and 3rd party outsourcing are but three examples)
3. Finding and retaining security staff that can translate business goals into technical strategies that are effective and sustainable over time

Given these challenges, many in the industry have concluded that true protection is unattainable, and therefore the focus should move to detecting and mitigating threats after they have penetrated defenses. This however is a very risky strategy. What is needed is a security architecture that adapts to dynamic business demands and is focused on prevention to ensure all key assets are completely protected.

Check Point Infinity is the only fully consolidated cyber security architecture that protects the business and IT infrastructure against Gen V (5th Generation) mega cyberattacks across all networks, endpoint, cloud and mobile.

1. **Advanced Threat Prevention:** The industry's leading suite of protection capabilities, deployed across networks, cloud and mobile
2. **Shared Threat Intelligence:** Check Point ThreatCloud, which amalgamates and distributes threat intelligence and protection updates in real-time
3. **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

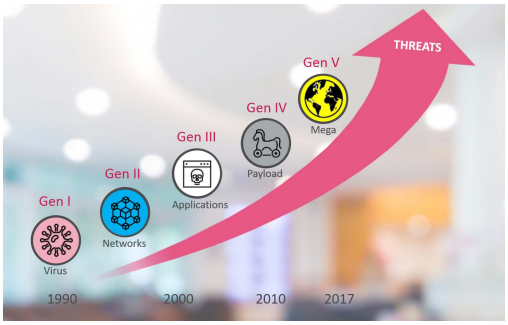
Check Point Infinity provides complete protection from known and zero-day attacks across the environment, including cloud and mobile. The simple, business-oriented management interface reduces complexity, making it easier to deliver security and compliance with constrained staff and budget. Infinity 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.

BACKGROUND

The rapid digital transformation of business is placing ever-increasing demands on security, and today we are seeing unprecedented cyber attacks carried out as large-scale, multi-vector mega attacks that inflict major damage on businesses and their reputation. Taking a closer look at types of attacks, it is easy to identify the different generations of both attacks and security solutions.

CYBER ATTACKS GENERATIONS

- **Generation 1 –** Late 1980s, virus attacks on stand-alone PCs affected all businesses and drove the rise of anti-virus products.
- **Generation 2 –** Mid 1990s, attacks from the internet affected all business and drove the creation of the firewall.
- **Generation 3 –** Early 2000s, exploiting vulnerabilities in applications affected most businesses and drove the rise in intrusion prevention systems (IPS) products.
- **Generation 4 –** Approximately 2010, rise of targeted, unknown, evasive, polymorphic attacks affected most businesses and drove the increase in anti-bot and sandboxing products.
- **Generation 5 –** Approximately 2017, large scale and multi-vector mega attacks using advanced attack technologies. Detection-only based solutions are not sufficient enough against these fast-moving attacks. Advanced threat prevention is required.



An example of a fifth generation attack opportunity is the "hybrid cloud/mobile/IoT" multi entry point environment. These types of multi vector connectivity environment creates huge numbers of new attack points to be exploited. Meanwhile, criminal organizations, nation state actors, and even the release of weapons leaked by agencies such as the NSA create ever more powerful cyber-attack technology, made available to ever increasing numbers of well-organized adversaries. Organizations are converging applications and data onto IP-based networks and rolling out and updating "cloud native" applications on a weekly or even daily basis. Company-owned desktops are being replaced with laptops, tablets, and BYOD, while applications are moving from the data-center into hybrid clouds fed by IoT devices, or outsourced completely to software as a service (SaaS). And if all that weren't enough, regulations such as GDPR are creating new data governance requirements that are difficult to implement across these IT environments.

Unfortunately, while security ***technology*** proliferates, effective security ***architectures*** are very rare. Ineffective deployment of traditional prevention products resulted in lots of log and alert data, most of which was ignored. This led to the conclusion that "they'll always get in", and therefore that the response should be to also implement detection and mitigation strategies, while still spending on traditional prevention. This approach leaves organizations lagging behind on security generations, leaving the business fully exposed to advanced attacks that not only affect operations and exposes critical information, but can also cause extreme reputational damage even to the point of threatening business viability.

Additionally, we end up with more complex security infrastructures and bigger budgets, but no improvement in protection, as the continuous stream of successful attacks in the press demonstrates.

Clearly an entirely new approach is needed to address these gaps – a well-defined security architecture that can stay ahead of Gen V attacks and succeeding generations' attacks. It must combine effective prevention technology, unified security policy, and an operational model that is realistic to implement across today's IT environment with a reasonable staffing and budget level. That new approach is Check Point Infinity.

"Enterprises need to protect themselves from sophisticated—and dangerous—attacks on all fronts: network, endpoint, mobile and cloud. These latest, fifth generation attacks (Gen V) require a comprehensive fifth generation cyber-security solution, such as Check Point's Infinity Total Protection, to keep critical business data safe from potentially devastating attacks across the entire enterprise."

— Doug Cahill, group director and senior cybersecurity analyst at market research firm, Enterprise Strategy Group

INTRODUCING CHECK POINT INFINITY

Check Point Infinity is the only fully consolidated cyber security architecture that protects your business and IT infrastructure against Gen V mega cyber attacks across all networks, endpoint, cloud and mobile. Infinity provides the most advanced cyber security for today's IT infrastructure, combining a multi-layered threat prevention solution with consolidated management and consistent APIs.

The Infinity architecture is based on three key elements. First, Infinity is focused on delivering the best threat prevention in the industry. Since our inception, Check Point has been focused on delivering the best security possible and as such we are intensely focused on innovating technologies and products that PREVENT attacks. Our prevention technologies are designed to stop both known and unknown "zero-day" attacks across all areas of the IT infrastructure, including cloud and mobile. And if an attacker does penetrate the perimeter, we terminate command and control channels and break the cyber-attack kill chain before he can extract data.

Second, Infinity delivers this protection from a unified platform. All Infinity components are based on the same common software platform, controlled and monitored by the same management, and share the same threat intelligence. This means that security policy, monitoring and prevention is consistently updated and applied across the entire IT infrastructure. Furthermore, while Infinity provides the foundation, we understand that any security infrastructure likely requires additional products and data sources. So Infinity provides a rich set of APIs to integrate 3rd party security tools as part of the broader security infrastructure. They also enable cloud orchestration integration for dynamic security services insertion and policy creation. Infinity is the architecture upon which the entire security infrastructure operates as a single, cohesive wall of protection.

While the threat prevention platform is critical, even the best security solutions are worthless if they are not properly managed. Check Point has a long history of providing the best security management available. Effective management is absolutely essential for accurate, efficient security operations. Infinity management is the key and common underpinning to truly unified and cohesive security operations, monitoring and response – across all networks, cloud and mobile. For example, Infinity management allows organizations to write a single policy and apply it across the entire IT infrastructure, enabling hybrid multi-cloud flexibility without compromising security. That policy supports rich constructs based on attributes such as identity, application intelligence, location, threat prevention policy, and much more. Unified security event management and role-based delegation of administration round out the most comprehensive security solution available. It is Infinity management that truly

What Is So Special About Check Point Infinity?

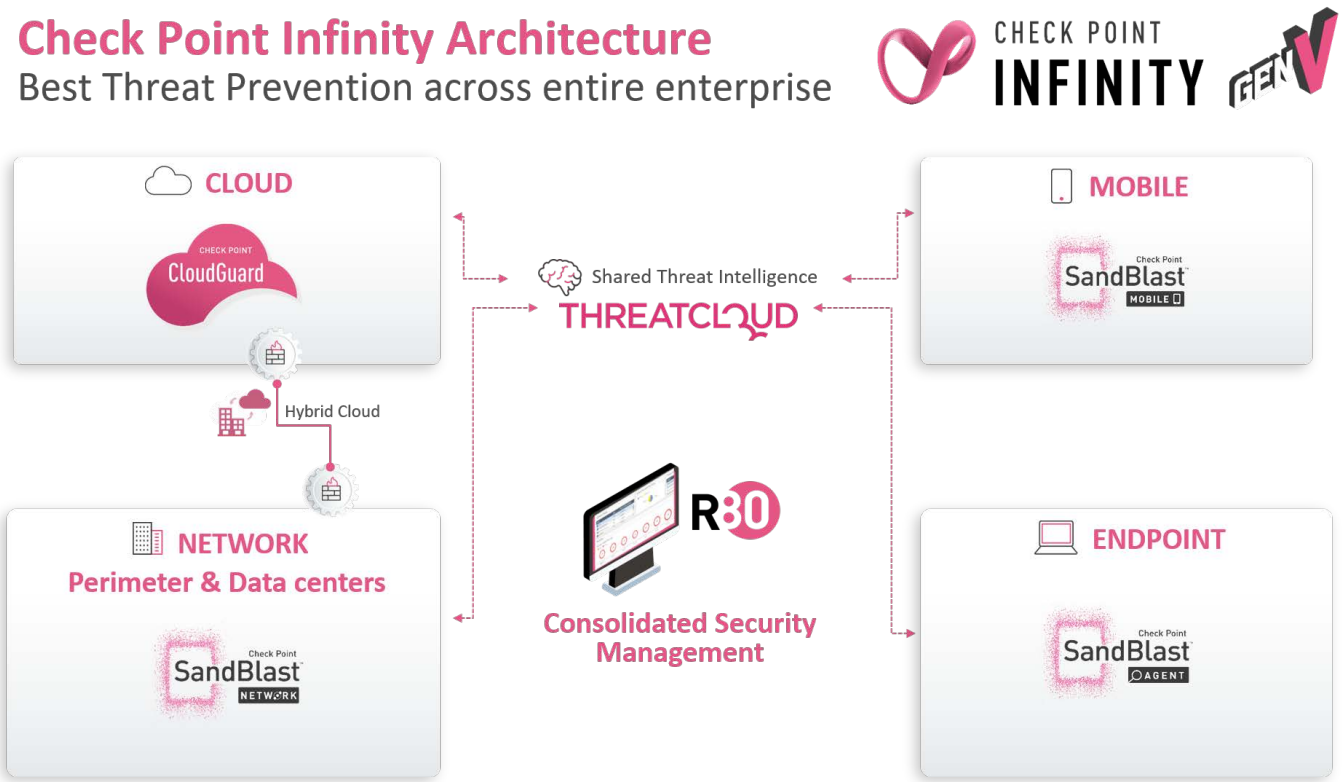
Check Point Infinity is an architecture for a single security system with common, cohesive policy, intelligence, prevention and management from monitoring to response – across all your network, cloud and mobile. And because you may have other, non-Check Point security products as part of your security infrastructure, Check Point Infinity supports integration of these products to ensure a truly cohesive security system. This is in contrast to many homegrown infrastructures where security products operate on their own islands and do not share policy, intelligence or management capabilities. Check Point Infinity enables you to build a single, cohesive security posture while making your security team more efficient and effective in their operations.

empowers security teams to properly protect IT operations whether a small business, large enterprise or managed service provider.

Infinity's key differentiator when compared to other approaches is the integration of best in class threat prevention and management across the architecture. No other vendor has Check Point's level of leadership in both areas, which is why we are the only vendor in the top-right section of Gartner's 2017 Magic Quadrant for both next-generation firewalls and unified threat management. While others concede attackers will get in and are pivoting to detection and response, our focus remains on stopping attacks before they succeed. This focus is demonstrated in capabilities that include:

- CPU-level sandbox prevention which blocks attacks before they can begin their evasion techniques
- Threat Extraction which delivers safe and clean files to users thus protecting them from infection
- Anti-phishing which detects phishing attacks and blocks them before users can get infected
- Anti-Ransomware which detects and blocks ransomware attacks, and restores any files initially encrypted

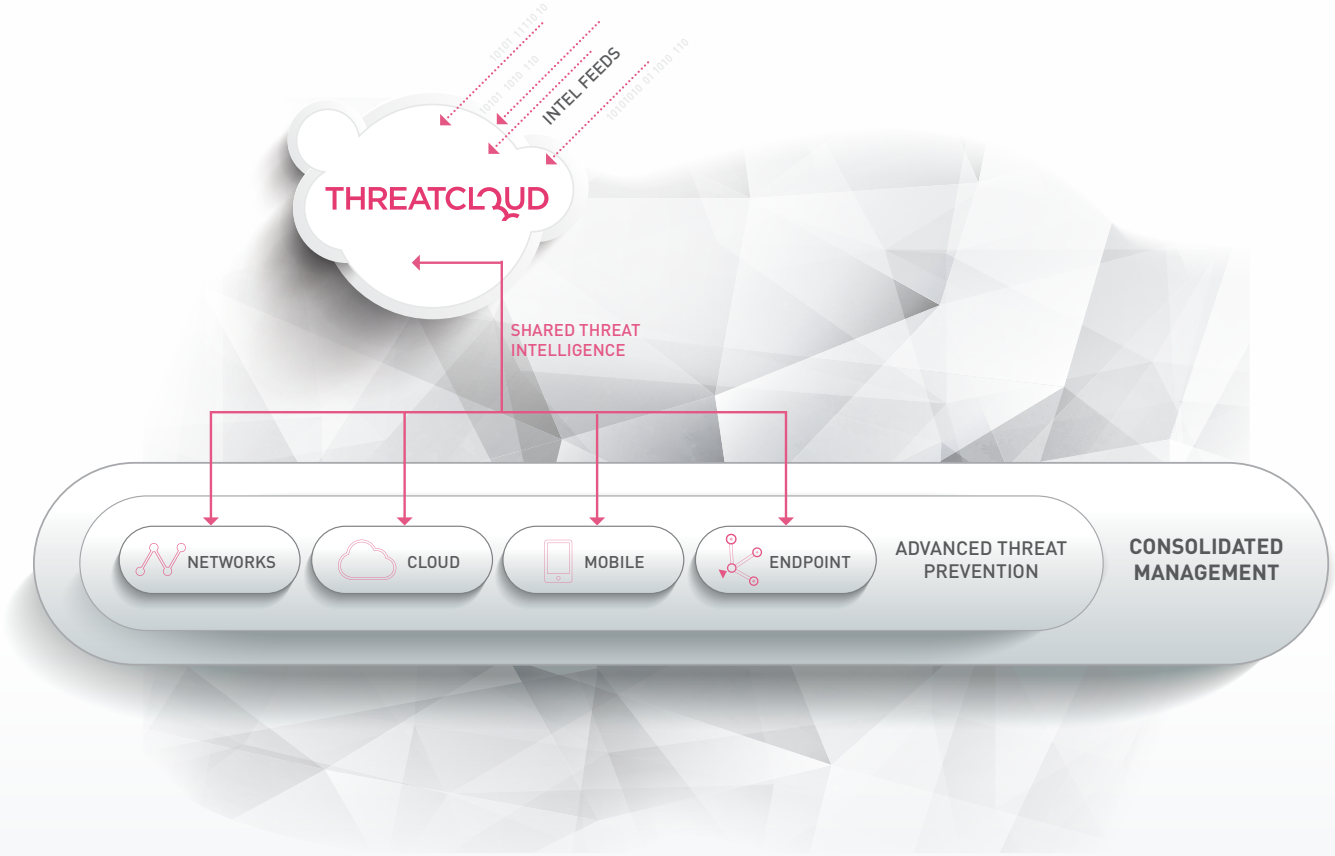
The further addition of threat intelligence across the architecture completes the picture, by ensuring that the



entire attack surface is protected consistently. Finally, open APIs allow Infinity to integrate into the broader IT infrastructure to share policy, identity, and event information. This integration is crucial to implementing business-oriented threat protection in an operationally viable manner, with full separation of duties, logging and compliance controls.

CHECK POINT INFINITY IN DETAIL

Let's drill down into Infinity's architecture, to better understand how it delivers threat prevention and policy enforcement. Infinity is comprised of three layers as shown below.



The layers work together to define the policy, translate the policy into enforcement rules, and then push those rules onto the enforcement points throughout the environment. Lastly, events and threat intelligence produced by the enforcement layer are consolidated and presented to the Security Operations team, analyzed for compliance control assurance, and fed into ThreatCloud to update all Check Point customer's threat prevention in real time.

CHECK POINT SECURITY POLICY MANAGEMENT

Check Point's policy management is designed to make it easy to translate business goals into security policies. It doesn't matter how good the security technology is if the policy required by the business can't be expressed in the management system. It is no longer sufficient to simply write static, network-based rules that have no mapping into what the business is actually trying to do or protect. Management must also consolidate the policy across network, cloud and mobile, rather than depending on Security Operations to manually align policy across multiple point solutions.

Check Point has long realized this necessity, both for effective threat prevention and access control, and also to minimize administration overhead. The management component of Infinity supports all of the following business-oriented dimensions (and many more) to deliver the industry's most complete offering.

ELEMENT	EXAMPLES
User or Group	Joe, Marketing Group, Summer Interns
Application	Twitter, Instagram
Data and Content	Credit Card Numbers, ABA Bank Routing
Target for Enforcement	Amazon AWS, VMware Cluster, Mobile

Name	Source	Destination	Services & Applications	Content	Action	Install On
Access to Internet according to Web control policy	InternalZone	Internet	Any	Any	Web Control	Policy Targets
DNS server should have access to	DNS Server	ExternalZone	domain-udp-Protocol-Signature... domain-tcp-Protocol-Signature-...	Any	Accept	Policy Targets
Block abuse/ high risk applications	Corporate LANs Branch Office LAN	Internet	Inappropriate Sites	Any	Drop Blocked Message - Access Control	Corporate-GW
HR can access to social network applications	HR	Internet	Facebook Twitter LinkedIn	Any	Inform Access Approval Once a day Per application/site	Policy Targets
All employees can access YouTube for work purposes	Corporate LANs Branch Office LAN	Internet	YouTube Vimeo	Any	Ask Company Policy Once a day Per application/site	BranchOffice

Unified policy in R80.x: Security Management based on business-oriented security policy, not IT constructs

MANAGEMENT DELEGATION AND AUDITING

The management layer supports delegated authority, with full administration auditing. This allows responsibility for security policy to be distributed to the people who are best in a position to judge what should be permitted. It also makes security more responsive to the needs of the business. Check Point management includes workflows and approvals for all policy changes. This capability is critical to ensure that the correct policies are implemented, outage-causing mistakes are avoided, and internal audit and compliance controls on administration activity are implemented.

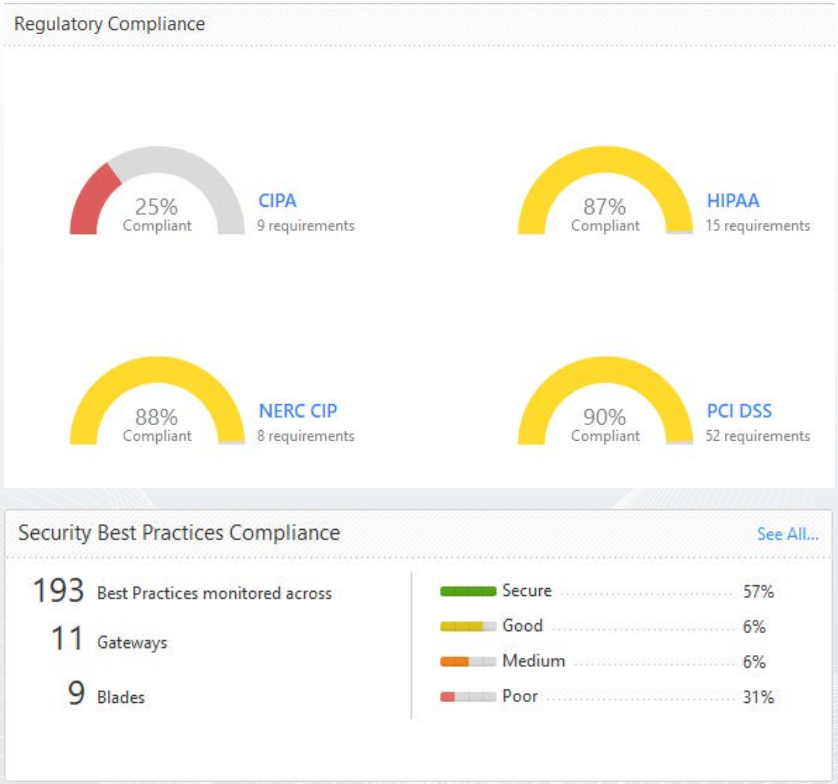
Modular management enables the definition of access and data control policies and the activation of threat prevention separately. The threat prevention policies can then be applied automatically to traffic allowed by the access and data control policies but could also be managed by separate people or even outsourced.

Example: Delegated Policy Management

The Marketing team is constantly needing access to new SaaS applications, as well as having to exchange information with an ever-changing list of contractors and agencies. They open piles of Help Desk tickets for access, which inevitably get delayed while the exact need and supporting approvals are clarified.

With Check Point Infinity, the Marketing Team can take responsibility for their own security policy. They can nominate one of their employees to act as the policy manager, and that person can update the policies for the Marketing Team and their data, but not the rest of the organization. All such activity can be audited by Security and Compliance for validation, while the Security team can still enforce key threat protections such as malware mitigation and data leakage prevention.

COMPLIANCE MANAGEMENT



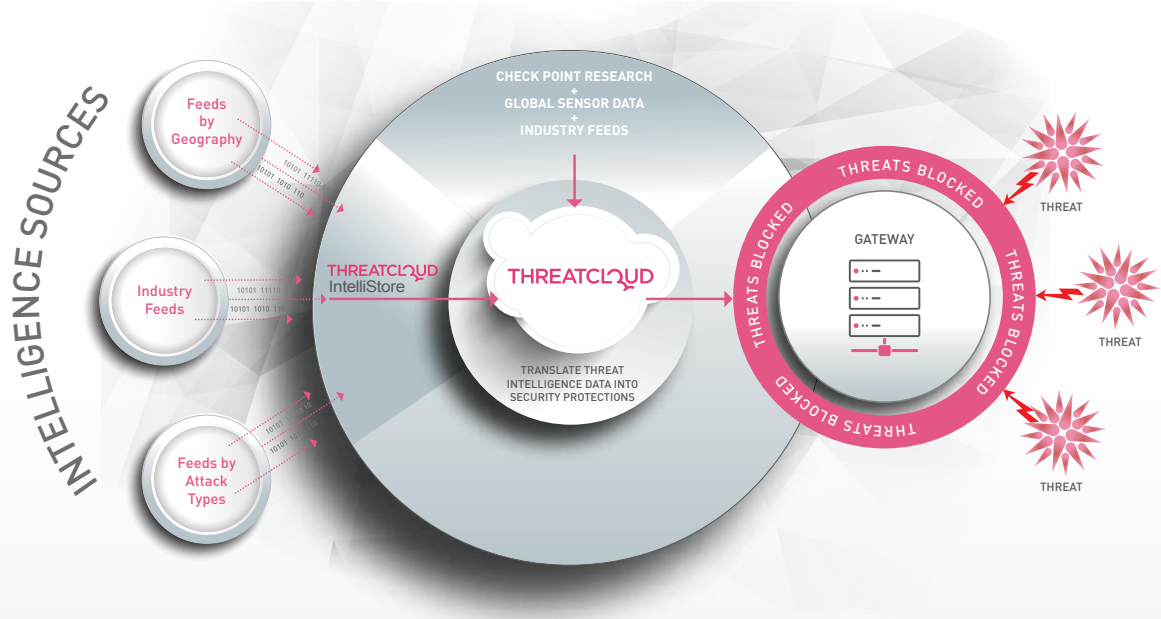
At-a-glance dashboard of compliance posture

Check Point Management includes an optional component to validate security configurations across the Infinity architecture. The Compliance Software Blade relies on a database of thousands of best practice configuration and compliance rules, and applies them across the architecture. Violations are flagged immediately, and recommended remediation actions are provided. A regulatory dashboard and supporting reports makes compliance validation and audits for standards such as PCI, ISO 27001, PCI DSS and GDPR a simple and painless exercise.

CONTROL AND THREAT INTELLIGENCE

Two core functions of the Infinity architecture are to distribute policy configured at the management layer to the enforcement points, and to derive and distribute automated threat intelligence and prevention updates. Crucially, the architecture is differentiated by its ability to distribute policy across network, mobile and cloud, deploying a unified protection profile across enterprise assets.

Infinity breaks down security silos by ensuring comprehensive and timely intelligence across the entire infrastructure. Check Point ThreatCloud houses all threat intelligence, which is derived from a broad array of sources: Check Point Research, sandboxing analysis, Incident Response, security gateway appliances, Computer Emergency Readiness Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs), security product vendors and other organizations within the security community.



ThreatCloud contains over 11 million malware signatures, 2.7 million malware-infested sites and over 5,500 different botnet communication patterns.* ThreatCloud is constantly updated with new threat information from a worldwide network of sensors, third party feeds, Check Point security researchers, security research organizations and Check Point gateways.

*As of Q3, 2017

The Infinity ThreatCloud platform combines and analyzes all of these sources of information, extracts new threat prevention protections, and dynamically pushes them to the enforcement protection points for immediate application. In this collaborative process, if one company is attacked with malware, the relevant attack information is instantly shared with ThreatCloud. A signature of the attack is added to the database, and is leveraged instantaneously by all other Check Point customers. This collaborative, dynamic and automated approach is the only realistic way to stay in front of today's fast moving threat landscape.

ThreatCloud in Action

Attack: A malicious email is sent to a company Office365 account, but blocked by Sandblast Cloud

Intelligence: ThreatCloud receives the incident of compromise (IOC) related to the attack, expands it to additional IOCs

Automated Distribution: ThreatCloud pushes updates across the Infinity Architecture

Protection: Related attacks via SMS and infected website are blocked

THREAT PREVENTION – PREVENT ATTACKS BEFORE THEY HAPPEN

One of the biggest challenges facing security practitioners is Gen V attacks – the combination of a wide breadth of threats, large scale attacks and a broad attack surface. True comprehensive protection requires an architected approach that prevents attacks before they happen. Ultimately, the goal is to defeat all attacks across all possible vectors. A security architecture that enables and facilitates a unified and cohesive protection infrastructure is going to provide more comprehensive and faster protection than an infrastructure comprised of pieces that don't work together. This is the heart of what Check Point Infinity delivers – a security architecture to prevent attacks before they happen. Let's take a closer look at the "tip of the spear" – the Infinity threat prevention capabilities.

1. Known Threats

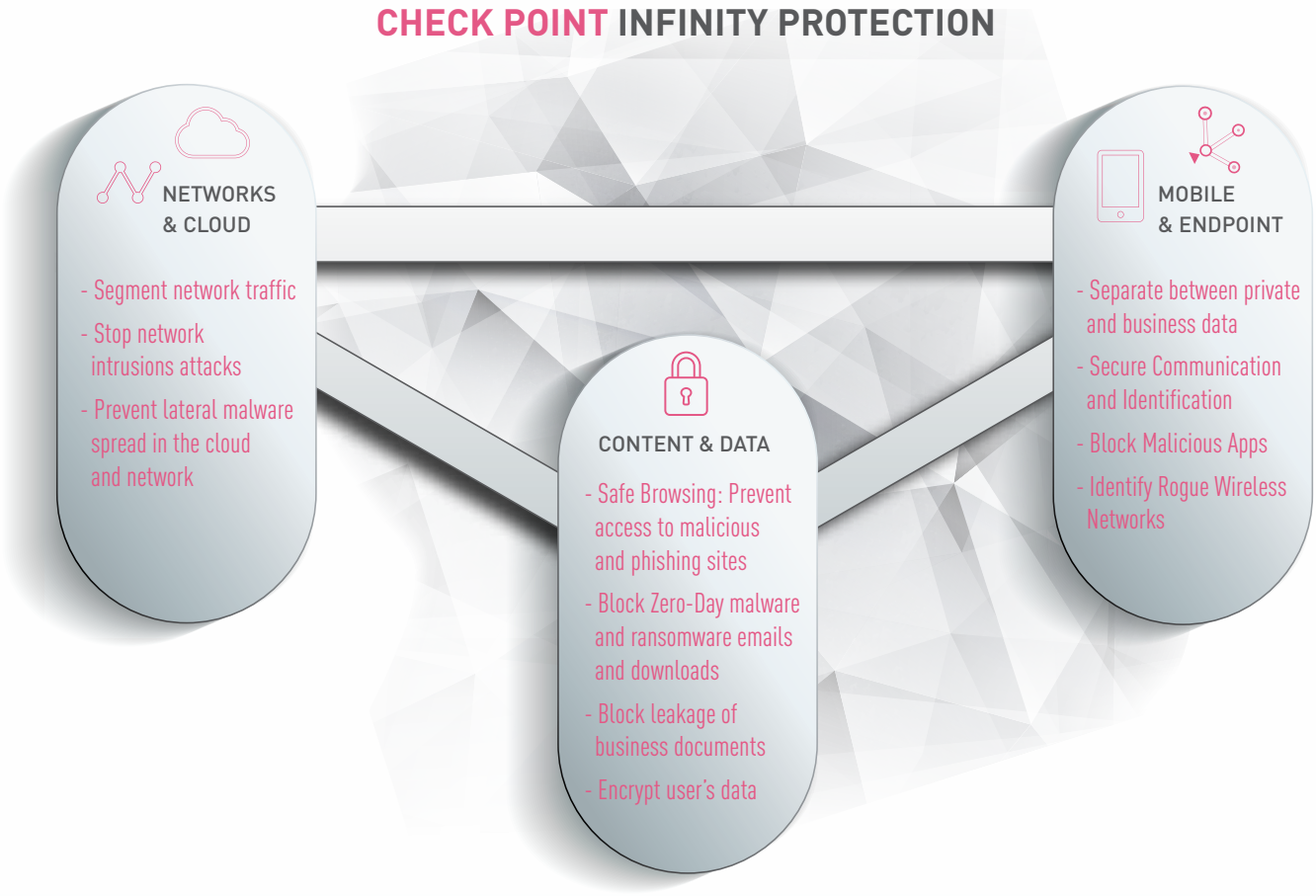
The majority of attacks being hurled at your network right now are known attacks. Known attacks are previously detected, analyzed and have a defined set of attack indicators and associated details. Prevention of known attacks is essential to any IT security plan and system. Infinity provides the foundation and capabilities to protect against known attacks with network-based threat prevention in every security gateway fed by the attack intelligence in Check Point ThreatCloud. Specifically, Check Point Infinity prevention against known attacks is led by industry best intrusion prevention to prevent known exploits against known vulnerabilities, anti-virus to prevent known bad files and URLs, and post-infection BOT capabilities to block outbound connections to known Command and Control destinations. At some point, all attacks attempt to traverse your network and Infinity network-based protection will block them – at multiple points in the cyber kill chain.

2. Advanced and Unknown Threats

While far, far fewer in number, it is the unknown attacks – especially the attacks specifically customized to target your business – that cause us the most worry. Unknown threats often go undetected longer, thus causing more damage. This is where many homegrown security infrastructures will fail – adding standalone, best of breed protection against unknown and advanced attacks. To combat the threat, instantly sharing fresh intelligence about previously unknown and targeted zero-day attacks with the rest of your security infrastructure is essential. Check Point Infinity prevents unknown and targeted advanced threats as an integrated and cohesive part of its overarching security architecture. Led by the Check Point SandBlast product family, SandBlast provides an advanced set of protection including over 30 different innovative technologies that deliver capabilities to detect and prevent previously unknown, zero-day and targeted attacks across all parts of your IT infrastructure. And it is important to restate – instantly sharing indicators of just detected unknown and zero-day attacks with the rest of your security infrastructure is key to preventing attacks before they happen – and is exactly what Check Point Infinity does.

3. Preemptive Protection

If you could preemptively protect your business from cyber-attacks without impacting daily operations, would you? Innovative capabilities in Check Point Infinity allow you to do just that – preemptively protect against attacks without impacting daily operations. For example, SandBlast Threat Extraction sanitizes all malware



Infinity advanced threat Prevention delivers the broadest capabilities available in a unified architecture

from files that your end-users download from the Internet and receive in email – before they can open them and be infected. Consider the value of this capability for a moment – all files downloaded from the internet and received in email by all your end users are delivered clean, without impacting operations.

4. Endpoints

We all know that endpoints are both the repository for valuable corporate information, and are the most common cyber threat target. Yet the natural evolution of security technology isolated endpoint protection from network protection. For many years this artificial wall impeded advancement of a better unified and cohesive IT security and response – until now. Check Point Infinity not only protects the endpoint but also enables intelligence sharing and forensics with data and insights that that can only come from the endpoint. Specifically, the innovative and preemptive capabilities mentioned earlier in the Check Point SandBlast Agent prevent attacks from bad files and URLs and deliver post-infection BOT prevention and sandboxing to block unknown and zero-day attacks – plus anti-ransomware. This unique and innovative capability is both timely and extremely effective at detecting and blocking ransomware activity and restoring the affected files. As of this writing, Check Point Anti-Ransomware technology prevented both recent headline ransomware attacks – WannaCry and NotPetya. And via Check Point ThreatCloud, all threat intelligence is instantly shared to and from SandBlast Agent to prevent attacks before they happen on your endpoints and across your entire security infrastructure.

5. Mobile

Mobile devices are part of the IT fabric and business operations everywhere. Every one of us can connect to our employer's network and access any number of applications and proprietary information from our mobile devices while sitting anywhere in the world. A rule of thumb in security is to deploy the level of protection according to the value of the asset being protected. Unfortunately in most businesses, mobile devices are not secured anywhere nearly proportionate to the value of the assets that can be accessed through them. Now that is a threat vector to worry about! Again, as a security architecture, Check Point Infinity extends its core threat prevention capabilities to mobile devices to prevent attacks before they happen. Specifically, Check Point SandBlast Mobile provides advanced threat prevention to prevent varied attacks on iOS and Android devices: OS-level, rogue apps and attacks targeted at apps, and network-based such as "man-in-the-middle" (MiTM) techniques. As with all components of Check Point Infinity, SandBlast Mobile receives and shares threat intelligence through ThreatCloud to ensure the most comprehensive and timely security across your entire IT infrastructure.

6. Cloud

It's no secret that one of today's most business-altering technologies is the cloud. Appealing on many fronts in particular operational flexibility and cost savings, cloud deployments – either SaaS-based, public, private or hybrid – must be secured against all the same threats in all the ways we've talked about so far. This is yet another strength and benefit of Check Point Infinity architecture. The CloudGuard cloud security family provides consistent and comprehensive cloud security for virtualized datacenters to SDN, IaaS and SaaS applications, including the emerging threat of account takeover. The CloudGuard portfolio includes CloudGuard SaaS and CloudGuard IaaS, and seamlessly integrates with the largest number of cloud platforms and cloud-based applications.

7. Future-Proof

To fully understand the value of Check Point Infinity now and into the future, it is important to understand that Check Point is intensely focused on building products that will prevent attacks before they happen. As this whitepaper shows, Check Point Infinity is comprised of a core set of innovative and leading prevention technologies, intelligence sharing and management across all key IT platforms being used today. And we will extend the same capabilities to whatever new IT platforms and technologies are developed tomorrow – to continue preventing attacks before they happen.

The Future with Check Point Infinity

To fully understand the value of Check Point Infinity now and into the future, it is important to understand that Check Point is intensely focused on building products that will prevent attacks before they happen.

EVENT MANAGEMENT

Security management is a never ending process: Policies are defined, implemented, monitored, and updated continuously. Most organizations struggle to adequately monitor their multitude of point solutions, and update policy based on events. Check Point Infinity on the other hand combines the power of the management and unified platform to deliver this continuous security lifecycle.

The starting point for monitoring is event collection. Unlike most security products that just throw events up to a SIEM and hope something good comes of it, Check Point's architecture includes the SmartEvent component. SmartEvent performs real-time security event correlation and big data analysis. It collects, consolidates and correlates events from enforcement points deployed in the network.It then offers the ability to provide a consolidated and correlated view of incidents based on multiple sources of information. An accurate event view is provided and helps incident responders identify the necessary actions to be taken in order to defend the organization. Incident responders are provided with real-time visualization of the chain of events, which allows identification of initial attack vectors as well as subsequently subverted hosts and compromised data.

R80.x SmartEvent dashboard consolidates security events and speeds incident response

SmartEvent then goes even further, and automates threat prevention updates. An investigation can generate new threat indicators for malware, threat behavior and network addresses associated with each identified attack. These indicators are then fed automatically to the ThreatCloud platform and distributed from there to the Enforcement Layer in order to protect the organization with real-time blocking.

This closed loop aspect of Infinity is a key advantage. It eliminates the need for the Security Team to architect and manage what should be a unified, automated process. This improves security posture, and frees up resources for high-value tasks such as incident response and policy oversight.

TECHNOLOGY INTEGRATION AND APIs

The Infinity architecture does not exist in a vacuum. It must support automated integration with the organization's broader IT environment for several reasons:

- **Speed and Agility:** IT is under pressure to be more responsive to the needs of the business, and this includes security. By moving from trouble tickets and manual activities to automated processes, security services and policies can be quickly applied where needed, eliminating bottlenecks to application deployment or access.
- **Improved Threat Response and Incident Response:** Security inevitably includes multiple systems and information sources (e.g. identity stores, asset inventories, event management) that must work in concert to deliver threat protection. In the case of Incident Response, analysts must gather information from multiple sources as efficiently as possible in order to determine the appropriate response. The more these interactions are automated, the more timely the updates to threat prevention.
- **Policy Accuracy:** Very often security breakdowns occur because a manual process is improperly executed, or not done at all. Automation replaces unreliable manual steps, improving policy accuracy. Automation of compliance controls also reduces the effort to respond to audits, and lowers the chances of audit findings.
- **Delegation:** For both enterprises and service providers, some level of policy control needs to be delegated to those in the best position to make the decision. Service providers may want to push day to day access control decisions to their customer's staff, while enterprise security teams may want to delegate such decisions to the relevant lines of business. API-based integrations enable these use cases, while retaining a full audit trail of activity.

Infinity includes a rich set of APIs that support these goals, and these APIs are used by Check Point's technology partners to develop integrated solutions. Both RESTful APIs and command line access are available. A wide range of applications are possible with the APIs, but sample use cases include:

- **Cloud Based Data Centers (IaaS(and Virtualization:** As applications are increasing deployed using automation or DevOps methodologies, security must also be automated to avoid being a bottleneck. To this end, Check Point's APIs support automated deployment of software gateways and policy instantiation. This includes zero-touch provisioning for OpenStack, Amazon AWS, VMware NSX, and more. Check Point has also integrated with Office 365 for seamless application of threat prevention to incoming email objects.

Check Point Infinity in the Software-Defined Datacenter

The dynamic nature of today's software-defined data center makes traditional methods of security management based on static rules obsolete. To overcome this challenge, Check Point has partnered with VMware to integrate Infinity with VMware's software defined datacenter (SDDC) stack. The integration automates security so that virtual servers are protected dynamically based on pre-defined policies. This enables organizations to protect the data center without inhibiting the agility demanded by the business.

Check Point's integration with VMware SDDC and NSX supports both the placement of gateways, and the security policies applied on them. So for example if the VMware team adds a server to their cluster and moves virtual applications onto it, Infinity automatically spins up a new virtual gateway (CloudGuard IaaS) instance on that server. It then applies security policies on that gateway to protect the virtual applications migrated to the new server. This "microsegmentation" strategy inserts security immediately adjacent to the protected assets, where effectiveness is maximized. Infinity can even notify NSX when a server appears to be infected, so that the VMware team can implement either manual or automated remediation actions.

- **Cloud Applications (SaaS):** Check Point has also integrated with SAAS application to prevent account takeovers by blocking access of unauthorized users and compromised devices and preventing threats and data leaks in SaaS applications such as Office 365 Email, OneDrive & SharePoint, G Suite, Box, ServiceNow and many more.
- **Object and Rule Table Updates:** The most common administrative tasks are changes to membership of object groups, or changes to the rule table. Automating these tasks both frees up significant staff time and decreases the change of mistakes due to human error.
- **Threat Prevention:** The application of threat protections based on incident response or 3rd party policy. This includes sharing identity awareness with the infrastructure to support identity-based policies, for example with Cisco ISE, ACI and TrustSec.
- **Self-Service:** The provision of customer or line-of-business portals for delegation to relevant staff who are informed and empowered for policy decisions for their organization.
- **Incident Response Ticket Enrichment:** The data mining of Check Point logs for entries relevant to a person or system of interest to automate IR investigation.

To support our customer's efforts to use our APIs, Check Point hosts Checkmates, our user community. Community members can ask questions, interact with their peers, share code, and collaborate with Check Point R&D. The section dedicated to API developers can be accessed here.

Check Point's goal is to ensure that any activity or data retrieval process in the Infinity architecture which can be done manually can also be performed programmatically through reliable, audited APIs. This commitment to automation elevates Infinity from simply a security infrastructure to a business enabler that remains relevant and viable as applications transition to dynamic, cloud-native architectures.

GETTING STARTED WITH THE INFINITY ARCHITECTURE

The implementation of any architecture requires a methodology that accounts for the operational realities and business goals of the organization. Let's see how Infinity could be applied in practice in a phased approach that accelerates time to value while minimizing risk.

1. Risk Assessment

The core goal of IT security is to lower business risk. Therefore, any new security

initiatives should start with a risk assessment. This is a two-step process:

a. What risks are we trying to minimize? Production downtime, loss of intellectual property, damage to reputation, failure to meet regulatory requirements? What weighting do we assign to each one? These are difficult choices that must involve the leadership of the organization, who may not always want to go "on the record" making these decisions. This is a purely business oriented discussion; there should be no IT technology introduced at this point. The output should at least include a list of risks, a relative weighting of importance, and a discussion of the process and people used to arrive at the output, to avoid second-guessing.

b. What is our current level of risk exposure to each of the risk types identified? This can be approached by first identifying the IT and data assets that are relevant to each risk type, and then evaluating how each asset may be compromised.

2. Understand Current Security Posture

The next step is to evaluate what security systems and processes you have. This requires a realistic evaluation of what is in place, which sounds simple but can be challenging in practice. A common pitfall to avoid is relying entirely on the security staff to do the evaluation. The Security team may simply not be able to provide an objective view of how the posture is constructed. They may not want to reveal their shortcomings, or may at least play down the exposure. They may also have their own axes to grind: systems they want but didn't get budgeted, or people or teams they don't trust or communicate well with. And lastly, they may not be in the best position to evaluate the human element: What is the impact of end-user and IT administrator behavior on the security posture? Whatever the reasons, it is important to get non-security people involved in the process to keep it as objective and broad as possible.

3. Understand Business and IT Goals

The third step is to look forward: What are the future projects, strategies, and execution constraints that will affect the security architecture? Are acquisitions likely? Will new locations open or is consolidation the way forward? Will IoT projects create new risks to production availability that do not exist today? Will we be subject to new data privacy regulations such as GDPR? And what is the attitude towards IT cloud migration and outsourcing (MSP/MSSP)? Usually these decisions are taken at a business, not technical level, and are critical to planning.

4. Define and Build Future Security Architecture

Only after the first three steps are taken can the organization turn towards the actual task of building the architecture. We suggest trying to proceed on dual tracks: strategic and tactical. At a strategic level, it is important to be realistic: What solutions can the organization realistically implement given staffing, budgets and executive attitude towards risk? Can you get the necessary time, support and patience to implement strategies that might take two years to fully implement? However, don't overly focus on strategy, because there may be key risks identified that need faster remediation. Look for tactical quick wins that will help justify and validate the entire effort.

It is also important to leverage existing cyber-frameworks when setting goals for improving security posture. Examples such as NIST, PCI, and SANS establish a solid initial framework of controls to be evaluated against the risks established in prior steps. They are also a great way to decrease the risk that organizational biases will de-focus the effort.

SUMMARY

Depending on your view, IT operations and security is in the midst of a major disruptive period, or undergoing a tremendous renaissance. Regardless of how you see it, as an IT security professional, you are under tremendous pressure to increase the efficiency and effectiveness of your IT business operations. You are likely trying to solve risk management problems related to technology sprawl and infrastructure diversity, while trying to meet demands for agile and flexible services for customers and end-users. And you must deliver these services securely and at scale. A thoughtful plan built upon an architecture that can meet these operational demands while providing cohesive control, service elasticity and extensibility to meet future needs can deliver renaissance, and not disruption, to your business.

Check Point Infinity is the architecture upon which you can build a new IT security system. Infinity is the only fully consolidated cyber security architecture that protects your business and IT infrastructure against Gen V mega cyberattacks across all networks, endpoint, cloud and mobile. It provides the highest level of threat prevention against both known and unknown targeted attacks to keep you protected now and in the future. It is important to understand that Check Point Infinity is not "marketecture". Check Point Infinity is the culmination of our overarching vision to build a security architecture that unifies the best security, the best intelligence, and the best management across your entire IT infrastructure. Check Point R80 is the product version that brings together the security, intelligence and management capabilities to meet the many and varied IT security demands of today. While R80 is a product version, the entire, unique set of capabilities is much more than a single product. They set the foundation for you to design and deploy a cohesive security infrastructure, a single system in fact, that will meet your security requirements now, yet is also extensible to meet your changing requirements in the future. Together these capabilities form an architecture and that architecture requires a name, which is Check Point Infinity.

1. Protection

Check Point believes in a preemptive security strategy, focused on real-time prevention rather than detection only. Our goal is to block attacks before they succeed. Check Point Infinity extends our multiple security layers from signature-based detection to the advanced prevention capabilities of the SandBlast family of products across your entire IT infrastructure of network, cloud instances and mobile devices for consistent, effective threat prevention.

2. Intelligence

Comprehensive and timely threat intelligence delivered simultaneously to all of your enforcement points is essential to preventing attacks before they occur. Check Point Infinity delivers threat intelligence across all your enforcement points. Through Check Point ThreatCloud, all enforcement points in your network, endpoint, cloud and mobile are armed with threat intelligence derived from multiple external feeds, internal research, and indicators from Check Point customers around the world, including indicators from just-detected unknown and zero-day attacks from Check Point Sandblast sandbox analytics.

3. Management

Check Point is the recognized leader in security management. We know that better management means better security. The Infinity architecture consolidates management of multiple security layers based on your business-oriented security policy and gives your team a centralized view of all activity across your environment: from policy management to monitoring, response, compliance and more.

Think about it: To have a single, cohesive security system across all your enforcement points, bolstered with comprehensive and timely threat intelligence, driven by unified management across your entire IT infrastructure of network, endpoint, cloud and mobile. Check Point Infinity delivers all this, and gives you the protection, flexibility and control you need to manage today's and future IT disruption, and turn it into a renaissance for your business.