



Tectia[®] SSH Client/Server vs OpenSSH

Comparison sheet

Summary

Tectia is the original SSH Client/Server with almost 30-year-long history. It is a commercially maintained product supported by an in-house team of experts.

Over the years, Tectia has been developed into a future-proof solution offered also in a [Quantum-Safe Edition](#) and [Zero Trust Edition](#).

[OpenSSH is an open-source product](#) based on the original Tectia SSH Client/Server.

In a fashion that is typical for open-source products, it is managed and maintained by volunteers only. Despite that, OpenSSH is incorporated into many commercial products.

	TECTIA		OPENSSH	
Costs	\$\$	Subscription costs based on the size of the IT environment	-	No initial costs (open-source software)
Software management	-	No management costs (included in the subscription costs)	\$\$\$	Requires in-house expertise (integration, salaries, open-source licence management)
Authentication integration	-	None, is bundled along with the product	\$\$	Requires in-house expertise (maintenance, salaries)
Support	\$\$	Expert support based on customer requirements	\$\$\$\$	No expert support/limited support
Compliance	-	Guaranteed by SSH	\$\$\$\$	Cannot be guaranteed (risk of non-compliance and potential fines)
Post-quantum cryptography (PQC) risks	-	Tectia is offered as Tectia Quantum-Safe Edition	\$\$\$\$\$	Unclear path to PQC (data isn't protected, it can be captured and decrypted later)
Back-door entry	-	Tectia narrows down the possibility of back-door entry	\$\$\$	Potential back-door entry

Note: Dashes and dollar signs represent a scale from - (no attached costs) to **\$\$\$\$\$** (the highest attached costs).

Detailed overview

		TECTIA	OPENSSH
Costs	Initial purchase costs	Relatively large, depending on the size of server estate and other factors	No initial costs for the software itself, but need to allocate in-house experts' time for installation and configuration
	Maintenance costs	Distribution packages ensure no need for in-house maintenance	Need to allocate in-house experts' time for maintenance, potential training costs
	Costs to accommodate X.509*	Supported without any additional costs	Another CA that can handle SSH certificate signing and issuance
Software management	Platform updates	Compiled and tested packages for all key platforms, centralized distribution of updates	Updates from multiple sources and patches separately for each platform can add administrative costs
	New software release	Consistent release cycle covering all separate platforms	Release cycles and policies are different for each source which multiplies maintenance
	Compatibility and integration	No compatibility and integration risks	Need to document all steps involved in deployment and maintenance
	Technology expertise	No need for in-house expertise	Need to maintain expensive in-house expertise, or alternatively use professional support (e. g. OpenSSH by SSH)

* X.509 is a widely supported protocol, so chances are that your organization already maintains trust with an internal or external X.509 CA, which can be utilized without any modification with Tectia.

		TECTIA	OPENSSH
Authentication integration	Authentication integration needs	Incorporates broad, tested, and documented authentication integration	Requires in-house development (requirement specification, development, testing, documentation, and maintenance)
	Needed in-house resources	Minimizes in-house engineering and other integration costs	Need for in-house project management and software engineering resources, need to rely on third-party patches with limited support
Support	General support	Dedicated professional support up to 24/7, R&D in the same organization	Support available from platform vendors, R&D are unpaid volunteers
	Support requests	Single point of contact for all Secure Shell related support requests	Multiple points of contact in Secure Shell related inquiries, inconsistent support and maintenance policies between different platforms
	Platform support	Extensive, consistent support packages available for all platforms	Limited support for Unix bundled OpenSSH packages, no support for in-house OpenSSH compilations
Compliance	General compliance	Enterprise-class feature set specifically created to address regulatory demand	Risk of non-compliance
	FIPS	Compliant	Compliance dependent on a platform vendor / non-compliant
Other	Path to post-quantum cryptography (PQC)	Supports post-quantum encryption algorithms recommended by NIST/BSI, protection against quantum attacks	Unclear path toward post-quantum cryptography
	IPR risks	In-house developed implementation means no IPR risks for customers	IPR infringement risks
	Future of the software	Extensive product roadmap developed and reviewed with customers	Uncertain future product roadmap

Looking for more information?

Interested in seeing Tectia in action?

[CONTACT US](#)