CHECK POINT INFINITY

The Cyber Security Architecture of the Future

Next Generation Threat Prevention Platforms

Check Point
SOFTWARE TECHNOLOGIES LTD

Learn More: checkpoint.com

EXECUTIVE SUMMARY

In this age of digital transformation, the world uses technology in new and exciting ways. For example, Internet of Things (IoT) devices are quickly going online in enterprise networks. At the same time, digital assets that used to be contained within enterprise security perimeters are now moving outside the safety of corporate controls as users become increasingly mobile. In addition applications, data and networks are moving to the cloud, exposing organizations to new and more sophisticated threats.

Separate security products for network, endpoint, cloud, mobile, and Everything-as-a-Service each focus on small elements within this new and evolving digital landscape, but they do not work together for better security. Nor do they give you a view of the bigger, more important picture.

Check Point Infinity Cyber Security Architecture

Check Point continuous innovation of cyber security technology delivers the most advanced threat prevention to our customers. Check Point Infinity is the first consolidated cyber-security platform, designed to future-proof businesses and IT infrastructures across all networks, cloud and mobile. This overarching platform enables businesses to prevent potential attacks with its multiple layers of advanced threat prevention which seal the gaps caused by the use of multiple unintegrated point solutions. Check Point Infinity is purpose-built to reduce the complexities caused by using disparate systems, having poor visibility into different cyber security silos, as well as challenges due to dynamic changes to the business/enterprise, such as expanding into multiple locations using new and more sophisticated technologies.

Check Point Infinity delivers a unified set of security functions across all parts of the IT infrastructure. All Check Point components, networks, cloud and mobile environments share the same threat intelligence, set of interfaces and APIs to enable consistent security and operations across all networks.

Focused on prevention rather than detection and mitigation, it introduces multi-layered cyber security capabilities that preemptively protect against the most sophisticated known and unknown threats, by preventing the damage before it happens. Check Point's advanced protections are led by the SandBlast product family with over 30 different innovative technologies that provide consistent zero-day protection across networks, cloud and mobile.

Check Point Infinity consolidated security management enables security admins to centrally manage and correlate all types of events across all network environments, cloud services and endpoint devices using a single console, providing unparalleled threat visibility and control.

This document describes how Check Point Next Generation Threat Prevention (NGTP) platforms fulfill the Check Point Infinity goal of keeping businesses protected against any threat, anytime and anywhere by providing threat visibility, shared intelligence and consistent cyber security controls across platforms, locations, and evolving technologies.

THE RATIONALE FOR ADVANCED THREAT PREVENTION

While our environments are becoming more complex, attacks are also growing in sophistication. We live in a world where security researchers see 99 percent of malware hashes for 58 seconds or less.[1] This means cyber security technology solely based on known malware signatures is woefully ineffective. Now more than ever, organizations must utilize more advanced techniques like virtual sandboxes to detect and detonate unknown threats. Additionally, Gartner predicts that by 2018 "85 percent of new deals for network sandboxing functionality will be packaged with network firewall and content security platforms."[2]

Closing the security gaps associated with sophisticated, unknown threats requires a combination of innovative technology for preventing threats in real-time coupled with an architecture that scales across multiple environments. Ultimately, it is a better choice to invest in technology that automatically prevents threats in real-time instead of investing capital to manually investigate each threat.

Regardless of the rapid changes shaping IT infrastructure and threats, the goal of network security should remain constant; to prevent threats at scale across multiple simultaneous sessions without introducing latency. Check Point NGTP platforms addresses these challenges using a focused, context-aware approach on optimized x86-based physical and virtual appliances. Check Point also leverages a collaborative global network and cloud-driven knowledge base to identify emerging outbreaks and threat trends. The output from this analysis is dynamic, real-time security intelligence updates delivered to every Check Point Network, Cloud and Mobile device.

The key aspects of this innovative approach to prevention include:

- **Focused, Context-aware Inspection**: By focusing on the relevant content for any given connection, Check Point NGTP platforms eliminate wasted processing, thus reducing latency. For example a layer 3 check of the IP and port helps NGTP make decisions quickly. When content inspection is needed, our protocol-parsing engine dissects the session into various contexts such as URL, domain name, or file checksum used by signatures. With our focused context-aware inspection, we quickly determine whether or not to allow the session. Security is applied at every layer while networking, policy lookup, protocol decoding, and content security are performed only once.
- **Concurrent Processing**: We optimized our NGTP platforms to run on x86-based multicore processors, where multiple sessions are processed simultaneously. 64-bit support provides high connection capacity. Multicore capabilities provide near-linear scalability on each additional core. Porting our NGTP security software to other environments is quick and easy due to the availability of x86 architectures on physical and virtual platforms. This supports deployments both on premises and in public or private clouds. Furthermore, additional processing cores can be added to Check Point appliances using dedicated acceleration network interface cards.

As a result, Check Point is able to deliver a network security software architecture that for the first time offers true threat prevention, not just threat detection. It does this without delay in one session, scales across multiple sessions, and is agile enough to deploy where you need security on premises and in the cloud.

BENEFITS OF INTEGRATED THREAT PREVENTION

When architected properly, integrated security provides significant benefits. Check Point's integrated approach minimizes configuration errors and prevents modern zero-day attacks. In addition, this approach offers the following benefits:

- **Shared Resources:** Shared resources minimize the need for processing. For example, HTTPS inspection can be performed once. Before emulating objects in the sandbox environment, static analysis is performed on the gateway minimizing the number of objects to be emulated.
- **Operational Efficiency:** When your network security device prevents threats (not just detects them) in real-time, this saves valuable IT staff time since there is no need for staffers to identify, isolate and clean infected systems.
- **Increased Visibility:** Collecting all security events in a central location streamlines monitoring, reporting and forensics. Including incidents from all network, cloud and mobile devices provides a total picture and timeline of threats.

The x86 Advantage

Check Point works closely with major chip vendors to optimize our software to take advantage of the latest advances in chip technology. Leveraging x86 architectures provide several advantages:

- **Security Portability:** Our security seamlessly adapts to any network environment. In particular, most public and private cloud platforms are also x86-based so porting our software to those platforms has been relatively easy.
- **Faster Development Time**: x86 processors provide ready access to a well-established ecosystem of software and hardware developers. Check Point maintains considerable investment in research and development compared to other security vendors. This commitment lets us develop new software technology relatively quickly compared to other vendors.
- **More Granular, Feature-rich Products**: Check Point leads in innovation across several key security capabilities. This lets us offer the industry's broadest support of applications available in our Application Control database, CVE coverage, and the number of data types available in our Data Loss Prevention policy. This is in large part due to the flexibility of the x86 architecture, which is not as restrictive as fixed-instruction set systems.
- **Better Performance Through Software Optimization**: Intel continually pushes development for higher performing and more feature-integrated processors. Likewise, Check Point optimizes our software to take advantage of improvements on these platforms. Customers benefit by simply upgrading to the latest software version.

Optimized, Concurrent Processing

How does a computing architecture that processes one instruction at a time compete with purpose-built ASIC and FPGA systems? The answer can be summed up in 3 words: optimized, concurrent processing. In practical terms this means reducing wait states, improving process efficiency, and distributing processing to additional processing cores.

- **Optimized**: Over the years, we've made our software more efficient in several areas. For example, we added SecureXL capabilities to accelerate packet throughput and connection rates instead of running every packet through the firewall. We utilize a common parsing engine that extracts only the content that needs to be inspected from a session stream. Content security signatures are preloaded into a common pattern matcher to optimize content security inspection. In addition we take advantage of fast memory caches where possible to ensure process doesn't have to wait for data to be retrieved from slower memory or from a disk.
- **Concurrent Processing**: As chip manufacturers have added physical and logical cores (Hyper-threading) to their CPUs, we've added support for multi-core systems and simultaneous multi-threading. These advances have resulted in nearly 100% and 30% performance improvements per core respectively. In addition, our latest appliances have the option of offloading processing to dedicated I/O acceleration cards which further increases performance while reducing latency.

CHECK POINT NGTP SOFTWARE ARCHITECTURE

Let's examine the components that make up the software architecture for NGTP, which applies security at every layer and performs networking, policy lookup, protocol decoding, and content security only once.

- **Network Security:** A key building block for network segmentation, our accelerated firewall processing delivers high performance and reduces the latency of packets passing through the security gateway. We do this by directing most traffic through an optimized path.
- **Multi-purpose Streaming**: For content security, we assemble packets into a stream and use passive or active streaming depending on which provides the best overall security. The streaming engines prevent retransmissions with modified data or TCP connection packets with no handshakes and decrypt HTTPS traffic so that it can be inspected.

- **Protocol Parser:** Internet traffic is composed of well-known protocols. We parse session streams into relevant contexts such as URLs, DNS host, and files. The content is normalized before inspection to thwart attempts to evade detection. The protocol parser detects and prevents protocol anomalies.
- **Content Security:** When enabling advanced security features like Application Control, URL Filtering, Content Awareness, IPS, Anti-Bot, Antivirus and SandBlast Threat Emulation (sandboxing); the security gateway inspects content using the contexts derived from the protocol parser. The gateway's local cache is augmented with real-time cloud updates and zero-day threat protection.

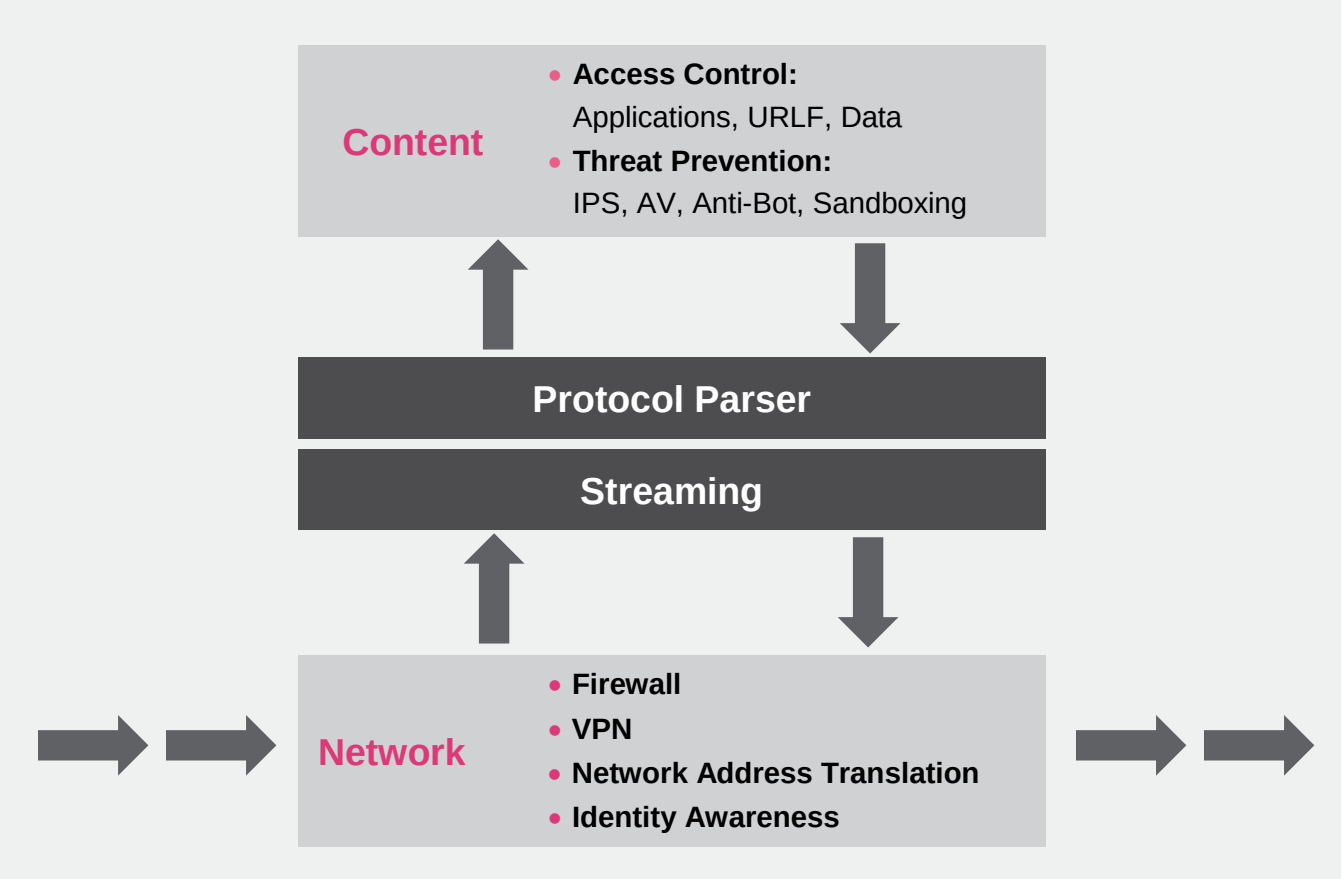

Figure 1: Packet flow in the NGTP Software Architecture

Network Security: A Strong Foundation

The stateful-inspection firewall is a core component of the Check Point NGTP platform. A stateful firewall tracks the state of network connections in memory. It does this to identify other packets belonging to the same connection and to dynamically open connections that belong to the same session. Allowing FTP data connections using the information in the control connection is one such example. The firewall dynamically recognizes that the FTP control connection is opening a separate data connection to transfer data.

While IP and port-based inspection is insufficient for providing outbound application control, it remains useful for inbound inspection and network segmentation where you can apply the principle of least privilege: only allowing access that is necessary for a legitimate purpose. This means that a decision based upon IP and port is made quickly, which reduces latency. At the same time you protect your network from reconnaissance, the first step in the cyber-kill chain.[3]

Accelerated, Concurrent Processing

On a multi-core system, the firewall kernel is replicated multiple times. Each replicated copy, or firewall instance, runs on one processing core. These firewall instances handle traffic concurrently. Each firewall instance is a complete and independent firewall inspection kernel.

The SecureXL device and the firewall module enforce security policy based on source, destination and port information. In Check Point documentation you will hear about three paths; Fast, Slow and Medium. Fast Path refers to SecureXL. Slow Path refers to the firewall module. Medium Path refers to content-security inspection where packets are received directly from the SecureXL device.

We have discussed how multiple firewall instances run on separate cores in a multi-core system and how many instances can run in parallel. In the Check Point architecture, content security inspection runs in a monolithic part of the firewall kernel. When content security inspection is needed, packets can be received from the SecureXL device or from the firewall module. Receiving packets directly from the SecureXL device uses less CPU resources, thus the name medium path.

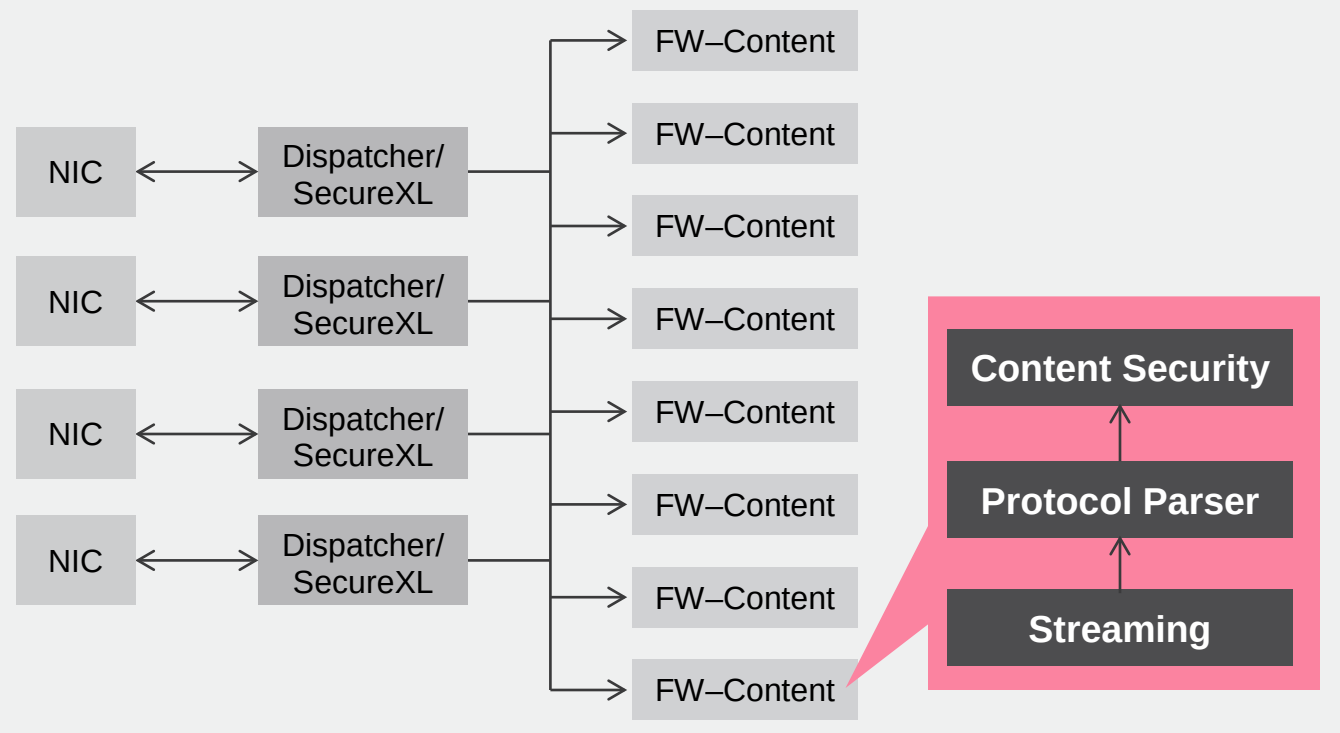

Figure 2: Accelerated concurrent processing

Multi-purpose Streaming Enables Prevention

Streaming serves an important function in the NGTP software architecture. The streaming process creates an ordered packet stream and directly performs a number of security functions on the stream. NGTP can assemble packets into a stream in two ways, passive or active, depending on the nature of the traffic. Each has advantages and disadvantages.

The passive mode gives little opportunity for modifying the traffic stream. In contrast, the active mode can modify the connection. Active mode essentially proxies the TCP connection and is necessary when performing HTTPS inspection. Active streaming also facilitates timing and buffering when inspecting content such as large files.

Keeping the goals of integrated, high security effectiveness and performance in mind, Check Point chose to provide the option to do passive and active streaming, which provides the best balance of security and optimized performance based on actual usage conditions.

Protocol Parser: Finding the Needle in the Haystack

Finding malware in a network session can be like finding a needle in a haystack. To improve detection, we parse the stream into protocol contexts. Protocols include HTTP, SMTP, DNS, IMAP, Citrix, and many others. The protocol parser picks apart a session stream to determine what the different pieces are. For example, where does a file transfer start and stop, what is the file type, when is the user posting data versus downloading data, when is a command being executed. All of this information is context that is used for scanning the content for files, data, threats, and URLs. By performing focused content scanning on the relevant parts of the stream, we save significant processing power.

Protocol parsers test for conformity to RFCs and look for anomalies. Another job of the parsers is to normalize content. For instance, characters within a URL like an uppercase “A” may be encoded as %41. The parser will normalize this content before passing the URL to the protections for inspection. Normalization before inspection thwarts attempts by threats to evade detection.

Applying the Content Security Policy

When advanced security features are enabled such as Application Control, URL Filtering, Content Awareness, IPS, Anti-Bot, Antivirus and SandBlast Threat Emulation (sandboxing), the security gateway performs content inspection using the contexts derived from the protocol parser.

During policy installation, signatures are compiled into Pattern Matchers (PM) with one PM for each context such as URL, Host header etc. The PM quickly identifies harmless packets, common signatures in malicious packets, and if needed, does a second-level analysis to reduce false positives. The engine uses a two-tiered inspection process.

The first tier quickly filters out the vast majority of traffic, which is clearly harmless, by looking for signatures that are simple to find at a low CPU cost. If the first tier identifies a common attack signature, it passes the connection to the second tier to do a second level analysis. This increases confidence there is indeed an attack.

It is worth noting that in some cases, the determination is a simple comparison. For instance, minimal processing time is needed to check an IP, a URL, a domain, or a file checksum against a known list. These comparisons are done first.

Real-Time Cloud Assist

After a match, additional processing is done as needed by the security application. This is done by checking a local cache, and when needed, our cloud service updates the cache in real-time. For instance:

- **Application Control** retrieves all the data regarding the application (its categories, priority, etc.) from a cache based on the signature that was matched. If a match is not found or social-network widget detection is needed, then the online cloud service is checked and the cache is updated with the result.
- **URL Filtering** checks for the URL category in the local cache. If not found, then the online cloud service is checked. The cache is then updated with the result.
- **Threat Emulation** is a special case where the Pattern Matcher can be bypassed. If the checksum of a file is not cached, then the sandbox needs to receive a complete file. The protocol parser extracts the file and sends the file to our cloud service for processing where compute, disk and memory are virtually unlimited. If the protocol requires immediate delivery as in the case of HTTP/S, we offer user agents to notify the user and deliver only safe content to the user while the emulation happens in the background. Newly discovered threats are added to the local cache and sent to the cloud database to protect other Check Point platforms.

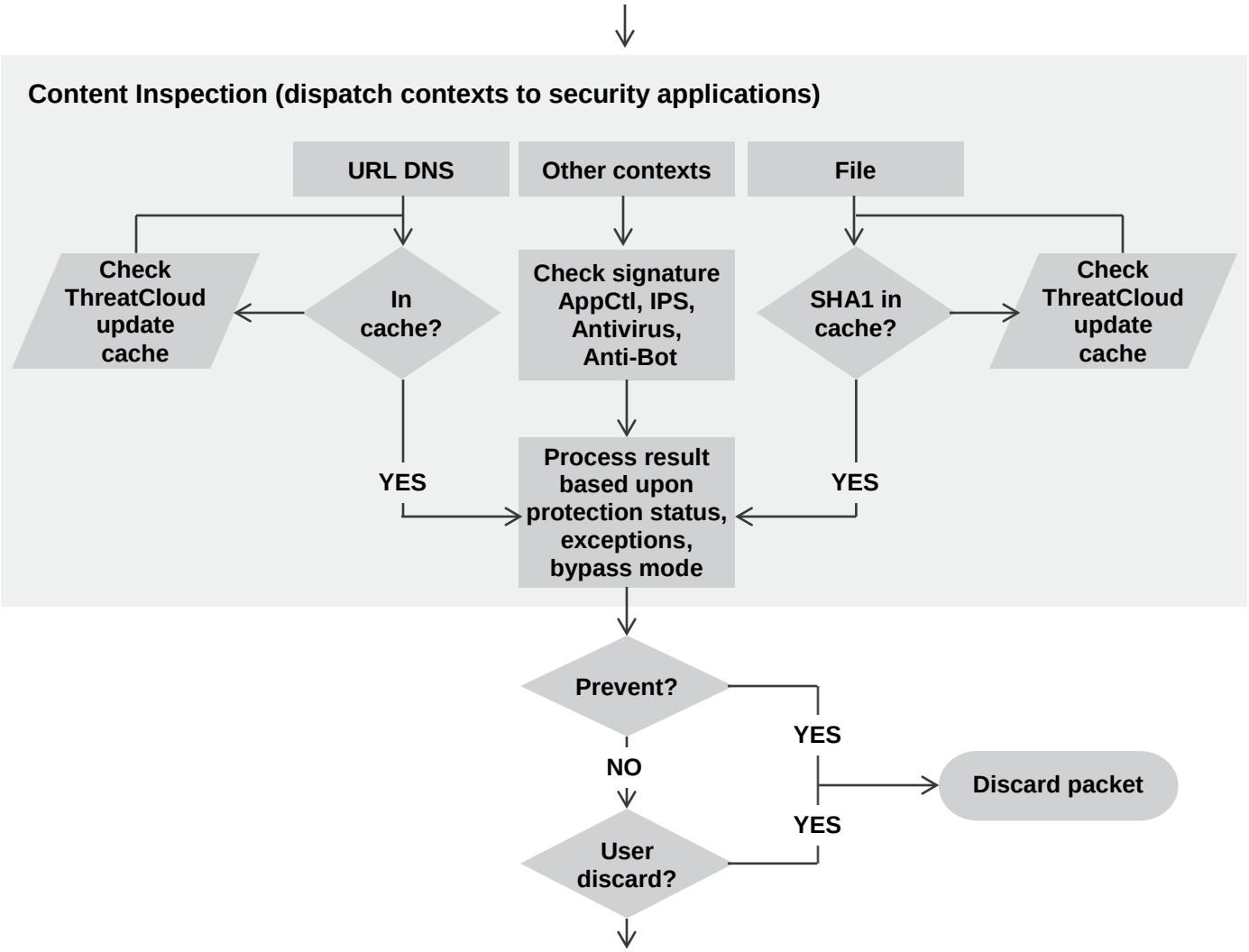

Figure 3: Content security in the NGTP Software Architecture

SECURITY IS ONLY AS STRONG AS YOUR ABILITY TO MANAGE IT

Identity Based Policy Decision

Based on networking and content inspection, a single security policy is applied to traffic. When Identity Awareness is enabled, a kernel table maps user related information like the user, group and machine related information to the IP address. Based upon the security policy action, the packet will be allowed or prevented. If the action requires user intervention, our unique UserCheck involves the user in the policy decision.

Setting Management Priority

We know that some situations can overwhelm a security gateway. When traffic levels exceed the hardware's throughput, either from a spike in legitimate traffic or from a DoS attack, it is vital that we can maintain management communications and continue to interact with dynamic routing neighbors. To do this, our priority queues give a higher priority to control connections than to data connections.

Security Management Architecture

Check Point stands out when you have more than one gateway to manage. When you have a distributed deployment, management, logging and reporting do not touch the data processing hardware. This is well suited for the central management model used in most enterprises.

CONCLUSION

The bottom line is that you must provide strong protection efficiently, so as not to impede business innovation. How do you accomplish this? You need intelligent technology that keeps ahead of the threat landscape – technology that can detect and block both known and unknown threats with the agility to be deployed where you need security both on premises and in the cloud.

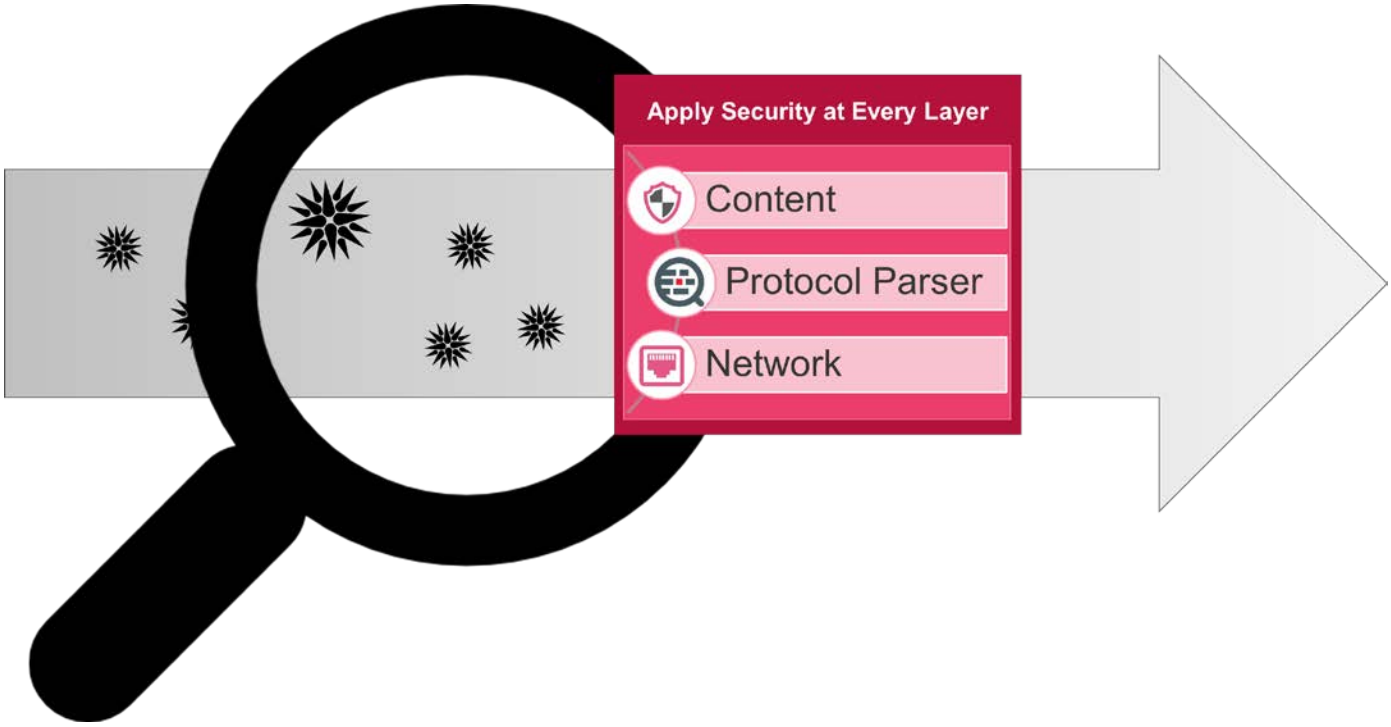

Figure 4: Next Generation Threat Prevention

As evasion techniques evolve and become smarter, so must the technology you use to keep your business secure. Robust security architecture lets your company be proactive in its approach to security, rather than reactive. When you are constantly reacting to problems after they occur, rather than preventing them, it wastes time, energy, and money that your company may not have to spend.

The Key is to Optimize Security

Our recommendation is to utilize a consolidated security platform that prevents threats in real-time and delivers comprehensive visibility into all network traffic, applications, events and threats. It is also important to have a security foundation that can easily block new threats as they appear or accommodate new technologies as needed to thwart those threats. This is achieved with a security architecture that can apply new technology in software and does not require swapping out your existing security device.

References

[1] Verizon 2016 Data Breach Investigations Report

[2] Gartner Predicts 2015: Infrastructure Protection

[3] Lockheed-Martin Corporation, Hutchins, Cloppert, and Amin, Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, 2011