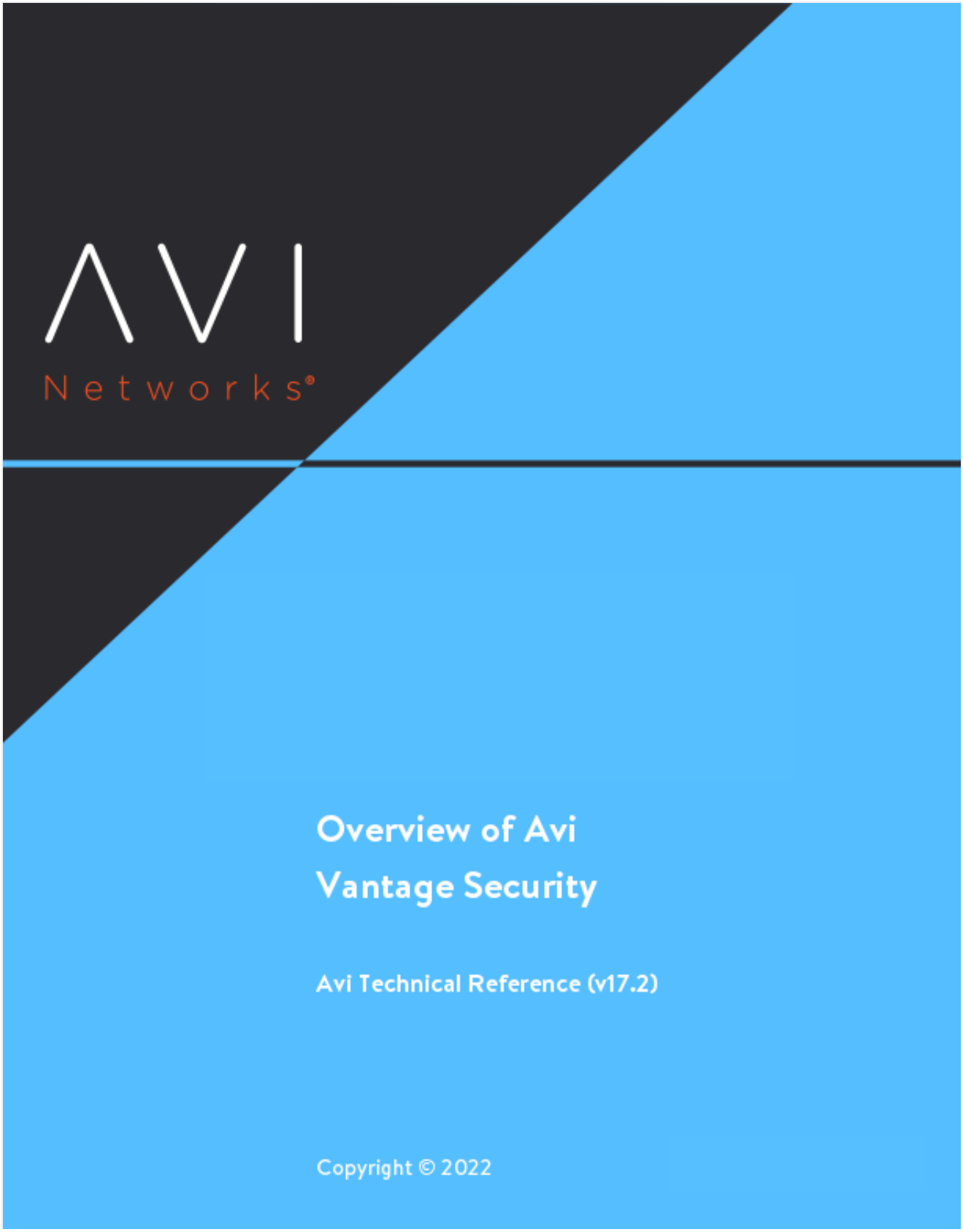

Overview of Avi Vantage Security

Avi Technical Reference (v17.2)

Overview of Avi Vantage Security

view online

Avi Networks strives to ensure the highest level of security, adhering to rigorous testing and validation standards. Avi Vantage includes numerous security related features to ensure the integrity of the Avi Vantage system as well as the applications and services protected by Avi Vantage. This article is focused on the security of Avi Service Engines and Avi Controllers.

Industry Validation

Many of the largest and most trusted brands on the Internet have subjected Avi Vantage to their own testing, or testing by third party companies such as Qualys and Rapid7. This continuous testing ensures that in addition to the proven success of Avi Vantage in public and private networks, it has been thoroughly vetted by known industry security leaders.

The following are a few examples of web UI and other attack vectors tested via external penetration testing:

- SQL injection
- Cross site request forgery (CSRF)
- Cross site scripting (XSS)
- Arbitrary code execution
- Credential disclosure
- Clickjacking
- Improper cookie settings
- Password protection via PBKDF2
- Encryption of SSL certificate's private keys
- Role based access control
- Strong output validation to guard against disclosure of sensitive fields such as passwords, export of keys

Patching Security Issues

Despite the best attempts to proactively resolve any potential threat prior to the release of code, it is important to ensure a solid plan of action in the event a security hole is discovered in customer deployed software. Avi Networks strongly recommends key administrators subscribe to Avi's mailing list. Security alerts are proactively sent to customers to notify them if an issue has been found and the potential mitigation required. Subscribe via Avi's customer portal. Avi also publishes responses to Common Vulnerabilities and Exposures (CVEs) of note, which include known vulnerabilities in Avi Vantage or software used by it, such as SSL and Linux. Avi may also publish CVE responses to issues that do not impact Avi Vantage to explicitly inform our customers that they are protected. These CVEs are published to the Avi Knowledge Base site, but not sent proactively via email alerts. See also:

- Support Terms & Conditions
- CVEs
- Upgrade Avi Vantage Software

Hardening Avi Vantage

With a basic deployment of Avi Vantage, the system is secured and reasonably locked down. However, many administrators may wish to customize the security posture or further tighten policies regarding who can access Avi

Vantage. Avi strongly recommends thoroughly reviewing the choices for securing Avi Vantage which are essential to guarantee the security of Avi Vantage in production environments where the potential exposure to malicious attack is more severe.

- User Account Management *Protocol Ports Used by Avi Vantage for Management Communication
- Controller-to-SE Communication
- Clickjacking Protection
- Securing Management IP Access