Solution Brief

Public Sector, Telco, Industry 4.0

Bringing Zero Trust Network Access (ZTNA) to Private 5G Networks

Zscaler's Zero Trust Exchange and SASE Connectors form the cybersecurity foundation for Trenton Systems Integrated Edge Solution 5G (IES.5G), an Intel® Xeon® Scalable processor-based platform designed for private 5G deployments

Enterprises are increasingly adopting private 5G networks to provide low-latency, scalable, and flexible wireless connections to a new generation of devices and machines, including IoT sensors, manufacturing robots, internal communications systems, production machinery, and more.

The availability of no-cost radio frequency spectrum in the U.S. (called Citizens Broadband Radio Service (CBRS)) and other countries was the last technical challenge to overcome and makes it possible for greater numbers of enterprises to deploy these networks using a systems integrator and best-of-breed platforms and network functions.

However, building a private 5G network could increase the risk of a cyber-attack by expanding an enterprise's attack surface. With more industrial devices connected to an enterprise's network, hackers have an increased potential to find a backdoor into the network for malware, ransomware, and other disruptive or criminal activities.

Anticipating this, Intel® Industry Solution Builders ecosystem members Zscaler and Trenton Systems have created the Integrated Edge Solution 5G (IES.5G) zero-trust security-enabled family of servers based on Intel® Xeon® Scalable processors. In addition to integrated security technology, the systems also feature workload acceleration technologies designed for 5G private networks.

Zscaler Protects Resources with Zero Trust Security

Zero trust is a cybersecurity strategy that assumes entities such as users, apps, services, operating systems, or devices must not be trusted by default. Before any connection is established—from an internal user or a remote user—trust must be established based on the entity's context and security posture. A zero-trust system must validate the user or entity whenever it requires new app access.

Another key element of a zero trust security system is operating on a least-privileged basis, which is a data access strategy that mandates that end users receive only the minimum access level needed to do their work.

Zero trust network access (ZTNA) applies this philosophy to remote network access. Also called a software-defined perimeter (SDP), ZTNA gives remote users secure connectivity to data center or cloud apps without placing them on the network or exposing the apps to the internet.

Zscaler delivers ZTNA for private 5G networks through its Zero Trust Exchange and secure access service edge (SASE) connector platforms, as shown in Figure 1.

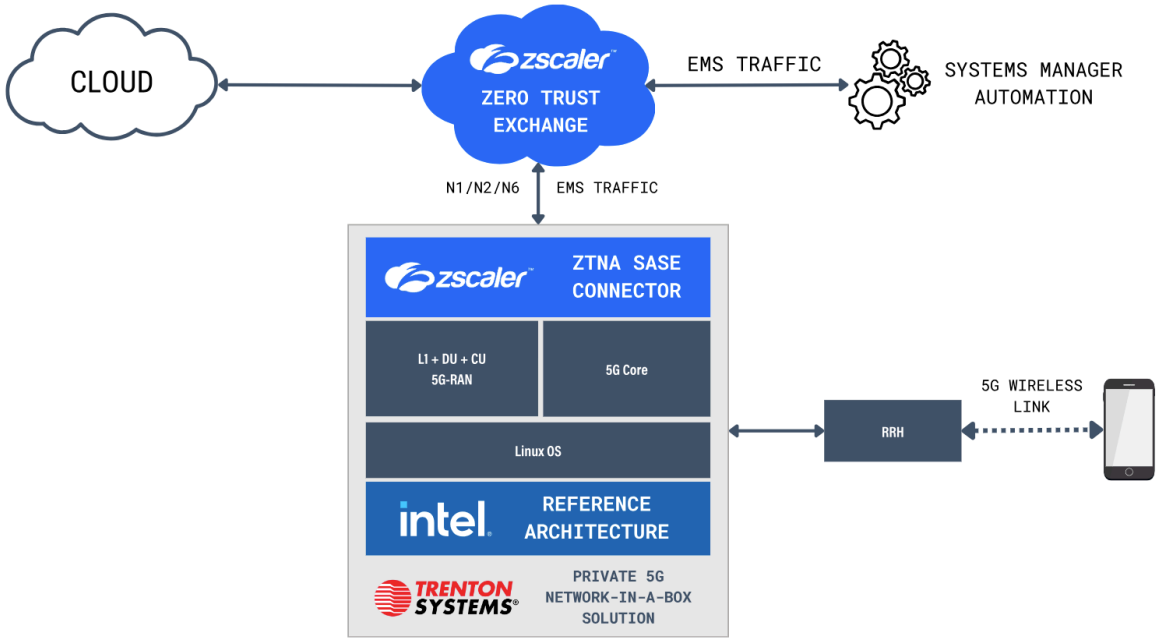

Figure 1. Block diagram showing how Zscaler's ZTNA technology can be deployed.

Zero Trust Exchange Secures Remote App Access

The Zscaler Zero Trust Exchange is a cloud-native platform that provides full zero trust security, including an adaptive trust model, where trust is never implicit, and policies dictate app access on a need-to-know, least-privileged basis. The platform follows a four-step process to implement ZTNA:

- Terminating the connection: Data packets enter the network destined for a particular resource. Zero Trust Exchange terminates that connection to facilitate deep packet inspection in the next steps.
- Verify access policy: The Zero Trust Exchange applies appropriate access policies to ensure the user has the proper resource and network access. It does this by verifying the user's identity, which is determined by considering the user's device, its location, and the application it is requesting. These data points are combined to authenticate the user.
- Inspect Content: The Zero Trust Exchange then inspects the content at IP layer 7 to detect malware.
- Broker connection: Once the user and data flow have been validated, the Zero Trust Exchange brokers a direct connection between the user and the requested application.

By connecting with the application directly, the cybersecurity attack surface is reduced, as is the possibility of lateral movement of malware—because malware cannot get access.

ZTNA SASE Connector for Branch Offices

The other security aspect of a 5G solution is the secure access service edge (SASE) for remote offices. The Zscaler SASE is cloud native and can run on the Trenton IES.5G and the 5G network functions.

The Zscaler SASE solution combines cloud-native security technologies with wide area network (WAN) capabilities to securely connect users, systems, and endpoints in a branch or remote office to applications and services anywhere. The five elements of Zscaler SASE are:

- First Software-Defined SASE Platform Built on Zero Trust: SASE architectures built on traditional SD-WAN could expand the attack surface and allow lateral threat movement undermining the zero trust architecture. Zscaler Zero Trust SASE is built on zero trust SD-WAN and AI to reduce business risk and network complexity.
- Secure Web Gateway (SWG): These gateways shield employees and users from accessing and being infected by malicious web traffic, vulnerable websites, internet-borne viruses, malware, and other cyber threats.
- Cloud Access Security Broker (CASB): CASBs ensure the safe use of cloud apps and services to prevent data leaks, malware infection, regulatory noncompliance, and lack of visibility. CASBs are good tools for securing cloud apps hosted in public clouds (IaaS), private clouds, or delivered as software-as-a-service (SaaS).
- Firewall as a Service (FWaaS): An FWaaS can replace physical firewall appliances with cloud firewalls that offer the same advanced Layer 7 / next-generation firewall (NGFW) capabilities, including access controls, such as URL filtering, advanced threat prevention, intrusion prevention systems (IPS), and DNS security.
- Centralized Management: The Zscaler SASE allows the management of services from a single console. This centralized management delivers consistent policies and eliminates the challenges of change control, patch management and coordination of outage windows.

Trenton IES.5G is Optimized for 5G Private Networks

The IES.5G is optimized for the performance requirements of private 5G networks and is architected to be zero trust based on tight integration with Zscaler technology.

The server family is part of Trenton's custom solutions product line. Available in 1U, 2U, 3U, and custom form factors, the IES.5G is a compact and rugged system that can be rack mounted or be deployed in a ruggedized chassis that is hardened for outdoor locations and can withstand dust, dirt and debris, extreme shock, vibration, temperature, and humidity.

The Trenton Systems IES-5G platform is a revolutionary solution designed to meet the demanding requirements of high-performance computing in rugged environments. Featuring a ruggedized design and an advanced thermal management system, the IES.5G ensures durability and optimal performance even in harsh conditions. With support for the latest 5G connectivity standards, this platform enables high-speed data transfer and low latency, making it ideal for mission-critical applications in defense, aerospace, telecommunications, and beyond. Its scalability allows it to adapt to varying computational needs, providing enhanced reliability, improved processing power, and future-proof connectivity. The IES.5G brings unmatched performance, reliability, and long-term cost-effectiveness, making it the go-to choice for embedded computing solutions in challenging environments.

High Performance Compute from Intel® Xeon® Scalable processors

The highest-performance IES.5G servers are powered by the latest generation Intel Xeon Scalable processors, including 5th, 4th, and 3rd generations. These processor families deliver compute agility and scalability. They benefit from decades of innovation for the most in-demand workload requirements. Intel Xeon Scalable processors feature an optimized architecture that supports Open RAN and other workloads with built-in acceleration and hardware-based security features.

Trenton has integrated Intel® FlexRAN reference software into the IES.5G. The software provides PHY and MAC layer processing when running on an Intel processor. It delivers flexible and programmable control of the layer 1 wireless infrastructure through modular, virtualized control functions with well-defined interfaces.

For additional layer 1 performance, Trenton's Intel Xeon Scalable processor-based systems support specialized accelerators to process computationally heavy layer 1 tasks such as low-density parity check (LDPC) decoding and forward error correction (FEC). This acceleration is integrated into the 4th Gen Intel Xeon Scalable processor and is available on a discrete card (Intel® vRAN Accelerator ACC100 Adapter) for use with 3rd Gen Intel Xeon Scalable processors.

The Trenton Systems solution also uses Intel® QuickAssist Technology (Intel® QAT) to provide hardware acceleration for cryptography processing, including IPsec and TLS networking. Previously offered as a discrete offering, Intel QAT is now available as an integrated accelerator in 4th Gen and 5th Gen Intel Xeon Scalable processors.

For performance and data protection, the systems also offer up to 24 slots of DDR4/5 memory and high-capacity self-encrypting drives. For connectivity, IES.5G systems offer built-in Ethernet ports supporting up to 100GbE.

Ready for Integration

To create a network using the IES.5G, Trenton works with system integrators (SIs) to add the 5G core, radio access network (RAN), and other applications needed for a particular deployment. As many SIs have created or standardized on their own 5G network functions, this strategy provides integrators with a flexible, scalable, and secure platform for their software.

ECS Develops a Complete Solution

One system integrator that Zscaler and Trenton turn to for a complete 5G solution is Equus Compute Systems (ECS) which has a long history of building telecom and 5G networks.

ECS leverages its innovation-as-a-service platform for its success in designing, building, and deploying the digital infrastructure that MNOs need for 5G success.

ECS services range from integration and deployment, hardware design, infrastructure-as-a-service and software engineering to ESG-as-a-service, network operations center and executive briefing center. In addition, we feature our Innovation Lab allowing organizations to demo and test POCs on our AI/ML, cybersecurity, and immersion cooling appliances among others.

Trenton Systems has embraced a vendor-agnostic approach to implementing private 5G networks using the IES.5G. This approach allows customers to access a variety of 5G Open RAN, 5G core, and management and orchestration software frameworks. As a result, customers and systems integrators can deploy, orchestrate, and manage the entire solution from beginning to end.

Conclusion

Private 5G networks are growing in popularity, but they can increase an enterprise's cybersecurity risks by expanding its attack surface. ZTNA provides a cybersecurity solution that ensures that users are who they say they are before being granted application access. By authenticating each user and each app every time a connection is made and then brokering that connection, Zscaler's Zero Trust Exchange software protects against cybersecurity incidents and reduces the attack surface.

Trenton Systems has built Zero Trust Exchange functionality into its IES.5G server that uses Intel technologies for performance and capabilities, including Intel Xeon Scalable processors, Intel FlexRAN, and Intel QAT to name a few. The result is a system that system integrators can use to deploy manageable, scalable, and secure private 5G networks.

Learn More

Zscaler 5G Solutions

Trenton Systems IES.5G

Intel® Xeon Scalable Processors

Intel Industry Solution Builders

Equus Compute Solutions (ECS)

Notices & Disclaimers