zscaler™ | KLAS GOVERNMENT

Partner Brief

Deploying Zero Trust at the Tactical Edge

Being connected to the internet 24/7/365 with high-speed communication networks is no longer a luxury—it's an expectation. We expect to find the information we need, when we need it, without interruption. But for our tactical edge—the service members deployed on the front lines—the environment is very different.

For tactical communicators, the ability to securely connect to the internet from literally anywhere can be a matter of life and death; the difference between a successful mission and one that fails; or accurate intelligence delivered in time or too late.

In response to these needs, the Department of Defense (DoD) created the concepts of the tactical cloud edge and tactical compute nodes. The tactical cloud edge is typically hosted in-theater, such as at a regional hub node or on a vessel close to the warfighter, to bring the cloud physically within reach. In addition, tactical compute nodes are easily transported inside smaller vehicles and provide localized computing and storage that syncs with the tactical cloud edge when it is available.

But this begs a question: How do you secure communication to the open internet and the resources hosted within the tactical cloud without putting users on the network, exposing the warfighter to the enemy, or jeopardizing the mission?

The answer? A zero trust solution at the tactical edge.

Zscaler and Klas—extending zero trust to the tactical edge

Zero trust architectures maintain strict access controls, trusting no one by default—even those already inside the network perimeter. Unlike traditional network security approaches that expose applications to the internet and open the door for lateral movement, the Zscaler Zero Trust Exchange™:

- Connects users and devices to apps, not networks, to eliminate lateral threat movement
- Makes applications and users invisible to the internet, thus reducing the attack surface
- Uses a proxy architecture—not a passthrough firewall—to provide full content inspection, including encrypted traffic, and security

Zscaler, deployed and integrated with Klas Voyager's extreme network edge technology, provides warfighters the security, mobility, access, and ease they need in the field.

Klas Voyager Tactical Data Center (Voyager TDC)

Technology overview

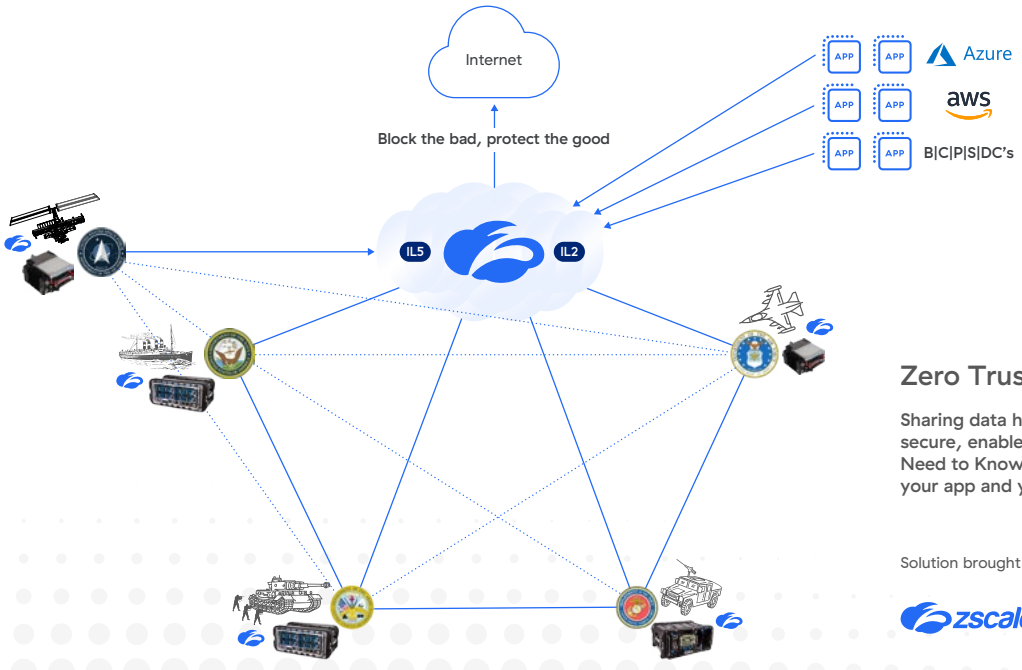
Zscaler Government Cloud comprises of two services—Zscaler Private Access™ (ZPA™) and Zscaler Internet Access™ (ZIA™).

ZPA is the first and only DoD Impact Level 5 (IL5) and FedRAMP-High JAB Authorized zero trust architecture solution. The cloud native solution provides remote access to internal applications running on the tactical cloud, a tactical compute node (such as Klas Voyager TDC), or a private data center. With ZPA, applications are never exposed externally, making them completely invisible to unauthorized users. The service enables warfighters to connect to mission applications via connections brokered in the Zscaler Government Cloud (or an on-premises extension) instead of extending the network to users. ZPA is 100% software-defined, so it requires no physical appliances.

ZIA is a FedRAMP-High "In-Process" secure internet and web gateway delivered as a service from the cloud. Think of it as a secure internet on-ramp—all you do is make Zscaler your next hop to the internet. This allows tactical users on expeditionary missions to utilize the enemy's networks to securely connect back to mission resources without being exposed to malicious threats.

Klas Government provides rugged, low size, weight, and power (SWaP) deployable communication solutions that enable rapid insertion of commercial technology for the tactical environment. Deploying Voyager compute modules at the edge allows data to be accessed and processed on-site, reducing the amount of data required to traverse transmission links while enabling C2 when those links are degraded or lost.

Klas Government's MIL-STD 810 and MIL-STD 461 Voyager modules can be the tactical cloud edge that operates and enables cloud-delivered capabilities both when connected and during times of contested/denied transport.



Zero Trust at the Tactical Edge

Sharing data has never been easier or more secure, enabled by leveraging "Digital Dynamic Need to Know." For mission success, just bring your app and your users—we do the rest!

Solution brought to you by

zscaler™ | KLAS GOVERNMENT

Conclusion

Together, Zscaler and Klas provide DoD and military components with secure access to the internet, internally managed applications, and compute resources. Warfighters and mission partners can access the information they need and are authorized to access it without compromising the integrity of the underlying architecture's security itself. Zscaler and Klas provide a consistent way to manage access and establish expeditionary networks regardless of whether teams are CONUS or OCONUS, TDY or deployed, or serving in maritime conditions.

Ready to bring zero trust to the tactical edge?

Request a virtual demo or proof-of-value of this solution by visiting zscaler.com/federal.

About KLAS Government
Klas Government makes the world's most powerful technology for the tactical edge. We provide rugged, low size, weight and power (SWaP) deployable communications solutions to meet the needs of government and military communicators in any operational environment. Klas Government enables customers to communicate more and carry less by delivering tactical and executive communications systems specifically designed for ultimate flexibility, scalability and portability. Klas Government's capabilities include product design and configuration, network management, solutions development, fielding and training.

KLAS GOVERNMENT

zscaler™ | Experience your world, secured.™

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com