YOU DESERVE THE BEST SECURITY

NEXT GENERATION FIREWALL
BUYER'S GUIDE

Table of Contents

The Cyber Security Landscape Is Shifting 3

Firewall Defined 4

The "Next Generation Firewall" Becomes the "Network Firewall" 8

Network Firewall Mandatory Capabilities 9

Security Management 9

Threat Prevention 9

Application Inspection and Control 10

Identity-Based Inspection and Control 10

Hybrid Cloud Support 10

Scalable Performance and Services 10

Encrypted Traffic Inspection 11

Autonomous Threat Prevention 11

Security Automation 11

IoT and OT Security 12

Check Point: A Holistic View of Enterprise Firewalls 14

Check Point Enterprise Firewalls: From Next-Gen to a Security Architecture 14

ULTRA-LOW LATENCY, HYPER-FAST FIREWALL 17

Summary and Next Steps 19

Appendix 20

The Cyber Security Landscape Is Shifting

The world as we know it has changed, and so has business. Companies around the globe are looking for ways to connect reliably, scale rapidly, and protect a mobile workforce. These changes are causing more organizations to shift toward cloud-hybrid environments, adding complexities to existing cyber security measures.

A 2023 IDC report confirmed that as data centers and enterprises are adapting a cloud-hybrid model, security remains a concern, with 56% of IaaS environments reporting one or more major breach in the last two years. This is tied to the overall rise in cyber attacks, as indicated by Check Point's 2023 Cyber Security Report, which noted a surge in several industries, including a staggering 74% increase in attacks in the healthcare industry.

In addition to specific infrastructure breaches, the increased fragmentation of IT environments poses logistical and management challenges for security teams. To future-proof security, organizations need solutions that reduce administrative overhead, integrate with cloud and on-prem infrastructure, and enforce granular policies, all while delivering consistent security and performance across their networks.

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 (NGFW):** Deep packet inspection Firewall with application level inspection.
- **AI-Powered Firewalls:** Ability to block evasive zero-day threats that do not yet have known 'signatures'

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 level, 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 set up to examine packets transferred between computers. They've come a long way since then, but the basic principle behind why they're soimportant 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.

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, as well as 'trusted' traffic within a data center.

Firewalls are also multi-purpose network devices, using dynamic routing protocols to route traffic and serving as virtual private network (VPN) termination points for site-to-site and client-to-site infrastructure.

Perhaps the most important of all these capabilities is threat prevention. Next Generation Firewalls focus on blocking malware and application-layer attacks. Integrated IPS (intrusion prevention system) in 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.

The main job of firewalls is threat prevention. This is accomplished through micro-segmentation that enforces zero trust, lease privilege access for devices (including IoT), users, groups, applications, and systems. Traffic is thus inspected across environments, including on-premises, cloud, and hybrid. The capabilities below are critical for Next Generation Firewalls to detect and prevent attacks.

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 accompany networks 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

Firewalls serve as virtual private network (VPN) termination points for site-to-site and client-to-site infrastructure. 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 targeted phishing attacks and zero-day malware.

Web Security

Web is so ubiquitous that it requires constantly updating web protocol inspection capabilities, accurately categorizing millions of websites, dynamic objects for automatically updating lists of trusted cloud services as well as AI-backed threat intelligence. Threat actors use web infrastructures to hide malicious activity and directly or indirectly exploit vulnerabilities including users by tricking unsuspecting web users with targeted phishing campaigns.

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.

TYPES OF FIREWALL DEPLOYMENTS

While network firewalls have traditionally been deployed as a hardware security gateway, this is not the only application. They have evolved and are now deployed in a variety of form factors.

Resilient, Scalable 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 balance workloads across all hardware resources available in a cluster architecture for high availability and resiliency.

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.

Latency Sensitive, High Throughput Applications

Data center, e-commerce and service provider environments have special requirements for securing trusted traffic at multi-hundred Gigabit/sec or Terabit/sec speeds. In addition, financial services such as high frequency trading require firewalls that operate at low ultra-low latency. Firewalls have evolved to secure these demanding environments.

Hybrid Mesh Firewall

A hybrid mesh firewall platform is deployed across hardware and virtual appliances, cloud-based and as-a-service models with a unified cloud-based management plane. It supports hybrid environments by offering continuous integration/ continuous deliver (CI/CD) pipeline integration and advanced security capabilities, including IoT and DNS-based attack prevention. Hybrid mesh firewalls offer multiple deployment options together with centralized visibility and management.

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 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 guide will define the mandatory capabilities of the modern 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.

For example, Check Point continuously innovates AI-based threat prevention capabilities. This includes its ThreatCloud AI global threat intelligence platform, which delivers real-time threat updates to Check Point firewalls around the globe. Check Point's latest generation of AI-Powered firewalls and security gateways leverage over 50 AI engines to identify and block the most evasive zero-day exploits. Check Point delivers the industry's leading security effectiveness, as measured through independent 3rd party testing.

Since 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 defending against modern attacks requires an Enterprise Firewall to support nine critical capabilities:

SECURITY MANAGEMENT

Effective enterprise firewall architectures are impossible without management. The features on a firewall are useless if they can't be used efficiently, so the quest for a nextgen 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 staff 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, including reviews, super-approver edits and approvals
- Automation and orchestration with third-party IT and security solutions, and with data center virtualization, cloud and DevOps automation
- Regulatory and industry Compliance including audit control validation and reporting

THREAT PREVENTION

The most significant capability added to enterprise firewalls has been the integration of robust layer 1-7 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, anti-bot, and DNS (Domain Name Service) security 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 Indicators of Compromise (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 (asmany 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.

HYBRID 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

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

Most web traffic is encrypted, oftentimes with TLS encryption. 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 policy controls and prevent threats. 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 automated 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 more recently Internet of Things devices and cloud applications, services and workloads. Security is better when 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.

SECURING IOT AND OT

Internet of Things (IoT) devices include everything from Smart doorbells and building management systems in homes and offices to more specialized devices such as wearable medical devices in hospitals. Programmable Logic Controllers (PLC) are found in manufacturing, energy, telecom, and other Operational Technology (OT) environments. OT security is particularly important for critical infrastructure industries that are prime targets for cyber attacks through their Industrial Control Systems (ICS)

Securing these environments requires firewalls that can control the protocols that IoT/OT devices use and firewall management linked to discovery systems that continuously monitor and apply policy to secure IoT.

WHAT DIFFERENTIATES TODAY'S NETWORK FIREWALLS?

Many firewalls on the market offer seemingly similar capabilities, leaving organizations at a loss when comparing vendors or products. Understanding how the nuances of features and performances of firewalls match your needs is key to choosing the right solution.

Throughput measures the speed of traffic that a firewall can handle, and ranges from gigabits to terabits per second, according to the specs of the appliance and the needs of the organization.

Threat efficacy of firewalls refers to what percentage of threats are detected or prevented. Some firewalls can detect threats but do not prevent them, resulting in alerts only after an infection has occurred. Independent 3rd party testing reports provide valuable insights for users interested in comparing solutions.

Port modularity offers flexibility for future growth, so an organization can add modules to increase port density and keep up with changing network requirements, or provide high speed direct connections to critical servers.

Clustering is the ability to deploy multiple firewalls synchronously and with the capacity for integrated load balancing and high availability configurations.

Network connectivity options should suit your individual needs. Whether you want zero-touch deployment for your small business or continued services for complex needs, your firewall connectivity is key to success.

Integrated cloud security services are becoming essential for cloud and hybrid businesses. Check to see if your provider offers options for IoT, SASE, SDWAN, and other cloud security necessities.

Operating software is a critical part of NGFWs. Protection is more than just the appliance and requires a smart software "brain" to identify new threats. Sophisticated providers leverage machine learning and AI for zero day threat prevention.

Security management provides unified visibility and policy management across your network security ecosystem. An intuitive and user-friendly system is essential for firewall management.

These differentiating factors can prompt important questions for vendors to choose a provider and model. There are also several third parties, such as Miercom, that conduct independent testing of these parameters across different firewalls. These tests are often conducted on "zero+1 day" threats, which are within 24 hours of discovery, the most critical time in threat prevention.

Securing DNS Communications DNS (Domain Name System) is a standard internet communication protocol used to assign and associate IP addresses to domain names. When a system doesn't know the IP address or name of a device it wants to communicate with, the information is provided by a DNS server on a local network or via a cloud service on the internet.

Unfortunately, the underlying DNS communication protocol is not inherently secure and therefore can be hacked to establish 'command and control' communications with an enterprise's servers. Additionally, the DNS communications protocol can be hijacked to 'tunnel' stolen credentials or other sensitive data.

Traditional NGFW firewall security mechanisms cannot identify or block these new types of attacks because they are highly sophisticated and elusive. Therefore, modern AI engines are required.

Identifying False Domain Names Hacking organizations can now create thousands of 'fake' domain names using mathematical algorithms. These false domains can temporarily bypass common firewall security systems (i.e. by 'flying under the radar'). Because enterprise IT security systems will not initially have known 'signatures' or threat intelligence to identify these domain names as invalid, hackers will be able to set up temporary command and control communications with enterprise servers — giving the hackers minutes or hours to breach the network.

In this case, recognizing and blocking algorithmically generated domain names requires modern AI techniques.

Check Point: A Holistic View of Enterprise Firewalls

Check Point takes a holistic approach to security architecture, most recently showcased in our Infinity Architecture. Each component leverages real-time threat intelligence to provide a unified view of the threat landscape, so cyber attacks can quickly be discovered and mitigated. This approach starkly contrasts the isolated security point solutions on the market today. We believe that firewall gateways fit into a broader security narrative, one in which firewalls have:

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

Hyperscalability

Enable growth on demand and utilization of existing resources with efficient N+1 (load sharing) clustering capabilities

The key to modern security is operationalizing and integrating security solutions into increasingly complex architectures. Thus, selecting next-gen or enterprise firewalls requires consideration of scaling operations, rather than looking for 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 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

Check Point's management has been developed based on the real-world lessons learned over nearly 30 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 attacks, in addition to more conventional attacks that are still widely used.

This focus is demonstrated in capabilities that include:

- **ThreatCloud AI**, Check Point's dedicated Cloud-based platform that shares and delivers real-time dynamic security intelligence to our firewalls, and our mobile and endpoint security products.
- **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. This 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 the early stages of attacks that lead to ransomware infections.

ACTIONABLE THREAT MANAGEMENT

Logs and monitoring menu provides a rich and customizable, interactive view 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 9,000 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 simplify security management and get broad security coverage based on a single set of identity-policies. The combination of identity and application awareness is mandatory for building dynamic security policies.

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, modular scaling options for both hardware and software-based firewalls. Modular port flexibility is built into new Quantum Force products to keep up with changing network needs, while the Maestro Hyperscale solution brings the scale, agility and elasticity of the cloud into on-premises, using efficient N+1 firewall clustering with intelligent load balancing, based on Check Point HyperSync technology.

Check Point firewalls and security gateways can be clustered in a Maestro configuration to deliver up to 1 Tbps (1,000 Gbps) of advanced threat prevention throughput, while still being managed as a single entity. Enterprises can start with a smaller system, knowing that they can easily scale when needed, without risky and complex upgrades or network re-designs.

Check Point Maestro supports modern use cases, such as capacity planning, remote workforce requirements, intelligent load balancing, and in-service firewall migrations. Organizations can add capacity seamlessly to support new needs and unexpected traffic spikes. Maestro also offers performance autoscaling to temporarily shift firewall resource from underutilized security groups to critical applications during high demand. The firewall resource will then automatically revert to its original 'security group' after the server or application demand has stabilized.

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 comprehensive services as our physical firewalls, with transparent policy management across on-premises, virtual, and cloud gateways. In fact, both Quantum on-premises firewalls and CloudGuard cloud firewalls share the same operating system, security features, and are managed through the same unified policy management console.

ULTRA-LOW LATENCY, HYPER-FAST FIREWALL

Enterprises need data center security to perform at the speed of the network, to enable the transfer of hundreds of terabytes of data in minutes instead of hours, provide low latency for high frequency financial transactions, while scaling on demand to support high growth businesses like online commerce.

Quantum Security Gateways offer hyper-fast firewalls deliver up to 1,400 Gbps (1.4 Tbps) of stateful firewall throughput in a single appliance with an ultra-low 3 microsecond latency.

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 autoscaling 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.

Appendix: WHY DO YOU NEED FIREWALLS?

Prevention is key. Every network needs malware defense, which 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.

Phishing: In this attack, messages that appear to be legitimate manipulate a user, causing them to install a malicious file, click on a malicious link, or divulge sensitive information such as access credentials.

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.

DNS Breaches: Unfortunately, the underlying DNS communication (Domain Name Service) protocol used by all enterprises is not inherently secure. DNS can be hacked to establish 'command and control' communications with a customer's servers. The DNS communications link can be hijacked to 'tunnel' stolen credentials or other sensitive data.

DDoS Attacks (Distribution Denial of Service): In these attacks, hackers flood an enterprise's servers with an overwhelming amount internet traffic to prevent customers from connecting to online services. This oftentimes interrupts an organization's business for hours or more.

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 stay in compliance.

To **learn more**, visit www.checkpoint.com/quantum/.

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