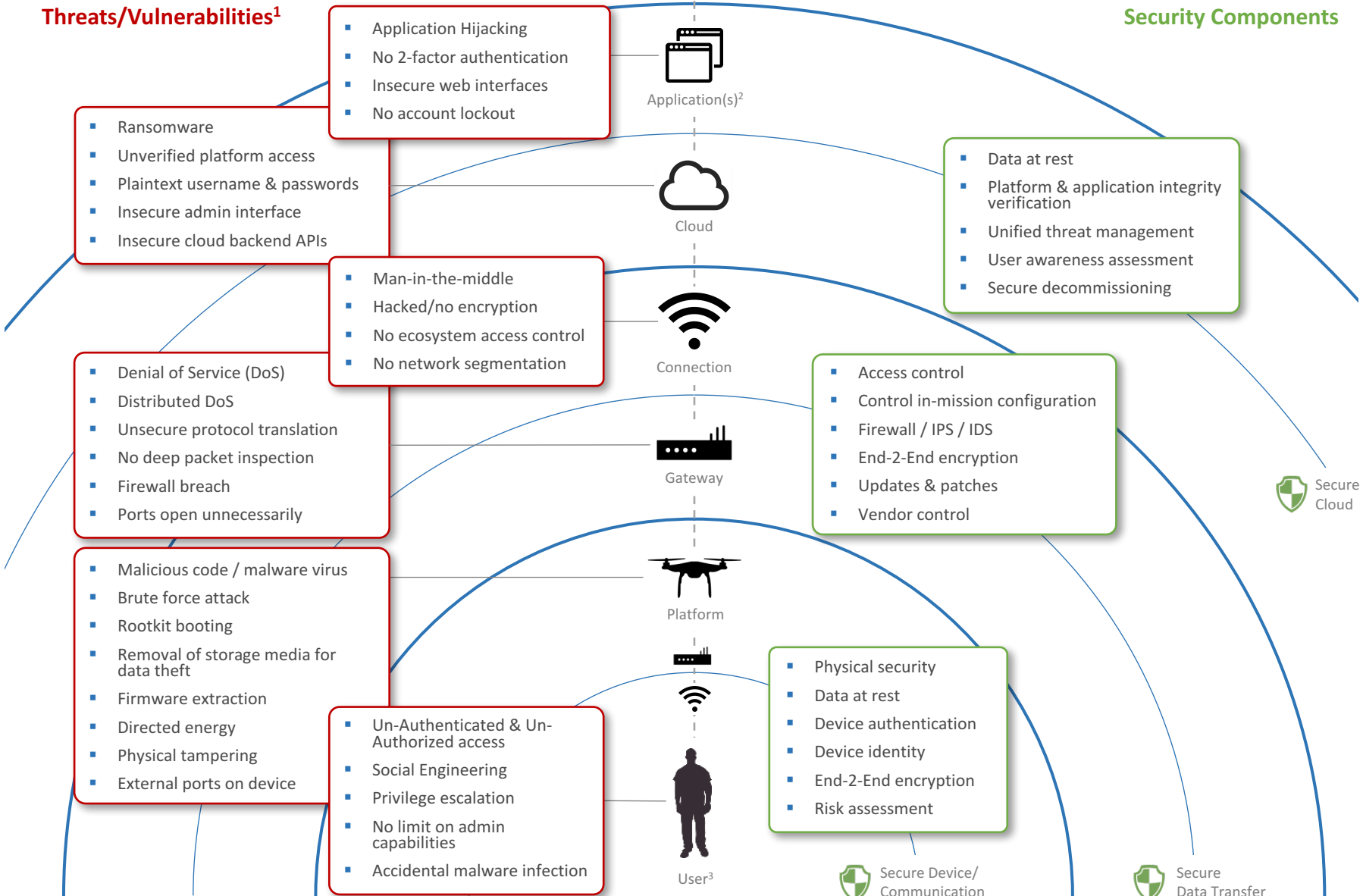


The Layer-Cake of Drone Data Protection

Threats/Vulnerabilities¹

Security Components



- Ransomware
- Unverified platform access
- Plaintext username & passwords
- Insecure admin interface
- Insecure cloud backend APIs

- Application Hijacking
- No 2-factor authentication
- Insecure web interfaces
- No account lockout

- Denial of Service (DoS)
- Distributed DoS
- Unsecure protocol translation
- No deep packet inspection
- Firewall breach
- Ports open unnecessarily

- Man-in-the-middle
- Hacked/no encryption
- No ecosystem access control
- No network segmentation

- Malicious code / malware virus
- Brute force attack
- Rootkit booting
- Removal of storage media for data theft
- Firmware extraction
- Directed energy
- Physical tampering
- External ports on device

- Un-Authenticated & Un-Authorized access
- Social Engineering
- Privilege escalation
- No limit on admin capabilities
- Accidental malware infection

- Data at rest
- Platform & application integrity verification
- Unified threat management
- User awareness assessment
- Secure decommissioning

- Access control
- Control in-mission configuration
- Firewall / IPS / IDS
- End-2-End encryption
- Updates & patches
- Vendor control

- Physical security
- Data at rest
- Device authentication
- Device identity
- End-2-End encryption
- Risk assessment

¹ Attacks on identity & access management is a possible threat on all layers

² e.g.: CRM, ERP, SCM, PLM

³ User: can represent a person, device, process, application or system