
# CHECK POINT

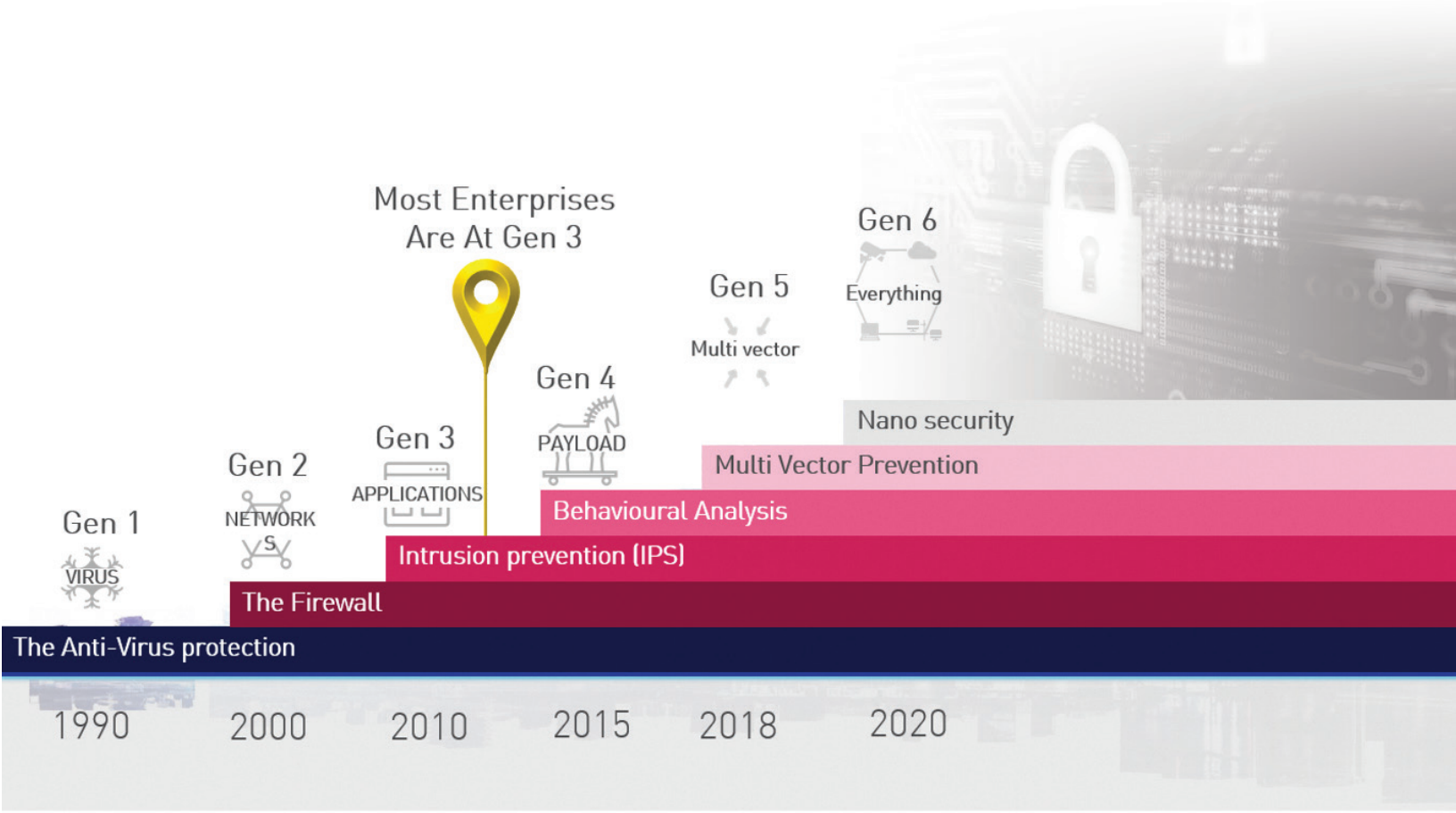
## NEXT GENERATION FIREWALL BUYER'S GUIDE

# TABLE OF CONTENTS

# The Cyber Security Landscape Is Shifting

The world as we know it has changed, and so has your business. In 2020 companies around the globe looked for ways to connect reliably, scale rapidly, and stay protected as workforces transitioned from on-premises to remote work. At the same time, threat actors did not miss a step. In December the discovery of the SolarWinds supply chain attack became public, one example of a 6th generation cyber attack. Sixth generation cyber attacks include nation state and malware as a service (MaaS) attacks. Check out the graphic below to understand the different generations of cyber attacks.

According to the 2021 Cyber Security Report the Sunburst attacks that breached thousands of government and private sector organizations was just the tip of the iceberg making up the 2020 attacks. 87% of organizations experienced an attempted exploit of a known vulnerability. In addition to the nation-state style attack of SUNBURST, financially motivated threat actors continued to wage their malware campaigns.



In 2020, on the malware campaign front, we saw double extortion ransomware, email thread hijacking, voice phishing (vishing) as well as attacks targeting cloud infrastructures. Authors of malware campaigns evolved their techniques to take advantage where they could. The costs to businesses and municipalities from ransomware grew from $11.5B in 2019 to $20B in 2020. Attacks against remote access technologies such as Remote Desktop Protocol (RDP) and VPN increased. In the first half of 2020 almost a million attack attempts against RDP were observed every day. In the second half threats shifted and focused on vulnerable VPN portals, gateways and applications as new vulnerabilities in these systems became known.

# Firewall Defined

A Firewall is a network security device that monitors incoming and outgoing network traffic. A Firewall enforces an organization's security policy by filtering network traffic. At its most basic a Firewall is essentially the boundary or barrier between two networks to identify threats in incoming traffic and blocks specific traffic, once flagged by a defined set of security rules, while allowing non-threatening traffic through.

Firewalls have existed since the late 80's and started as "packet filters," which were networks set up to examine packets transferred between computers. They've come a long way since then, but the basic principle behind why they're so important remains: It allows an organization to enforce security policies at the network level, protecting all the devices behind the firewall without having to implement these policies on every device.

## TYPES OF FIREWALLS

- **Packet Filtering:** Data is blocked or permitted based on a small amount information (e.g. network address) in the header of each packet.
- **Proxy Service:** Network security system that protects while filtering messages at the application layer.
- **Stateful Inspection:** Dynamic packet filtering that monitors active connections to determine which network packets to allow through the Firewall.
- **Next Generation Firewall:** Deep packet inspection Firewall with application-level inspection.

# WHAT DO THEY DO?

A Firewall is a necessary part of any security architecture and takes the guesswork out of host level protections and entrusts them to your network security device. In a properly segmented network, firewalls enforce zero trust least privileged access for IoT devices, users, groups, applications, and systems. This includes macro segmentation boundary controls for north/south traffic entering and exiting the protected segment and micro segmentation to inspect east/west traffic between virtual machines in private, public and hybrid cloud environments.

Firewalls are also multi-purpose network devices. They use dynamic routing protocols to route traffic flows. They translate network addresses from one network to another; private to public and IPv4 to IPv6. They are virtual private network (VPN) termination points for site-to-site and client-to-site VPNs. When work shifted to remote in early 2020 remote access VPN and SSL VPN portal capabilities were vital for keeping employees connected.

Perhaps most important of all of these capabilities is threat prevention. Next Generation Firewalls focus on blocking malware and application-layer attacks. Integrated IPS (intrusion prevention system) in Next Generation Firewalls quickly and seamlessly enables companies to virtually patch vulnerable systems, sometimes before a security update is developed. Bottom line, they can better defend your network and carry out quick assessments to detect invasive or suspicious activity, like malware, and shut it down.

# WHY DO YOU NEED THEM?

Prevention is key. Every network needs malware defense, and advanced malware defense involves many layers of safeguards. There are many types of malware that a Firewall can protect against, including:

**Virus**: A virus is a malicious, downloadable file that attacks by changing other computer programs with its own code. Once it spreads those files are infected and can spread from one computer to another, and/or corrupt or destroy network data.


**Worms:** A worm is a standalone malware that can propagate and work independently of other files, where a virus needs a host program to spread. They can slow down computer networks by eating up bandwidth as well as the slow the efficiency of your computer to process data.

**Trojan:** A trojan is a backdoor program that creates an entryway for malicious users to access the computer system by using what looks like a real program, but quickly turns out to be harmful. A trojan virus can delete files, activate other malware hidden on your computer network, such as a virus and steal valuable data.

**Spyware:** Much like its name, spyware is a computer virus that gathers information about a person or organization without their express knowledge and may send the information gathered to a third party without the consumer's consent.

**Adware:** Can redirect your search requests to advertising websites and collect marketing data about you in the process so that customized advertisements will be displayed based on your search and buying history.

**Ransomware:** This is a type of trojan cyberware that is designed to gain money from the person or organization's computer on which it is installed by encrypting data so that it is unusable, blocking access to the user's system.

It also should be noted that Firewalls are ubiquitous in regulatory compliance regimens. They are usually mandated to protect in-scope systems from the Internet and from other parts of the organization's environment. They are configured with security policies that deny all traffic except that required for production applications, safeguard data in transit within encrypted tunnels, and can also apply threat prevention controls required to be in compliance.

# TYPES OF NETWORK SECURITY PROTECTIONS

Any discussion of firewalls requires a step back to look at the types of network security capabilities that organizations can expect from a Next Generation Firewall.

### Network Segmentation

Network segmentation defines boundaries between network segments where assets within the group have a common function, risk or role within an organization. For instance, the perimeter gateway segments a company network from the Internet. Potential threats outside the network are prevented, ensuring that an organization's sensitive data remains inside. Organizations can go further by defining additional internal boundaries within their network, which can provide improved security and access control.

### Access Control

Access control defines the people or groups and the devices that have access to network applications and systems thereby denying unsanctioned access, and maybe threats. Integrations with Identity and Access Management (IAM) products can strongly identify the user and Role-based Access Control (RBAC) policies ensure the person and device are authorized access to the asset.

### Remote Access VPN

Remote access VPN provides remote and secure access to a company network to individual hosts or clients, such as telecommuters, mobile users, and extranet consumers. Each host typically has VPN client software loaded or uses a web-based client. Privacy and integrity of sensitive information is ensured through multi-factor authentication, endpoint compliance scanning, and encryption of all transmitted data.

### Zero Trust Networks

The zero trust security model states that a user should only have the access and permissions that they require to fulfill their role. This is a very different approach from that provided by traditional perimeter-focused security model. Zero trust is a data first approach to achieve security using micro-segmentation. Using Firewalls, companies can enforce a least privileged access policy at the network level. So, only the right users and devices have the access they require to perform their duties.

### Email Security

Email security refers to any processes, products, and services designed to protect your email accounts and email content safe from external threats. Most email service providers have built-in email security features designed to keep you secure, but these may not be enough to stop cybercriminals from accessing your information.

### Data Loss Prevention (DLP)

Data loss prevention (DLP) is a cybersecurity methodology that combines technology and best practices to prevent the exposure of sensitive information outside of an organization, especially regulated data such as personally identifiable information (PII) and compliance related data: HIPAA, SOX, PCI DSS, etc.

### Intrusion Prevention Systems (IPS)

IPS technologies can detect or prevent network security attacks such as brute force attacks, Denial of Service (DoS) attacks and exploits of known vulnerabilities. A vulnerability is a weakness for instance in a software system and an exploit is an attack that leverages that vulnerability to gain control of that system. When an exploit is announced, there is often a window of opportunity for attackers to exploit that vulnerability before the security patch is applied. An Intrusion Prevention System can be used in these cases to quickly block these attacks.

### Sandboxing

Sandboxing is a cybersecurity practice where you run code or open files in a safe, isolated environment on a host machine that mimics end-user operating environments. Sandboxing observes the files or code as they are opened and looks for malicious behavior to prevent threats from getting on the network. For example malware in files such as PDF, Microsoft Word, Excel and PowerPoint can be safely detected and blocked before the files reach an unsuspecting end user.

### Hyperscale Network Security

Hyperscale is the ability of an architecture to scale appropriately, as increased demand is added to the system. This solution includes rapid deployment and scaling up or down to meet changes in network security demands. By tightly integrating networking and compute resources in a software-defined system, it is possible to fully utilize all hardware resources available in a clustering solution.

### Cloud Network Security

Applications and workloads are no longer exclusively hosted on-premises in a local data center. Protecting the modern data center requires greater flexibility and innovation to keep pace with the migration of application workloads to the cloud. Software-defined Networking (SDN) and Software-defined Wide Area Network (SD-WAN) solutions enable network security solutions in private, public, hybrid and cloud-hosted Firewall-as-a-Service (FWaaS) deployments.

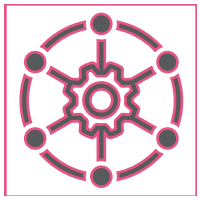
# The State of the Art: The "Next Generation Firewall" Becomes the "Network Firewall"

Enterprises have standardized on next generation firewalls (NGFW) because of their broad support for multiple critical security functions and application awareness. In fact, Gartner has started using the term Network Firewall to describe the rapid expansion in functionality beyond NGFW. Network firewalls are a critical element of any security architecture, but trying to choose which one to buy is not a simple task. While firewall technology used to be fairly straightforward, these days enterprise firewalls are true security gateways which support a wide variety of functions and form factors. Network Firewalls are not just physical appliances, but also include virtual firewalls offered as a firewall as a service (FWaaS) or as a virtual machine running on a hypervisor in a public and private cloud.

This Next Generation Firewall Guide will define the mandatory capabilities of the next-generation enterprise firewall. You can use the capabilities defined in this document to select your next Enterprise Firewall solution. In addition, we will explain how Check Point's solution goes beyond the basic requirements and provides best-in-class enterprise firewalls for any size business. Like Gartner, we focus on transformational technologies or approaches that deliver on the future needs of end users and businesses. Given the term "Next Generation Firewall" (NGFW) is still used by a majority of the industry we will use both "Next- Generation" and "Network" firewall terms interchangeably in this document.

# Network Firewall Mandatory Capabilities

Check Point believes that in order to defend against a rapidly expanding threat landscape, an Enterprise Firewall must support nine critical capabilities:



## SECURITY MANAGEMENT

Effective enterprise firewall architectures are impossible without superior management. The features on a firewall are useless if they can't be used efficiently, so the quest for a next-gen firewall starts with the management platform. Security management is not simply a matter of configuration; the complete security operational paradigm must be considered:

- Number one is ease of use, where the UI reduces the man-hours required to complete an operation. In other words, choose the best tool for the job.
- Consistent policy implementation across the security infrastructure (including but certainly not limited to the firewalls)
- Threat detection and incident response life-cycle management
- Scale (devices under management, number of administrators, and number of roles/teams involved in operations)
- Change management, workflow and segregation of duties
- Automation and orchestration: With third-party IT and Security solutions, and with data center virtualization, cloud and DevOps automation;
- Compliance and audit control validation and reporting

## THREAT PREVENTION

The most significant capability added to enterprise firewalls has been the integration of robust threat prevention. Initially the focus was on integrating IPS to consolidate hardware, but modern firewalls must go far beyond that: sandboxing, anti-phishing, anti-virus and anti-bot are all possible threat prevention techniques. Many vendors use cloud-based analytics and threat intelligence in conjunction with their firewalls. These cloud platforms push threat prevention updates down to the firewalls, and receive malware indicator updates so they can be shared with others. In addition, today's enterprise firewall must integrate with third party NAC and analytics systems that dynamically push IoCs to the firewall, creating a more secure and resilient ecosystem.

## INSPECTION AND CONTROL

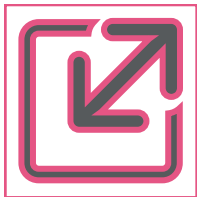
As applications have become more sophisticated, firewalls have had to evolve in order to identify them, as otherwise it's impossible to write a reliable policy rule based on application. Therefore it's key to pick a firewall that has application support that is broad (as many apps as possible), deep (sub-functions within applications), intelligent (able to find the app even if evasion technology is used) and dynamic (frequent updates as applications proliferate or change).

## IDENTITY-BASED INSPECTION AND CONTROL

Firewall rules based on simple IP addresses are becoming less and less relevant given the move to dynamic addressing, cloud architectures, and group-based policies. An enterprise firewall must support policies based on users or (more importantly) groups of users. The most common situation is a group-based policy that leverages the organization's primary identity store, typically Active Directory group membership. Policies such as these are tremendously beneficial as they automate typical processes (user moves/add/changes), and decrease configuration changes required on the firewall.

## CLOUD SUPPORT

It is axiomatic that cloud-based IT has joined on-premises infrastructure as viable enterprise architectures. Therefore, enterprise firewalls must extend security to protect strategic workloads. Obviously this means that the offering must include hardware and software based options to support hybrid cloud environments, but that is insufficient for true enterprise support. The vendor must also embrace the automation and orchestration management models in use, scalable performance based on dynamic workloads, and consumption models that allow cost-effective deployment.

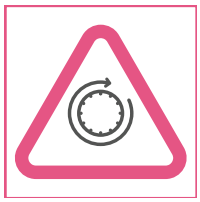


## SCALABLE PERFORMANCE WITH ADVANCED SECURITY FUNCTIONS

The wide variety of services supported by next-gen firewalls require significant amounts of compute and memory resources, which can create performance bottlenecks and affect application availability and user experience. There are multiple approaches to dealing with this consideration, all of which have their advantages and drawbacks. However the key requirements are being able to easily scale performance as requirements increase, and that hardware limitations don't prevent you from deploying the latest threat prevention technologies and algorithms, or result in very different performance considerations in virtual or cloud versus hardware deployments.

## ENCRYPTED TRAFFIC INSPECTION

A recent Google study showed that over 80% of the web traffic generated by the end-user Chrome browser activity was encrypted.[1] Unfortunately at the same time, malware creators have learned to leverage Certification Authority (CA) automation initiatives like encryption to create phishing sites trusted by browsers. As encrypted traffic and threats proliferate, firewalls must be capable of inspecting such traffic both to apply control policy and for threat prevention. It also must be sophisticated enough to support complex policies such as selective decryption so that certain traffic (e.g. employee's on-line banking) can be excluded from decryption to avoid regulatory or liability pitfalls.



## AUTONOMOUS THREAT PREVENTION

Threat detection and prevention technology is not just contained in a single network device, but is a system of interconnected components. In addition to network security enforcement points monitoring network traffic, there are management systems that set policy, feed updates as threats change, collect log data from the enforcement points and analysis engines to find the threats in the billions of events seen daily. Threat response times are lower when infrastructure processes are autonomous and do not need manual control.

## SECURITY AUTOMATION

Network security is one part of an enterprise infrastructure which also includes identity stores, communications equipment, databases, web services, network components and most recently Internet of Things devices and cloud applications, services and workloads. Security is better when some of these systems are interconnected, e.g. firewalls connect to Windows Active Directory or IAM (Identity and Access Management) systems to create a stronger and more dynamic user-based security policy. With the shift to cloud and Software-defined Networking (SDN), firewalls have become modular components that can be provisioned, configured and included in an automated security orchestration and response (SOAR) to threats.

[1] Google Transparency Report on HTTPS encryption on the web
https://transparencyreport.google.com/

# Check Point: A Holistic View to Enterprise Firewalls

Check Point takes a holistic approach to security architecture. Each component leverages real-time threat intelligence to provide a unified view of the threat landscape, so cyber attacks can be discovered and mitigated quickly. This approach is in stark contrast to the isolated security point solutions on the market today. The evolution of firewall capabilities and applications hasn't changed this unified approach, which is most recently manifested in Check Point's Infinity Architecture. We believe that firewall gateways fit into a broader security narrative, one in which firewalls are:

## Centralized Management

*Centralized management of unified policy that supports application-based controls that are user, content and data aware*

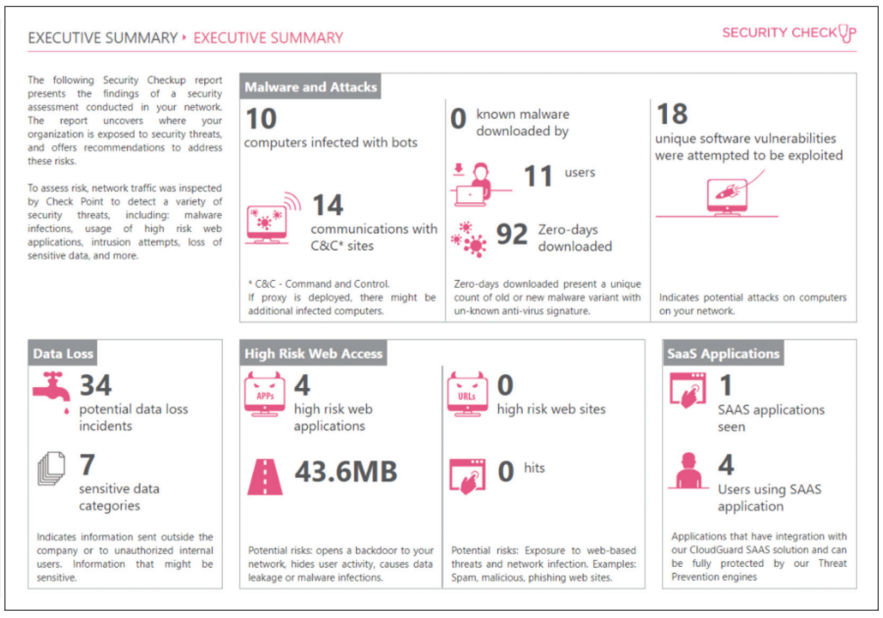
## DevSecOps Automation and Orchestration

*Codify provisioning, configuration management and threat response workflows in CI/CD pipelines*

## Hyperscalable

*Enable growth on demand and utilization of existing resources with efficient N+1 (active/active) clustering capabilities*

Virtually all organizations are struggling to operationalize security, in large part because they acquire point solutions and try to integrate them (unsuccessfully) into an inevitably complex security architecture. Therefore, we believe that organizations selecting a next-gen or enterprise firewall need to think in the context of operations at scale, instead of looking at product-specific feature lists or price/performance claims. In the following section of the Buyer's Guide we will describe how Check Point's support for the enterprise firewall capabilities map to our security architecture narrative.



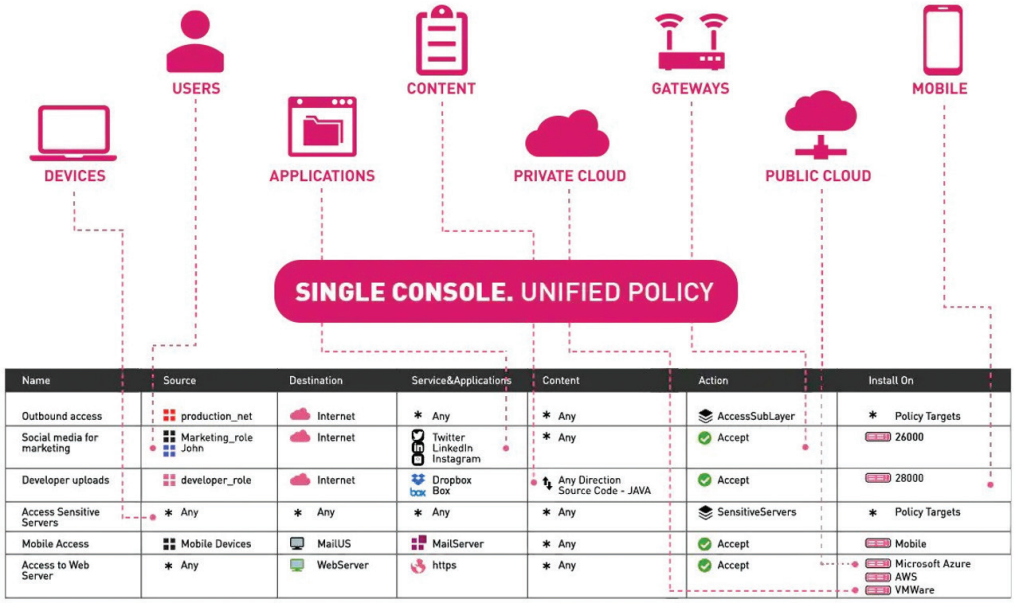

*Check Point leverages security technology to drive business outcomes.*

# Check Point Enterprise Firewalls: From Next-Gen to a Security Architecture

## SECURITY MANAGEMENT

Check Point security management has always played a fundamental role in our architectures, and drives operationally viable policy management, incident response, and compliance. At the highest level, the management architecture supports:

- A single policy construct across network, cloud, endpoint, mobile and IoT in the Infinity architecture
- Unified threat prevention and access control in a single policy across on-premises and cloud
- Compliance control validation, with template support for common compliance regulations
- Consolidated, actionable threat management (SmartEvent) and integrations with major SIEM vendors
- Group-based delegation of administration authority, with full workflow support
- Orchestrating integrations with virtual and cloud environments including automated services insertion
- Open APIs to empower third party integrations and software development tools Ansible and Terraform




*Unified Access Policy: Write once, deploy anywhere with full identity and application awareness.*

Check Point's management has been developed based on the real-world lessons learned over 27 years of customer experience operating our firewalls and security gateways. As a result, we are able to deliver up to a 50% reduction in human investment for ongoing operations. An exhaustive description of our management capability is clearly beyond the scope of this document, however in the final analysis it's the management that makes the difference between success and failure when it comes to operationally viable network-based security.

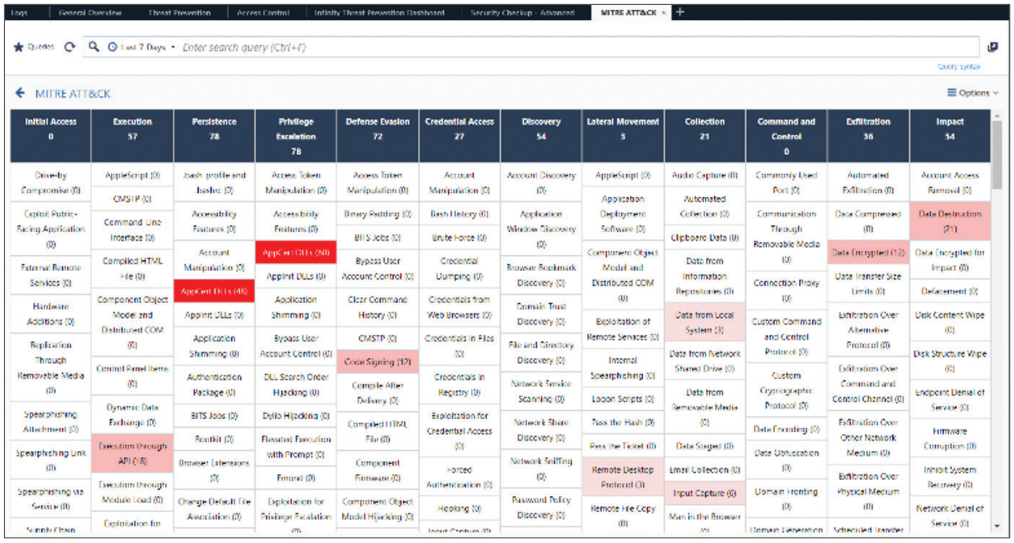
# THREAT PREVENTION

A key Check Point differentiator when compared to other firewalls is the integration of best-in-class threat prevention across the architecture. While others concede attackers will get in and are pivoting to detection and response, our focus remains on stopping attacks before they succeed. This includes tackling the latest large-scale, multi-vector GenVI attacks, in addition to more conventional attacks that are still widely used.

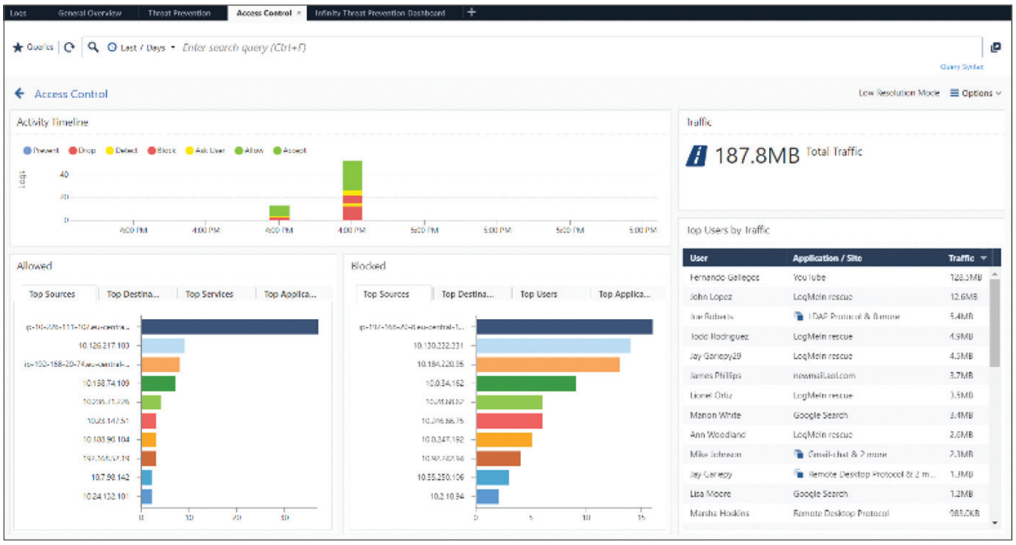

*AI backed Threat Prevention*

This focus is demonstrated in capabilities that include:

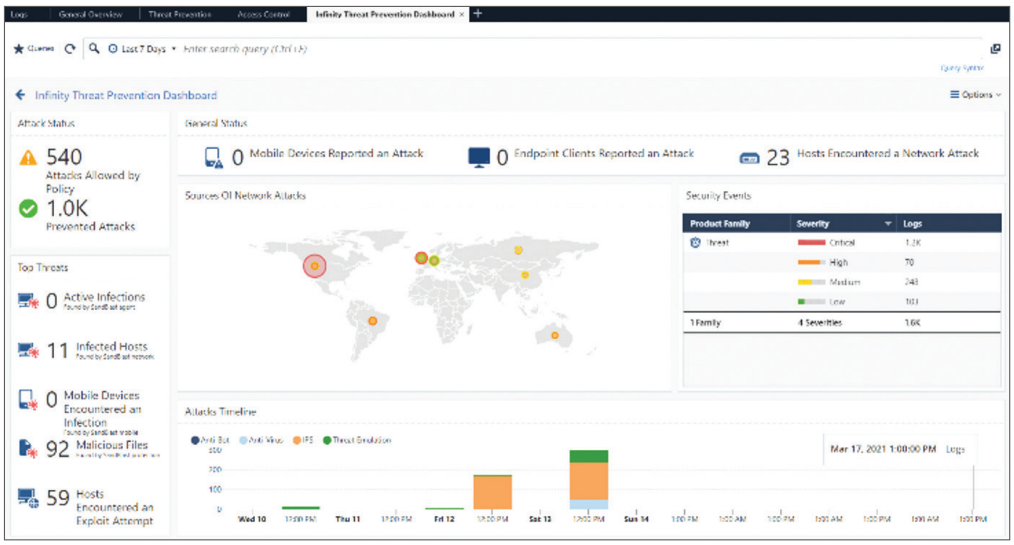
- **ThreatCloud** is a Cloud-based platform that shares and delivers real-time dynamic security intelligence to the Infinity architecture, including our firewalls, security gateways, mobile and endpoints.
- **New ThreatCloud AI engines** that detect malware well beyond AV and static analysis, while reducing false positives ten-fold.
- **SandBlast Threat Emulation** (sandboxing) which blocks even zero-day attacks before they can begin their evasion techniques.
- **SandBlast Threat Extraction** (Content Disarm & Reconstruction) which delivers safe and clean files to users protecting them from infection. Includes web threat extraction and document sanitation for web downloads.
- **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



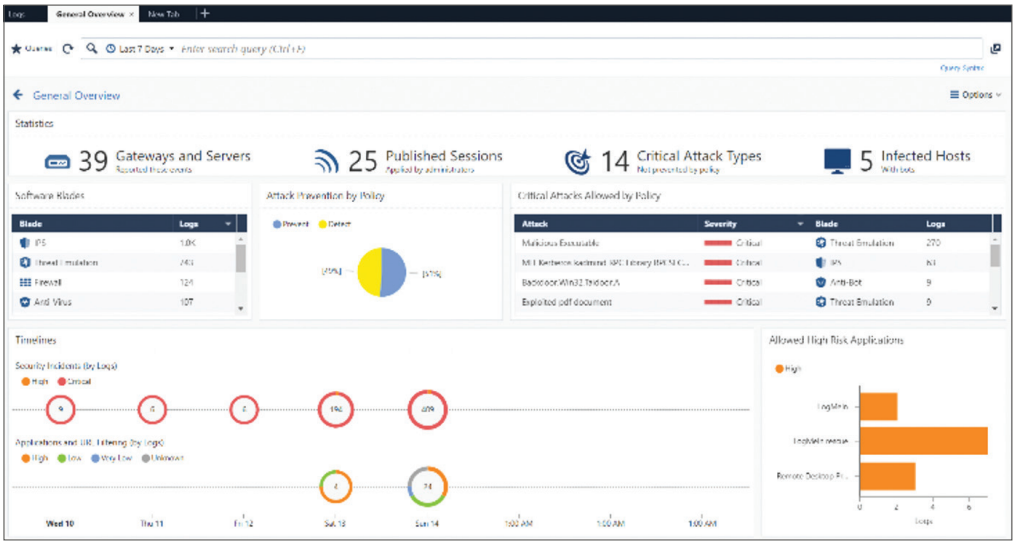

*Integrated MITRE Attack View*




*Access Control View*




*Threat Prevention Dashboard*




*General Overview for Quick Assessment*

# Consolidated Traffic Monitoring and Improved Indexing Capabilities

Logs and monitoring menu provides a rich and customizable interactive views of all network and security activities recorded on physical/internal gateways, cloud-based gateways, endpoint/mobile devices and IoT. Administrators can use the raw log view pane, or choose to explore any of the predefined views in the views sub menu. Each view is an interactive dashboard comprised of multiple clickable widgets, creating customizable panes, providing the administrator an account of the network and events based on different themes e.g. Remote Users, MITRE ATT&CK (using a graphical representation of an updated MITRE heat map to locate the top techniques and drill down to the most relevant ones) or Threat Prevention.

## APPLICATION INSPECTION AND CONTROL

Check Point's Application Control capability supports security policies to identify, allow, block or limit usage of thousands of applications, including Web and social networking, regardless of port, protocol or evasive technique used to traverse the network. It currently understands over 8,500 Web 2.0 applications with more being added continuously. Advanced user interaction features allow security administrators to alert employees in real-time about application access limitations, and query them as to whether application use is for business or personal use. This enables IT administrators to gain a better understanding of Web usage patterns, adapt policies and regulate personal usage without interrupting the flow of business.

## IDENTITY-BASED INSPECTION AND CONTROL

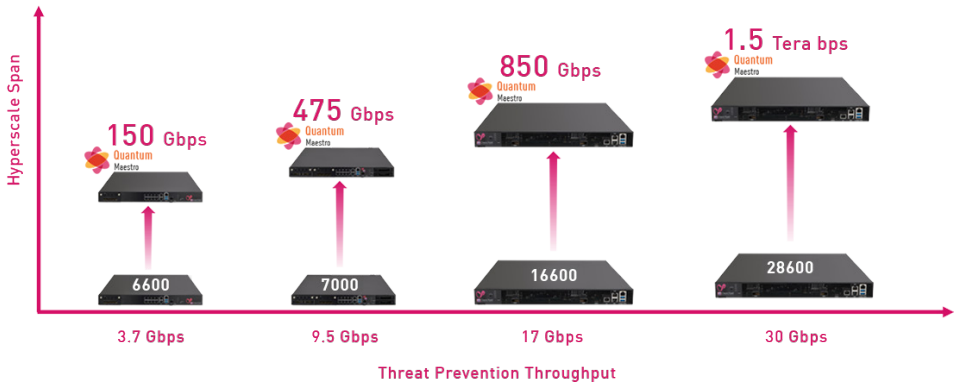
Check Point pioneered the development of user and group based policies. Our firewalls and management integrates with Microsoft AD, LDAP, RADIUS, Cisco pxGrid, Terminal Servers and with 3rd parties via a Web API. And because the management console supports these polices across our portfolio, you can limit the integration with the identity store to this one interface, and still get broad security coverage based on a single set of identity-policies. This support extends to security monitoring via the SmartEvent console. The combination of identity and application awareness is mandatory for building scalable security policies that protect the business without compromising user experience.

## CLOUD SUPPORT

Check Point firewalls support both virtual and cloud deployments, in addition to a complete portfolio of appliances that span remote office to data center requirements. Virtual systems support allows a single software security gateway to be segmented into multiple zones with independent resources and management. In addition to traditional vSphere, we support both NSX and Cisco ACI software-defined networking environments. For IaaS public cloud, all major vendors are supported including AWS, Azure, GCP, Oracle and Alibaba Clouds. Integration with cloud automation provides instantiation of both virtual gateways and template-based security policies without manual intervention. This enables new workloads to be secured as they are deployed, without implementation delays caused by manual security configuration.

# SCALABLE PERFORMANCE WITH ADVANCED SECURITY FUNCTIONS

Check Point's portfolio offers powerful scaling options for both hardware and software-based firewalls. The Maestro Hyperscale solution brings the scale, agility and elasticity of the cloud on premise with efficient N+1 hardware clustering based on Check Point HyperSync technology. Up to 52 gateways/firewalls can be clustered to deliver up to 1,500 Gbps of throughput, while still being managed as a single entity. Start with what you need today, knowing that you can easily scale when needed without risky and complex upgrades or network redesigns. Check Point Maestro can support many modern use cases, such as capacity planning and work-from-home needs; organizations can add capacity seamlessly exactly when it's needed to deal with new needs and traffic peaks.For cloud deployments, Check Point offers CloudGuard, available in both Pay-as-you- go (PAYG) and Bring-your-own-license (BYOL) pricing models. CloudGuard supports the same services as our physical firewalls, with transparent policy management across on-premises, virtual, and cloud gateways.




*Maestro Hyperscale brings agility and non-disruptive scale to the data center for business of all sizes.*

# ENCRYPTED TRAFFIC INSPECTION

Check Point enterprise firewall software includes SSL/TLS decryption and inspection, so that security policies can be applied to encrypted traffic. The software leverages crypto hardware acceleration built into Intel processors. Furthermore, our SecureXL technology supports crypto acceleration using Check Point hardware models available on many of the security gateways. This acceleration is critical in situations requiring high-scale inspection and policy enforcement upon HTTPS encrypted traffic. Finally enterprise firewalls must securely categorize HTTPS traffic using the Server Name Indication (SNI) extension, inspect all of the latest cipher suites and curves such as TLS 1.3.

## AUTONOMOUS THREAT PREVENTION

Check Point has the industry's first autonomous Threat Prevention system, which eliminates labor-intensive manual threat classification and updates. All gateways are updated automatically by AI-based threat prevention for complete protection against even zero-day threats. The Infinity Threat Prevention policy enables security administrators to implement threat prevention in a single click. The policy is then continuously updated automatically.

Five out-of-the-box profiles are available to choose from. Simply choose a protection profile that matches your network; Perimeter, Internal Network, Data Center East-West, Guest or Strict. Each profile includes: IPS, reputation-based protections (IP, URL, domain, etc.), sandboxing (our Threat Emulation), Sanitization (CDR) which is our Threat Extraction, and Command and Control protection. Each is customized according to the relevant security requirements of the network segment. Just choose the appropriate profile for your organization's needs, and you are protected.

## SECURITY AUTOMATION

Check Point has a long history of technology partner integrations and today has over 100 technology partnerships with industry leading IAM, SIEM, cloud, mobile, network, SD-WAN, threat intelligence, and IoT discovery vendors. For customers this large ecosystem of technology partnerships means that Check Point firewalls will fit seamlessly into any infrastructure. This is made possible by open APIs and adoption of industry standards. One of the best examples of this is our cloud network firewalls which use cloud-native APIs. Auto-provisioning and auto-scaling along with automatic policy updates ensures security protections keep pace with all changes in public and private cloud environments. Another use case is configuration management using third party tools like Terraform and Ansible. With software development tools repetitive tasks can be codified into workflows and CI/CD pipelines. A third use case are the Check Point integrations with leading SOAR vendors to automate and orchestrate response to threats. In a fourth use case consider provisioning and deploying security to remote offices using a light footprint virtual security gateway or a FWaaS integration with leading SD-WAN vendors. Finally, to secure Internet of Things (IoT) devices Check Point integrates with leading IoT discovery vendors to auto-segment, control IoT network access and prevent threats to vulnerable IoT devices.

# Summary and Next Steps

As a society, the Internet is our lifeline, it is the schools we send our kids to, the banks we entrust our finances to, the health insurance we rely on, and the business we conduct. It is imperative that we secure it. As internet traffic and corporate networks grow each year, cyber-attacks are becoming more sophisticated and harder to detect. It should be clear from this Buyer's Guide that "next-generation firewalls" are much more than enforcement points for network traffic policies. These enterprise-class devices are really security gateways, which include Layer 7 application intelligence and multi-dimensional threat prevention. When selecting an enterprise firewall vendor, ask the follow questions while reviewing the mandatory capabilities:

- How should I weigh the importance of each capability, based on what is most important to me?
- Can I eliminate other tools and devices if I deploy enterprise firewalls broadly, lowering both capital investment and staff costs?
- What is going to be my approach to scaling performance, given the inevitable increase in traffic and sophistication required to combat the ever-evolving threat landscape?
- What IT and Security infrastructure will I need to integrate with the firewalls and their supporting components?
- Most importantly: Have I thought through the complete operational model I will use to provision, monitor, and upgrade these devices, consistent with my staff size and capabilities?

Like any technology, next-gen firewalls are only part of the solution: people, policies and procedures are essential to building and operating an effective security architecture. By combining all of these, organizations take a big step towards protecting their sensitive assets, meeting compliance requirements, and driving digital transformation.

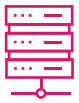
## Next Generation Firewalls


Rugged Firewalls


Small and Branch Office Firewalls


Enterprise Firewalls


Data Center Firewalls


Hyperscale Network Security


Cloud Firewalls


Firewall as a Service

**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**