SECURING SPACE MISSION: CYBERSECURITY FOR SPACE SYSTEMS

Space & Cybersecurity

Legacy cybersecurity models rely on static boundaries and trusted zones. But in today's contested, connected, and cloud-enabled space environment, this is no longer sufficient.

Modern space systems are moving toward Zero Trust architecture to meet mission security requirements. This approach implements unified access management across user interfaces, application interfaces, and data at rest.

The layered approach recognizes that it cannot always eliminate all risks but works to limit the consequences of security breaches. **Zero Trust architecture looks ahead to future deployments**, including public cloud implementations that will require enhanced security measures.

What's Changing?

Without Zero Trust
- Static access controls
- No "secure by design"
- Easy to make mistakes in access management
- Little security on satellite link

With Zero Trust
- Dynamic, risk-based access
- Secure by design
- Unified access management
- Security on satellite link

Why Zero Trust?
- "Never Trust, Always Verify"
- Continuous authentication & authorization
- Real-time threat detection & response

Terma's Approach towards Zero Trust

Terma makes a major step toward Zero Trust cybersecurity tailored for space missions, where every connection, system, and user are verified.

Limits number of technologies:
- NATS
- REST
- Web UI

Flexible & platform neutral
- Bare metal
- Public / private cloud
- Windows / Linux

If you have questions, please contact our team terma.space@terma.com