Solution Brief

Turbocharging Prophaze's Web App Security with Intel

Prophaze tests performance of its Web Application and API Protection software running on a server based on 4th Gen Intel® Xeon® Scalable processors and finds that core loading and SSL performance improves security functions

Enterprises are experiencing an increase in sophisticated cyber threats targeting web applications and APIs. These attacks bypass conventional security measures, focusing on manipulating application logic and data flows. This trend necessitates different security solutions and strategies, with an emphasis on robust web application firewalls (WAFs) and API protection software.

To defend against these attacks, Intel® Solution Builder member Prophaze has developed its Web Application and API Protection (WAAP) comprehensive platform designed to safeguard modern web applications and APIs from a wide range of cyber threats. The company recently tested the loading capacity and SSL termination performance of the 4th Gen Intel® Xeon® Scalable processor to see what impact it can have on application security.

How Prophaze's App Security Platform Works

Prophaze's App Security Platforms is a specialized security tool designed to monitor, filter, and block HTTP traffic to and from web applications (see Figure 1). The platform acts as a shield, protecting web applications from common exploits like SQL injection, cross-site scripting (XSS), and other malicious activities that target application vulnerabilities.

Prophaze is a comprehensive security platform designed to protect applications and APIs, whether they are hosted in the cloud, on-premises, or across multiple cloud environments. One part of this solution is the Prophaze Web Application and API Protection (WAAP) which provides real-time defense against vulnerabilities such as SQL injection, cross-site scripting (XSS), and various other application-specific exploits. The platform is engineered to offer advanced threat detection and automated mitigation, ensuring that web applications and APIs remain secure without impacting performance.

Prophaze WAAP also includes bot protection and DDoS defense, providing a multi-layered security approach that effectively secures both web applications and APIs from attacks.

Prophaze WAAP is adaptable to a variety of deployment scenarios. The platform ensures that organizations are able to maintain robust security while allowing their applications to operate seamlessly. Its powerful defense mechanisms not only reduce the risk of data breaches and downtime but also help mitigate attacks in real-time, ensuring that critical business services remain protected.

By offering automated threat mitigation and comprehensive security, Prophaze WAAP enables businesses to focus on their growth and innovation with confidence that their applications and APIs are secure.

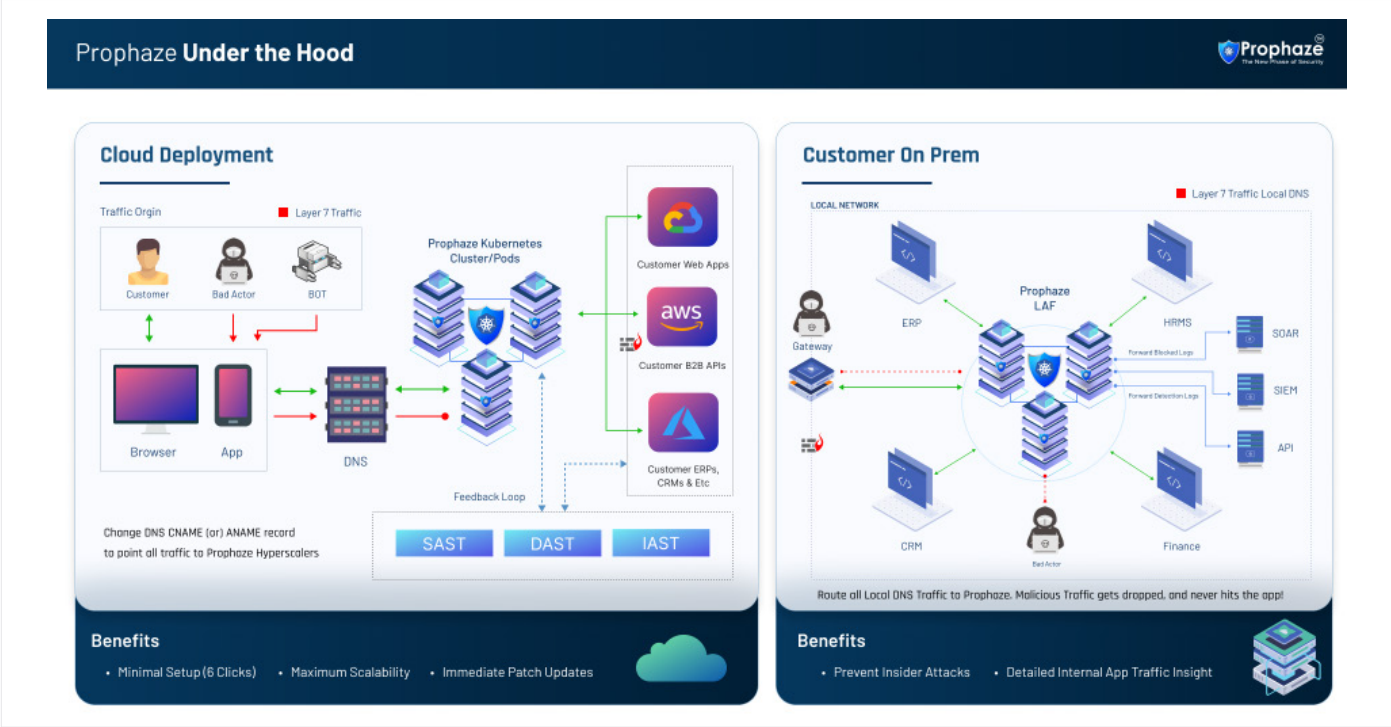

Figure 1. Block diagram showing how the Prophaze Web Application and API Protection platform monitors, filters, and blocks HTTP traffic to and from web applications.

Prophaze features a seamless integration with Dynamic Application Security Testing (DAST) tools. By taking inputs from these tools, Prophaze generates custom Web Application Firewall (WAF) policies tailored to specific customer needs. This integration allows for a smooth incorporation into a CI/CD pipeline, facilitating a hassle-free security setup.

App Security Depends on High-Performance CPUs

The effectiveness of Prophaze's App Security Platform's is heavily reliant on the processing power of the underlying hardware, particularly the CPU.

Prophaze's WAAP must analyze vast amounts of network traffic in real-time, applying complex rule sets and algorithms to identify and mitigate threats. This computational intensity makes CPU performance a critical factor in maintaining high throughput and low latency while providing comprehensive protection.

Prophaze Chooses 4th Gen Intel® Xeon® Scalable Processors

4th Gen Intel® Xeon® Scalable processors offer an improved architecture, enhanced power efficiency, and increased performance per watt. These improvements potentially translate to significant gains in Prophaze's WAAP performance, allowing for faster packet processing, more sophisticated real-time analysis, and the ability to handle higher traffic volumes without compromising security.

Other key features include:

High Core Counts: The 4th Gen Intel Xeon Scalable processors offer up to 60 cores per socket. Prophaze's WAAP is highly parallelizable and can benefit significantly from more cores, especially in environments handling a high volume of concurrent connections. More cores allow Prophaze's App Security Platform to handle more simultaneous requests and provide better performance under heavy loads. The 4th Gen Intel Xeon Scalable processor features architectural improvements that increase the instructions per cycle, enhancing the efficiency of each core. This improvement can lead to faster request processing and lower latency in Prophaze's App Security Platform.

Increased Memory Capacity: The 4th Gen Intel Xeon Scalable processor supports DDR5 memory, which provides improved performance and power efficiency. This is particularly beneficial for Prophaze's App Security Platform when used as a reverse proxy or load balancer, as it can cache more content in memory, reducing disk I/O and improving response times.

PCIe 5.0 and CXL Support: The support for PCIe Gen 5.0 and Compute Express Link (CXL) 1.1 in the 4th Gen Intel Xeon Scalable processor allows for faster data transfer between CPUs, GPUs, storage devices, and network interfaces. For Prophaze's WAAP, this means better network throughput and lower latency when communicating with backend servers or storage, which is critical in high-traffic environments or when using Prophaze's App Security Platform for load balancing.

Direct Data Streaming: The Intel® Data Streaming Accelerator (Intel® DSA) in the 4th Gen Intel Xeon Scalable processor optimizes data movement and transformation operations. This feature can reduce CPU overhead for data-intensive tasks in Prophaze's WAAP, such as SSL termination, compression, and decompression, allowing the processor to handle more requests efficiently.

Intel® Crypto Acceleration and Intel® QuickAssist Technology (Intel® QAT): The 4th Gen Intel Xeon Scalable processors come with integrated acceleration for cryptographic operations, including SSL/TLS handshakes, which are common in HTTPS traffic managed by Prophaze WAAP. With these accelerations, Prophaze's App Security Platform can handle encrypted traffic more efficiently, offloading computationally expensive encryption and decryption tasks from the main cores, which reduces latency and improves overall throughput.

Lower Power Consumption and Higher Efficiency: The efficiency improvements in the 4th Gen Intel Xeon Scalable processor mean that servers can do more with less power, which can reduce operational costs and improve the sustainability of data centers running Prophaze's App Security Platform Prophaze's App Security Platform, particularly in large-scale deployments.

Processor Testing Insights and Analysis

The first part of the tests was designed to demonstrate the performance of the Prophaze Web Application and API Security Platform running on a server under test (SUT) powered by a 4th Gen Intel Xeon Scalable processor, Prophaze tested the SUT compared to the performance of a server based on 3rd Gen Intel Xeon Scalable processors with all other configuration details the same. For example, both servers featured 512 GB of RAM, 300 GB of storage, and Ubuntu 22.04 LTS.

The only difference between the machines is that one system under test (SUT) featured Intel® Xeon® Gold 6438N processor (4th Gen SUT), and the other server used an Intel Xeon Gold 6338N processor (3rd Gen SUT).

Traffic was generated using various load testing tools, such as wrk and ab, from a separate machine. All machines were on the same local network, with Prophaze's App Security Platform deployed on both the 3rd Gen SUT and 4th Gen SUT.[1]

Load Handling

The testers calculated the system load averages using the uptime command within Ubuntu. These values indicate how busy the system is, and they are averages of the number of processes that are either in a runnable state or waiting for CPU time.

The uptime command provides three load average numbers that are the average system load over the last 1, 5, and 15 minutes, respectively.

For example, a load average of 1.00 means that, on average, one process was using or waiting for CPU time. If the load average is higher than the number of CPU cores, it suggests that there may be more processes competing for CPU resources, which could indicate high system load etc.

Figure 2 shows the load values of 3rd Gen SUT compared to the 4th Gen SUT under the same traffic conditions, artificially generated using wrk and ab tools.

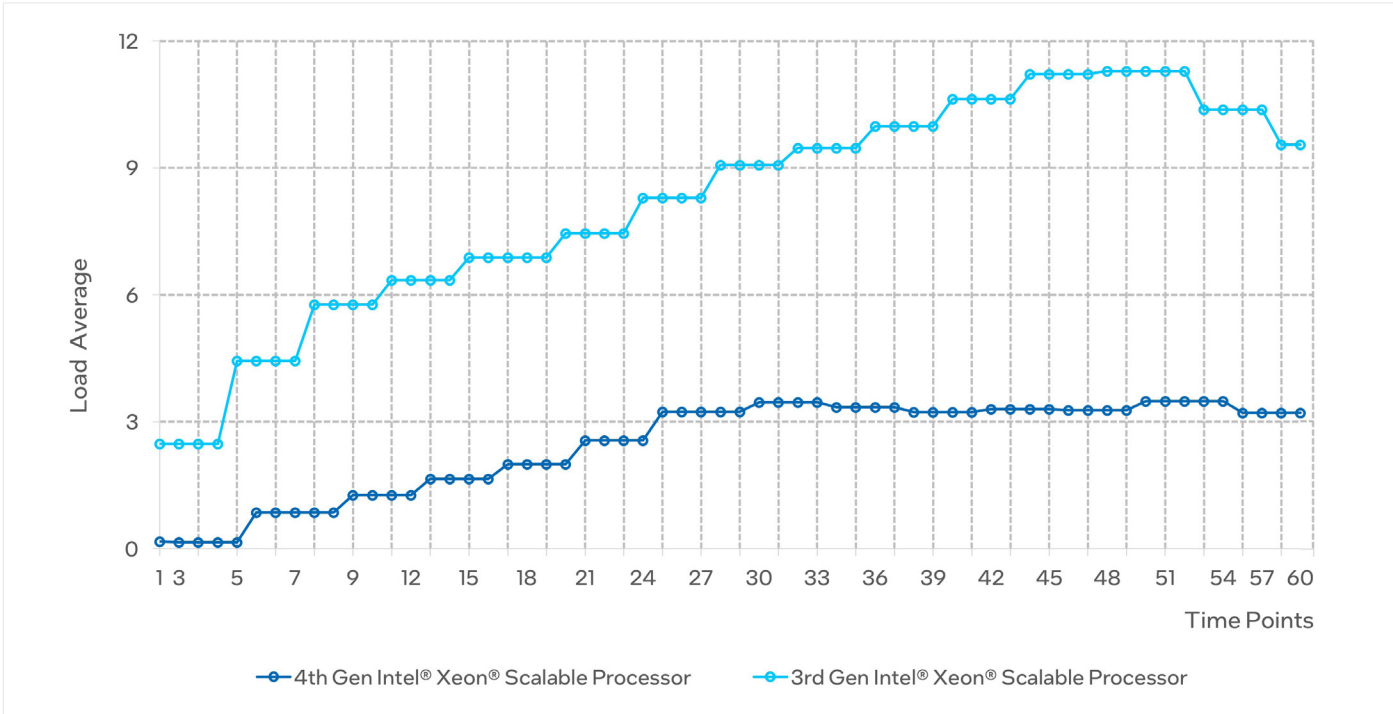

Figure 2. Load averages for 4th Gen SUT compared to 3rd Gen SUT.

In the tests, the 4th Gen SUT consistently showed lower load averages compared to 3rd Gen SUT throughout the entire dataset, suggesting:

- **Lower Load on 4th Gen SUT:** Due to more efficient processing and better hardware characteristics, the 4th Gen SUT handles incoming traffic faster and more efficiently, resulting in a consistently lower load average compared to the 3rd Gen SUT. The 4th Gen SUT demonstrated a much lower load range from 0.15 to 3.49 compared to the 3rd Gen SUT which had a range from 2.48 to 11.29.
- **Variable Load Averages:** The fluctuations in load average are normal and reflect the inherent burstiness of network traffic, task scheduling variations, and background system activities, even when the overall traffic rate remains the same.

How Faster Processors Improve Application Security Posture

Based on the load average comparison between the 4th Gen SUT and 3rdGen SUT, we can infer several advantages for running Prophaze's App Security Platform on servers powered by 4th Gen Intel Xeon Scalable processors.

Lower Overall Load: The 4th Gen SUT consistently maintained a lower load average compared to the 3rd Gen SUT. For operations, this translates to higher capacity to handle concurrent connections, more resources available for processing incoming requests, and reduced risk of server overload during traffic spikes. The 4th Gen SUT load increased more gradually, which suggests an Improved ability to handle growing traffic without significant performance degradation. The tests also indicate there is better performance during sudden traffic surges or DDoS attacks with consistent response times as load increases.

The stability of the 4th Gen SUT was improved as it showed smaller fluctuations in load average, which typically means more predictable performance for Prophaze's WAAP operations, reduced likelihood of service interruptions due to load spikes, and consistent resource availability for critical Prophaze's WAAP functions.

With a peak load for the 4th Gen SUT of 3.49, the server demonstrated a higher performance ceiling compared to 11.29 for the 3rd Gen SUT.

This shows that the 4th Gen SUT has greater headroom for resource-intensive rules and complex configurations that are a part of Prophaze's App Security Platform. The server also supports the ability to handle more simultaneous SSL/TLS connections, which are crucial for secure communication along with faster processing of Prophaze's App Security Platform rules, potentially reducing latency in request handling.

Efficient Resource Utilization: The significantly lower load averages indicate more efficient use of resources, which delivers more CPU cycles for Prophaze WAAP's event-driven, asynchronous processing, improved capacity for Prophaze WAAP to perform deep packet inspection without bottlenecking, and the potential for running additional services alongside Prophaze WAAP without compromising performance.

Even at peak loads, the 4th Gen SUT maintained much lower load averages, implying more reliable performance during high-traffic periods or under attack conditions. This mean there is a reduced risk of Prophaze's App Security Platform becoming a bottleneck during intense scanning or filtering operations and provided the compute headroom to effectively reverse proxy and load balance under heavy loads.

The results of the test show that there is potential for more complex configurations enabling implementation of more sophisticated Prophaze App Security Platform rules without significant performance impact as well as complex reverse proxy configurations, such as advanced caching, compression, or request manipulation.

SSL Termination Performance

A second part of the test measured the secure sockets layer (SSL) termination capacity for both SUTs using the openssl s_time command built into Ubuntu to benchmark the performance of SSL/TLS connections. This OS function works by simulating a high volume of SSL/TLS requests. It measures how quickly a server can handle secure connections, giving users an idea of its performance under SSL/TLS load. The results are shown in Figure 3.

Metric	4th Gen SUT	3rd Gen SUT
# of connections	43,930	31,902
Time	13.05 seconds	13.17 seconds
Connections / user second	3,366.28	2,422.32

Figure 3. SSL termination performance metrics.

The 4th Gen SUT's increased performance offers efficient SSL offloading allowing the Prophaze WAAP software to offload SSL/TLS termination more effectively, managing secure connections with lower latency. With better connection handling, the 4th Gen SUT supports higher traffic volumes, ensuring that Prophaze can scale efficiently during peak loads. This performance delivers improved threat detection because it enables Prophaze to inspect more encrypted traffic in real time, leading to better threat detection and response.

Conclusion

In conclusion, the 4th Gen Intel Xeon Scalable processors demonstrate clear advantages for running Prophaze App Security Platform's WAF operations. The processor family's ability to maintain lower and more stable load averages translates to improved performance, stability, and scalability for web serving and security operations. This can lead to better overall service quality, increased capacity to handle traffic and attacks, and more flexibility in implementing advanced features and configurations.

Learn More

Prophaze Web Application and API Protection (WAAP) Platform

Prophaze bot protection

Prophaze DDoS defense

Intel® Industry Solution Builders

4th Gen Intel® Xeon® Scalable Processors

Notices & Disclaimers

[1] SUT CONFIGURATIONS

Gen 4 SUT: 1-node, 2x Intel® Xeon® Gold 6438N processor with 32 cores and 64 threads. Total DDR5 memory was 512 GB (16 slots/ 32GB). Intel® Hyper-Threading Technology - enabled; Intel® Turbo Boost Technology - disabled. BIOS version: Dell v0.2.3.1. Network controllers: four Intel® Ethernet Network Adapters E810-CQDA2 operating at 10 Gbps.

Software: OS was Ubuntu 22.04 LTS; kernel was Linux. Benchmark/workload software: App Security Platform. Other software: Wrk; ab; Intel® QuickAssist Technology (Intel® QAT); locust.io for simulated real-world traffic patterns; tcpdump to capture and analyze traffic; Grafana and Prometheus for logged system metrics; htop and atop for monitored resource usage; and OpenSSL s_time for measured handshake latency and encryption speed.

Test conducted by Prophaze in August 2024.

Gen 3 SUT: 1-node, 2x Intel® Xeon® Gold 6338N processor with 32 cores and 64 threads. Total DDR4 memory was 512 GB (16 slots/ 32GB) Intel® Hyper-Threading Technology - enabled; Intel® Turbo Boost Technology - disabled. BIOS version: AMI v05.01.01. Network controllers: two Intel® Ethernet Network Adapters E810-CQDA2 operating at 10 Gbps and two Intel® Ethernet Converged Network Adapters X550-T2 operating at 10 Gbps.

Software: OS was Ubuntu 22.04 LTS; kernel was Linux. Benchmark/workload software: App Security Platform. Other software: Intel® QuickAssist Technology (Intel® QAT).

Test conducted by Prophaze in August 2024.

0425/DP/DJA/PDF ♻ Please Recycle 364710-001US