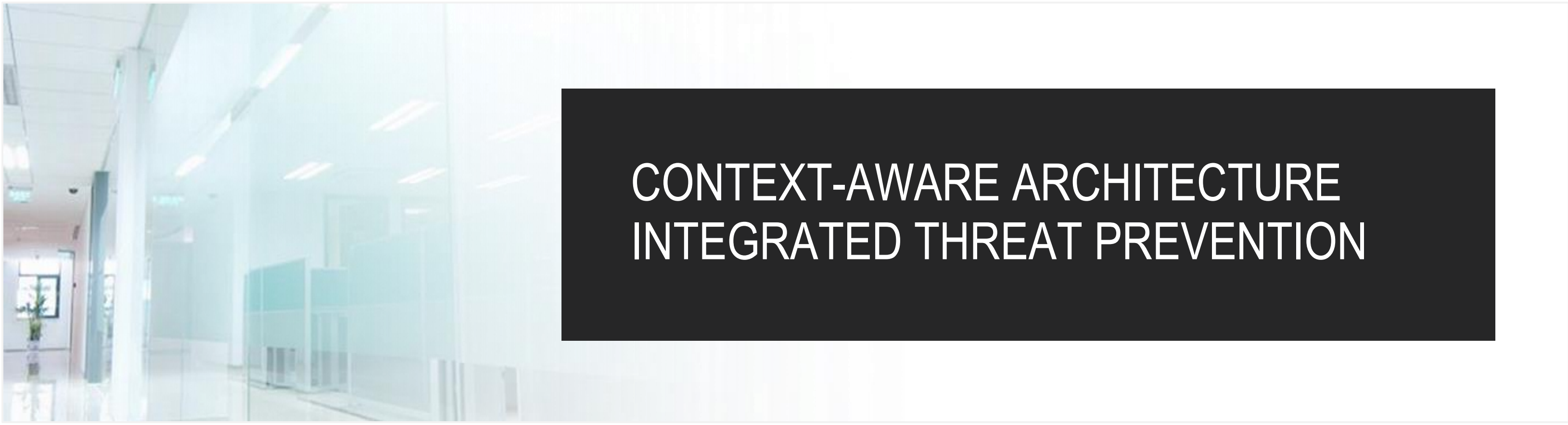


CONTEXT-AWARE ARCHITECTURE INTEGRATED THREAT PREVENTION

The goal of integrated network security devices is prevention, but architecture constraints force many solutions to focus on detection and mitigation rather than prevention. This reactive approach to cyberattacks is costly and ineffective, complicates security operations and creates inherent gaps in security posture.

FOCUSED, PARALLEL PROCESSING

Check Point delivers a network security software architecture that offers true threat prevention, not just threat detection. It does this without delay in one session, scales across multiple sessions, and is agile enough for deployment wherever you need security on premises and in the cloud.

The key aspects of this innovative approach to prevention includes:

- **Focused, context-aware Inspection:** By focusing on the relevant content for any given connection, Check Point eliminates wasted processing, thus reducing latency.
- **Parallel processing pattern matcher:** Once we know where to look, the content can then be processed simultaneously and efficiently using a common signature format.

ARCHITECTURE COMPONENTS

Security software focused on context-aware inspection is unique to Check Point Next Generation Threat Prevention. This is achieved with the following components:

Common streaming engine: The streaming process creates an ordered packet stream and directly performs a number of security functions on the stream to prevent attacks and decrypts HTTPS traffic so that it can be inspected.

Common protocol parsers: The protocol parsers pick apart a stream of packets forming a session to determine the different elements. For example, where a file transfer starts and stops and what the file type is, the URL and so on. By performing focused content scanning on the relevant parts of the stream, we save significant processing power.

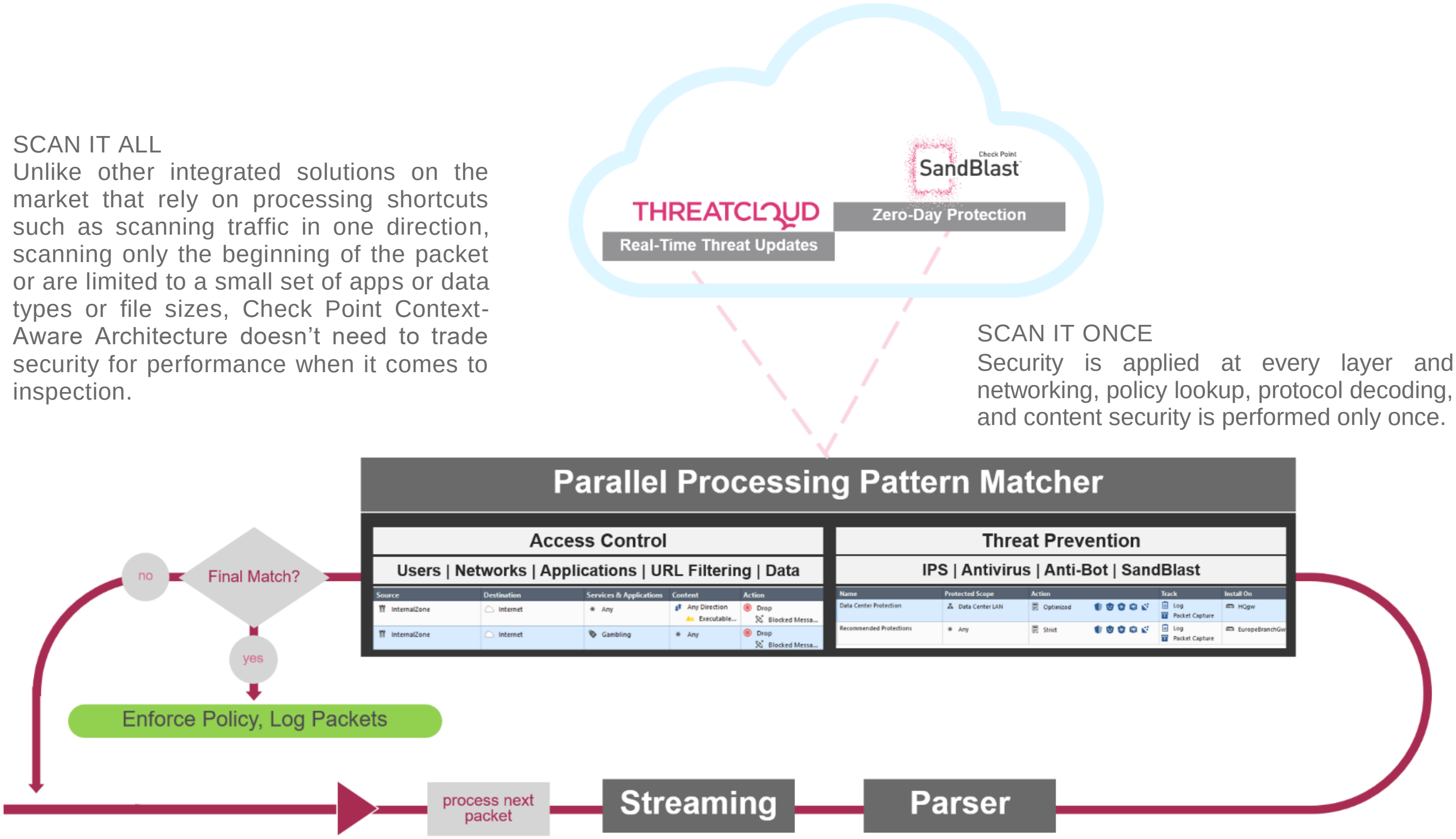
Common pattern matcher: Signatures from multiple sources, e.g. IPS and Application Control, are compiled together; one for each context, i.e. URL, host header etc. and inspected simultaneously. The pattern matcher quickly identifies harmless packets and common signatures in malicious packets.

SCAN IT ALL

Unlike other integrated solutions on the market that rely on processing shortcuts such as scanning traffic in one direction, scanning only the beginning of the packet or are limited to a small set of apps or data types or file sizes, Check Point Context-Aware Architecture doesn't need to trade security for performance when it comes to inspection.

SCAN IT ONCE

Security is applied at every layer and networking, policy lookup, protocol decoding, and content security is performed only once.



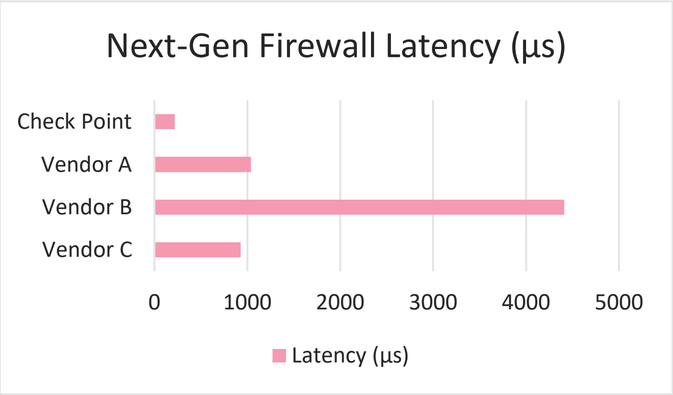
Source	Destination	Services & Applications	Content	Action
InternalZone	Internet	Any	Any Direction Executable...	Drop Blocked Messa...
InternalZone	Internet	Gambling	Any	Drop Blocked Messa...

Name	Protected Scope	Action	Track	Install On
Data Center Protection	Data Center LAN	Optimized	Log Packet Capture	HQgw
Recommended Protections	Any	Strict	Log Packet Capture	EuropeBranchGw

LOW LATENCY, SOFTWARE ACCELERATION

Below the Context-Aware engine is a stateful-inspection firewall, a core component of the Check Point NGTP architecture.

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.



Source: Silver Peak, Inc.

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.

When possible, throughput and connection rate are accelerated by the security acceleration (SecureXL) module. The SecureXL device enforces security policy based on source, destination and port information. Then content security is enforced by the context-aware engine. In multi-core systems this processing is distributed amongst the cores to provide near linear scalability on each additional core.

SUMMARY

The common components of the Check Point Next Generation Threat Prevention platform provide operational efficiencies that enable prevention of threats without compromising on security. At the same time acceleration technologies minimize latency and maximize efficient hardware utilization. This approach offers great flexibility to add functionality as the nature of threats changes over time and requires new approaches. Implemented in both physical and virtual appliances, our Next Generation Threat Prevention platform stops modern threats.

CONTACT US

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: 650-628-2177 | www.checkpoint.com