

SOLUTION DESCRIPTION

# Security Offload

FOR INTEL-BASED INFRASTRUCTURE  
PROCESSING UNITS (IPUs)



## SOLUTIONS

Telecom  
Cloud and Edge  
Cybersecurity  
Monitoring  
Infrastructure  
Financial

## PLATFORMS

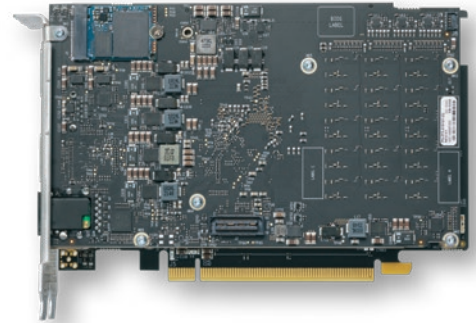
Link-Capture™ Software  
Link-Inline™ Software  
Link-Virtualization™ Software  
Link-Storage™ Software  
Link-Security™ Software  
Link-Programmable™  
Smart Network Interface Cards (SmartNICs)  
Infrastructure Processing Units (IPUs)

## APPLICATIONS

5G UPF Offload  
vSwitch Offload  
Network Offload  
Security Offload  
Storage Offload  
Data Capture  
+ More

## SERVICES

Professional Services  
Custom Development



NAPATECH F2070X IPU

## Napatech Infrastructure Processing Unit (IPU) solution maximizes the performance of data center security based on Transport Layer Security (TLS) encryption

Within enterprise and cloud data centers, Transport Layer Security (TLS) encryption is used to ensure security, confidentiality and data integrity. It provides a secure communication channel between servers over the data center network, ensuring that the data exchanged between them remains private and tamper-proof. However, implementing the TLS protocol on the server's host CPU imposes significant compute overheads and limits the number of CPU cores available for running services and applications.



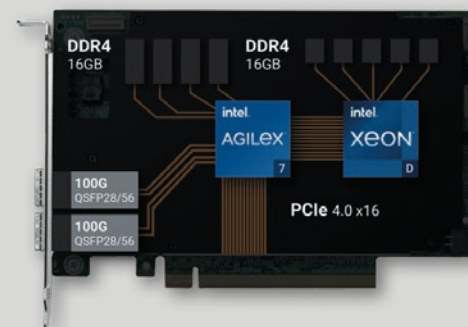
This solution brief explains how an integrated hardware-plus-software solution from Napatech addresses this problem by offloading the TLS protocol from the host CPU to an Infrastructure Processing Unit (IPU) while maintaining full software compatibility at the application level.

The solution not only frees up host CPU cores which would otherwise be consumed by security protocols but also delivers significantly higher performance than a software-based implementation. This significantly reduces data center CAPEX, OPEX and energy consumption.

It also introduces a security layer into the system, isolating system-level infrastructure processing from applications and revenue-producing workloads. This increases protection against cyber-attacks, which reduces the likelihood of the data center suffering security breaches and high-value customer data being compromised, while allowing customers full control of host system resources.

### Napatech F2070X IPU

The Napatech F2070X Infrastructure Processing Unit (IPU) is a 2x100G PCI Express (PCIe) card with an Intel® Agilex® F-Series FPGA and an Intel® Xeon® D processor, in a Full Height, Half Length (FHHL), dual-slot form factor.



The standard configuration of the F2070X IPU comprises an Agilex AGF023 FPGA with 4 banks of 4GB DDR4 memory, together with a 2.3GHz Xeon® D-1736 SoC with 2 banks of 8GB DDR4 memory, while other configuration options can be delivered to support specific workloads.

The F2070X IPU connects to the host via a PCIe 4.0 x16 (16 GT/s) interface, with an identical PCIe 4.0 x16 (16 GT/s) interface between the FPGA and the processor.

Two front-panel QSFP28/56 network interfaces support network configurations of

- 2x 100G;
- 8x 10G or 8x 25G (using breakout cables).

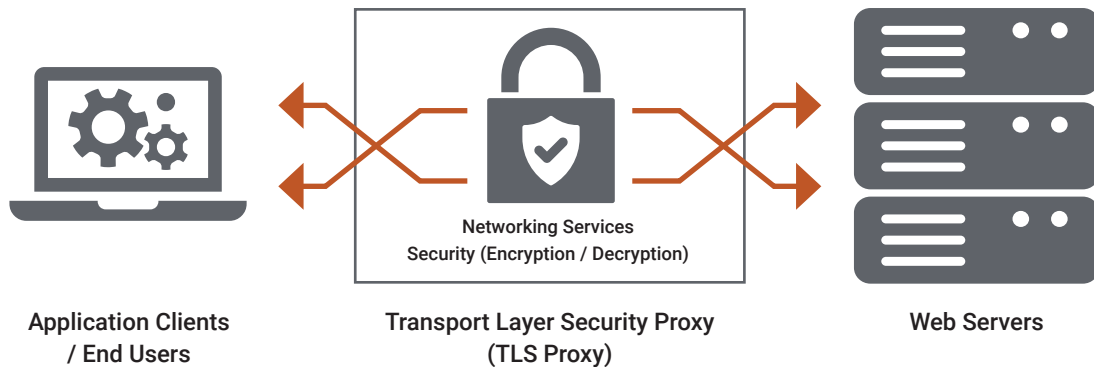
Optional time synchronization is provided by a dedicated PTP RJ45 port, with an external SMA-F and internal MCX-F connector. IEEE 1588v2 time-stamping is supported.

Board management is provided by a dedicated RJ45 Ethernet connector. Secure FPGA image updates enable new functions to be added, or existing features updated, after the IPU has been deployed.

The processor runs Fedora Linux, with a UEFI BIOS, PXE boot support and full shell access via SSH and a UART.

## TLS: the standard security protocol for communications between web applications and servers

Transport Layer Security (TLS) is a cryptographic protocol that provides end-to-end security for data sent between applications over the internet. It is mostly familiar to users through its use in secure web browsing, and in particular the padlock icon that



appears in web browsers when a secure session is established. However, it is also be used for other applications such as e-mail, file transfers, video/audio conferencing, instant messaging and Voice-over-IP (VoIP). TLS evolved from Secure Socket Layers (SSL) which was originally developed to secure web sessions. The first version of the protocol was released in 1999 and the most recent version is TLS 1.3, which was published in 2018.

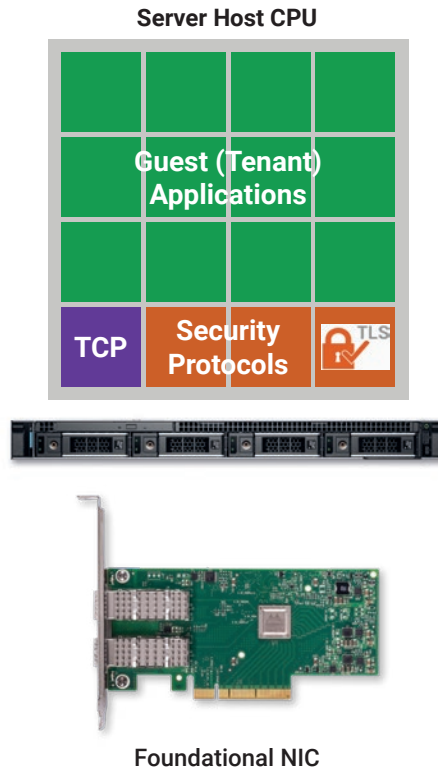
TLS is used in data centers to ensure confidentiality, authentication and data integrity. It provides a secure communication channel between servers over the data center network, ensuring that the data exchanged between them remains private and tamper-proof. Key benefits include:

- **Data Encryption:** One of the primary reasons for using TLS in data centers is to encrypt the data being transmitted between servers and clients within the data center. This encryption ensures that even if the data is intercepted by malicious actors, they won't be able to understand or decipher the actual content of the data. In a multi-tenant environment, where multiple tenants are using the same data center resources, TLS ensures that data belonging to one client remains private and inaccessible to others.
- **Data Integrity:** TLS provides mechanisms to ensure that the data being transmitted has not been altered or tampered with during transmission. This is achieved through techniques like Message Authentication Codes (MACs) and hash functions. Using TLS for internal communication ensures that even if a part of the infrastructure is compromised, the data exchanged between components remains protected.
- **Authentication:** TLS enables authentication of the parties involved in communication. This means that the client and server can verify each other's identity, ensuring that data is exchanged only with trusted entities. This is critical in a data center environment to prevent unauthorized access and data breaches.
- **Protection Against Man-in-the-Middle Attacks:** TLS helps protect against man-in-the-middle attacks, whereby an attacker intercepts and potentially modifies the communication between two parties without their knowledge. By encrypting the data and using digital certificates for authentication, TLS mitigates the risk of such attacks.
- **Compliance and Regulatory Requirements:** Many industries and regions have specific regulations and compliance requirements related to data security and privacy. Implementing TLS helps data centers adhere to these regulations by ensuring the confidentiality and integrity of the data they handle.
- **Secure Management Interfaces:** Data centers often have management interfaces and APIs that allow administrators to control and monitor various aspects of the infrastructure remotely. Securing these interfaces with TLS prevents unauthorized access and manipulation of critical systems.
- **Securing Cloud Services:** Many modern data centers provide cloud services and TLS is essential for securing communication between users and the cloud infrastructure, as well as communication between different cloud services.

In summary, TLS is critical to modern data centers because it provides a comprehensive layer of security, protecting the confidentiality, integrity and authenticity of data as it is transmitted and communicated within the data center environment.

### Limitations of software-only security architectures

Despite the compelling benefits of TLS for data center security, operators need to be aware of significant limitations associated with an implementation in which the protocol runs in software on the host CPU that is typically also running Transmission Control Protocol (TCP), on a server configured with one or more standard (or “foundational”) Network Interface Cards “NICs”:

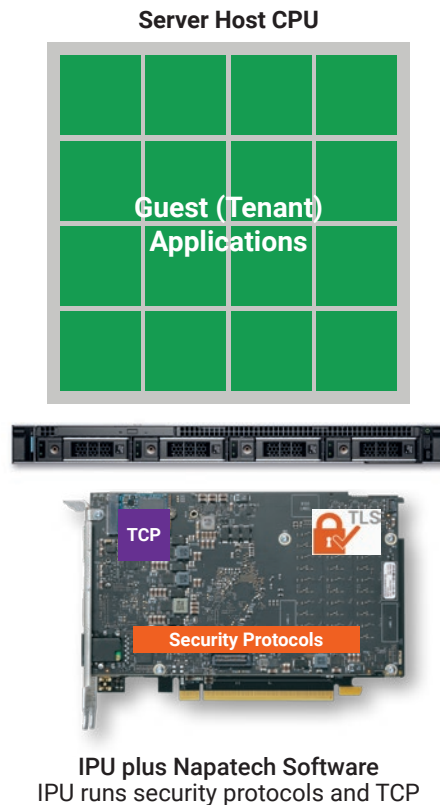


- **Performance Overhead:** Software-based TLS introduces additional computational overhead due to the encryption and decryption processes. This can lead to increased latency and reduced throughput, especially in high-traffic environments like data centers or high-performance computing clusters.
- **Scalability:** As the number of concurrent connections and the volume of data increases, software-based TLS implementations may struggle to scale efficiently. The encryption and decryption operations can become a bottleneck, limiting the overall system's ability to handle a large number of connections simultaneously.
- **Limited Hardware Acceleration:** While modern CPUs offer hardware instructions for cryptographic operations, not all software-based TLS libraries fully utilize these instructions. This means that the potential performance gains from hardware acceleration might not be fully realized.
- **Complexity and Maintenance:** Implementing and maintaining a software-based TLS solution can be complex. TLS libraries need to be updated regularly to address security vulnerabilities and stay compatible with evolving standards. This maintenance overhead can be burdensome, especially for organizations with limited resources.
- **Security Risks:** If the TLS library being used has vulnerabilities or is not properly configured, it can expose the system to security risks. A misconfigured or improperly maintained TLS implementation can negate the security benefits it aims to provide.
- **Key Management:** Managing cryptographic keys and certificates is a critical aspect of TLS security. In software-based implementations, proper key management practices are crucial to prevent unauthorized access or data breaches. Improper key management can lead to serious security vulnerabilities.
- **Compatibility and Interoperability:** Ensuring compatibility and interoperability across different software applications, platforms and versions can be challenging. Differences in TLS implementation choices and configurations can sometimes lead to communication issues.

For these reasons and more, a software-only architecture presents significant business and technical challenges for data center security.

## IPU-based security offload

Offloading the TLS protocol to an Infrastructure Processing Unit (IPU) which also runs services such as Transmission Control Protocol (TCP), addresses the limitations of a software-only implementation and delivers significant benefits to data center operators:



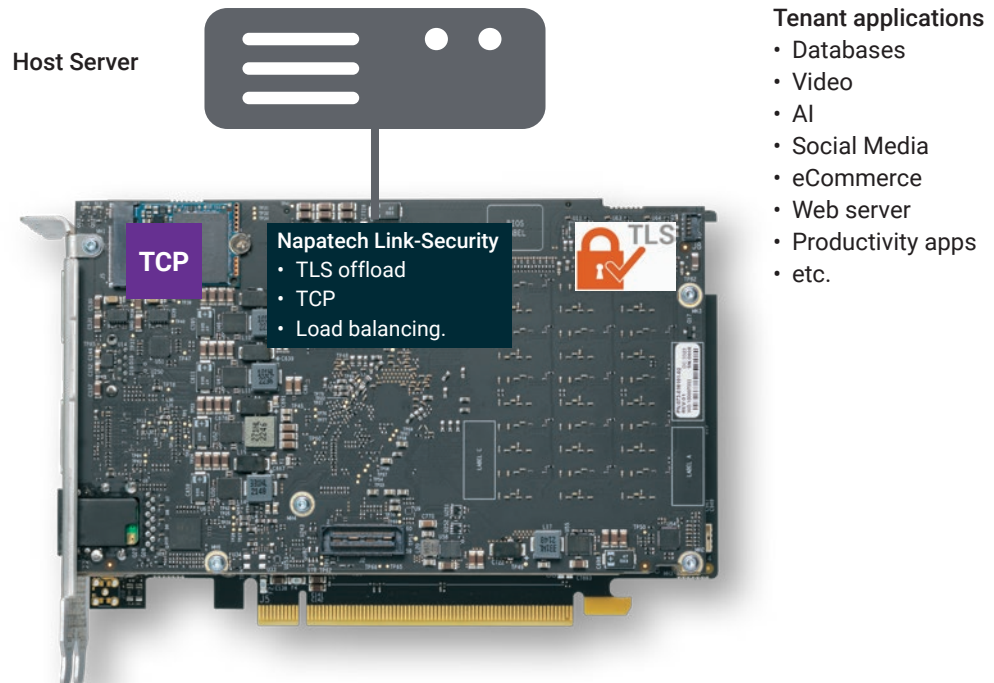
- **Resource Optimization:** Offloading the TLS protocol to an IPU frees up valuable CPU resources that can be used for guest (tenant) applications.
- **Performance:** IPU's are optimized to execute TLS encryption and decryption operations faster than general-purpose CPUs. Offloading TLS to an IPU leads to significant performance improvements, especially in scenarios where TLS processing is a bottleneck and/or there's a need to process a large volume of encrypted data.
- **Parallel Processing:** IPU's are designed for parallelism, allowing them to execute multiple tasks simultaneously. TLS operations involve mathematical computations that can be parallelized, enabling faster execution and more efficient resource utilization.
- **Scalability:** As traffic increases, IPU's can be scaled by adding more units to the infrastructure. This scalability helps maintain consistent TLS performance levels even when dealing with higher loads.
- **Low Latency:** IPU's can reduce the latency associated with TLS encryption and decryption. This is especially important for applications that require real-time communication, minimizing delays in data transfer.
- **Energy Efficiency:** Offloading TLS to an IPU and freeing up host CPU resources for guest applications can reduce the total number of servers required in a data center, resulting in energy savings and reduced OPEX.
- **Security Enhancements:** Many IPU's include hardware-based, zero-root-of-trust security features that enhance the security of TLS operations. These features provide additional protection against certain types of attacks and vulnerabilities.
- **Simplified Software Stack:** By offloading TLS operations to an IPU, the main CPU's software stack can be simplified, resulting in easier management and maintenance of the system. This can also lead to reduced security vulnerabilities.
- **Future-Proofing:** IPU's can be designed or updated in software to support new TLS encryption standards and algorithms as they emerge. This ensures that the data center infrastructure remains secure and compatible with evolving security requirements.

In addition to the above benefits that apply to the TLS workload, the IPU-based system architecture also introduces a security layer into the system, isolating system-level infrastructure processing from applications and revenue-producing workloads. This ensures that the TLS and TCP functions cannot be compromised by a cyber-attack launched by a tenant application. The infrastructure services themselves are secured since the boot process of the IPU itself is secure, while the IPU then acts as the root of trust for the host server.

## Napatech security offload solution

Napatech provides an integrated, system-level solution for data center security offload, comprising the high-performance Link-Security™ software stack running on the F2070X IPU.

See the sidebar for details of the F2070X IPU hardware.




The Link-Security software incorporates a rich set of functions, including:

- Full offload of TLS encryption and decryption from the host to the IPU;
- TCP processing, including TCP Checksum Offloading (TSO), Generic Receive Offload (GRO), Generic Segmentation Offload (GSO), Large Receive Offload (LRO) and checksumming;
- Load balancing to host CPUs;
- Web server acceleration (reduced page load time) with static file caching and image optimization;
- Enhanced security including Distributed Denial of Service (DDoS) mitigation and malicious traffic filtering;
- For legacy applications without TLS security, the IPU with reverse proxy adds TLS encryption layer on top of clear-text communications;
- Security isolation layer between the host CPU and the IPU, with no network connectivity exposed to the host.

Since the F2070X is based on an FPGA and CPU rather than ASICs, the complete functionality of the platform can be updated after deployment, whether to modify an existing service, to add new functions or to fine-tune specific performance parameters. This reprogramming can be performed purely as a software upgrade within the existing server environment, with no need to disconnect, remove or replace any hardware.





Napatech's integrated hardware-plus-software solution, comprising the Link-Security software stack running on the F2070X IPU, delivers high-performance TLS encryption and decryption without consuming host CPU resources by offloading the TLS workload from the CPU to the IPU while maintaining full software compatibility at the application level.



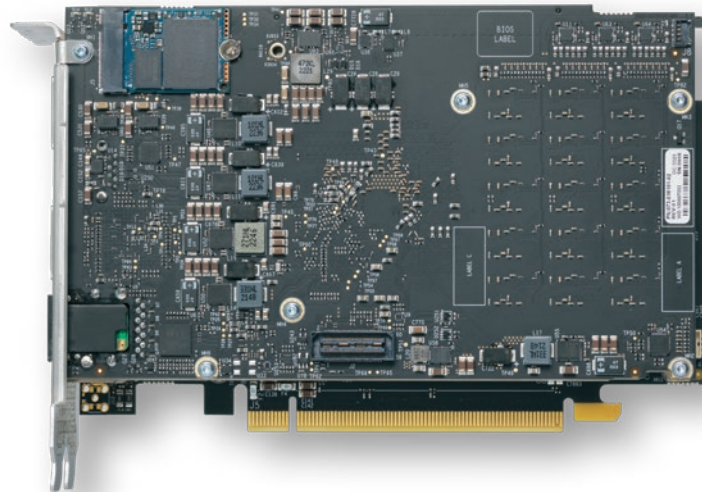
## Industry-leading performance

The Napatech F2070X-based security offload solution delivers industry-leading performance on benchmarks relevant to data center use cases, including 2x 100G line rate TLS encryption and decryption, while ensuring that no host CPU cores are utilized for TLS protocols.

This performance is measured as follows:

1. Run a web server (nginx) on the host CPU(s).
2. Run HTTP reverse proxy (nginx) on the IPU Xeon D processor.
3. Run an HTTP/HTTPS benchmarking application on another system to generate a load (HTTP requests) towards the web server.
4. Measure and record performance metrics.

*Note that the above benchmarks are preliminary pending general availability of hardware and software.*



## Summary

Within enterprise and cloud data centers, Transport Layer Security (TLS) encryption is used to ensure security, confidentiality and data integrity. It provides a secure communication channel between servers over the data center network, ensuring that the data exchanged between them remains private and tamper-proof. However, implementing the TLS protocol on the server's host CPU imposes significant compute overheads and limits the number of CPU cores available for running services and applications.

Napatech's integrated hardware-plus-software solution, comprising the Link-Security software stack running on the F2070X IPU, addresses this problem by offloading the TLS protocol from the host CPU to an IPU while maintaining full software compatibility at the application level.

Napatech's security offload solution not only frees up host CPU cores which would otherwise be consumed by security protocols but also delivers significantly higher performance than a software-based implementation. This significantly reduces data center CAPEX, OPEX and energy consumption.

The Napatech solution also introduces a security layer into the system, isolating system-level infrastructure processing from applications and revenue-producing workloads. This increases protection against cyber-attacks, which reduces the likelihood of the data center suffering security breaches and high-value customer data being compromised, while allowing customers full control of host system resources.

For more information, visit: Napatech at <https://www.napatech.com/support/resources/solution-descriptions/security-of-fload-solution/>

Napatech is the leading supplier of Smart Network Interface Card (SmartNIC) and Infrastructure Processing Unit (IPU) solutions used in cloud, enterprise, and telecom datacenters.

Through commercial-grade software suites integrated with high-performance hardware, Napatech accelerates network infrastructure and security workloads to deliver best-in-class system-level performance while maximizing the availability of server compute resources for applications and services.

Additional information is available at:  
[www.napatech.com](http://www.napatech.com)

**NAPATECH RECONFIGURABLE COMPUTING**

## EUROPE, MIDDLE EAST AND AFRICA

Napatech A/S  
Copenhagen, Denmark  
T +45 4596 1500  
[info@napatech.com](mailto:info@napatech.com)  
[www.napatech.com](http://www.napatech.com)

## NORTH AMERICA

Napatech Inc.  
Portsmouth, NH, USA  
T +1 888 318 8288  
[info@napatech.com](mailto:info@napatech.com)  
[www.napatech.com](http://www.napatech.com)

## ASIA-PACIFIC

[ntapacsales@napatech.com](mailto:ntapacsales@napatech.com)  
[www.napatech.com](http://www.napatech.com)