SSH

SOLUTION BRIEF

Role-Based Access: Secure Access with Tectia Zero Trust

Every cyberattack begins with misplaced trust

Don’t trust, always verify. Built around this principle, the Zero Trust paradigm challenges traditional IT security models.

The traditional ‘castle’ security model seeks to protect networks from outside threats but inherently trusts individuals or devices already within the network. This kind of approach is flawed as it leaves open the possibility for bad actors to roam freely and unchecked within the corporate network, accessing more corporate data along the way and increasing the scale and severity of a potential cyberattack.

Tectia is the original SSH (Secure Shell) client/server solution. Widely used by large corporations in financial and other industries, Tectia is repeatedly chosen because of its operational efficiency, usability, reliability, and enterprise-level support services.

We at SSH not only invented Secure Shell and developed Tectia, as the original solution, but we also consistently improve and make Tectia future-proof.

More than 20 years ago, we have introduced X.509v3 certificates to Tectia, followed by SHA2 algorithms that later became RFCs. In 2021, among other recent improvements, we launched Tectia Quantum-Safe Edition - an upgrade with Quantum-ready encryption algorithms. It ensures that encrypted communications captured today cannot be unencrypted in the future even with a quantum computer.

This paper covers another important upgrade available: **Tectia Zero Trust Edition**.

Tectia Zero Trust Edition makes it easy for our Tectia customers to take into use the recommended security paradigm of Zero Trust and leverage the full capabilities of their existing Tectia Client/Server infrastructure.

About Zero Trust

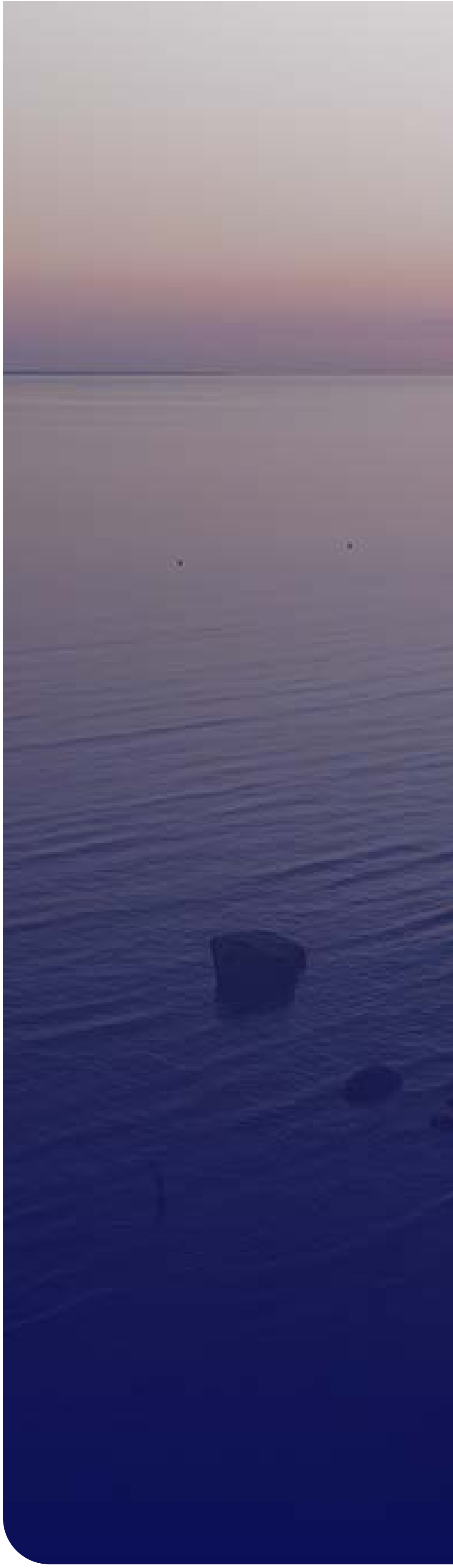
First described by John Kindervag in 2010, now defined by the National Institute of Standards and Technology (NIST) and highlighted by US President Biden, the Zero Trust security approach is becoming the new normal in information security. Zero Trust is not based on where you are, but who you are. Instead of relying on network- and perimeter-based access, Zero Trust emphasizes authentication based on roles.

For example:

- All devices in your organization must be treated as if they were freely accessible from the Internet.
- All devices and services must be authenticated based on users' roles.
- All application users (service account/functional) must authenticate themselves the same way as humans do.

The traditional perimeter defense approach is no longer sufficient in the modern world. Perimeters can be penetrated and you need to be prepared to keep your systems secure regardless of that. It is crucial to keep resources safe and their usage properly audited in distributed working environments and increasingly complex infrastructures. In order to do so, a scalable and more powerful approach is needed: Tectia Zero Trust Edition.

The good news for Tectia users is that Zero Trust can be achieved without a complete redesign of the existing infrastructure and working processes.



Towards Zero Trust

Rather than a single magic bullet, Zero Trust is a set of security principles that complement one another. For example, all network traffic, including internal networks, needs to be encrypted. This is something that Tectia already does by design. In case there are still unencrypted connections between servers, any TCP connections can be still secured with the automatic tunneling functionality that is already provided by Tectia.

Perhaps the most important step to take towards Zero Trust is eliminating standing credentials. This leads to a ‘defense in depth’ policy where actors in internal and external networks are treated the same and trust is no longer based on location. It also leads towards the elimination of permanent tokens that were granted or self-provisioned after proper authentication and can be used to shortlist users or systems for faster access. These tokens could be stolen and misused and getting rid of them removes a significant vulnerability in your system.

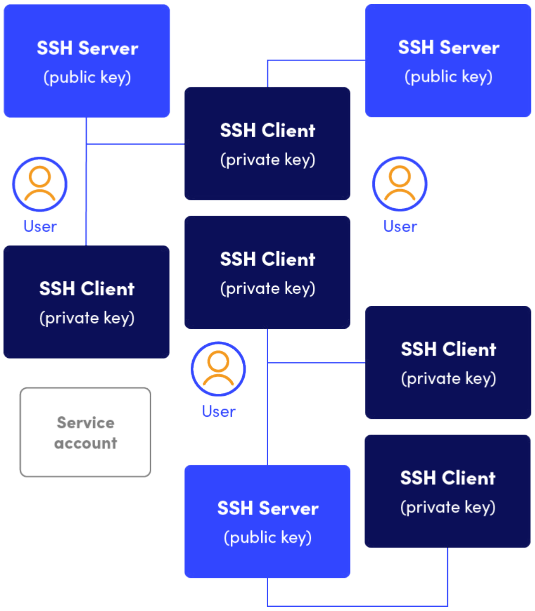
In a Zero Trust infrastructure, access is granted separately for each session and verified for each connection. Similarly, all sessions and connections are logged for auditing, so a malicious actor cannot cover their tracks and erase evidence of their past actions.

Zero Trust for Tectia

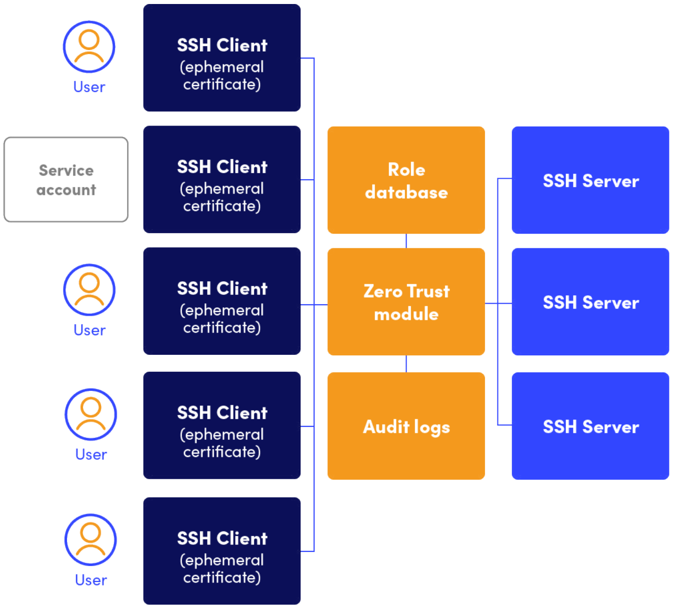
Existing organization infrastructures, including infrastructures governed by third-party organizations, often contain Tectia in an essential role protecting critical data in transit, both in public and corporate networks. When implementing Zero Trust with Tectia or any other Secure Shell solution, the major undertaking concerns eliminating standing credentials, like plain Secure Shell public keys which often are not only permanent but also user-controlled.

In Tectia Zero Trust Edition, the traditional plain public/private key pair is no longer accepted for user authentication. Instead, it is replaced by Just-In-Time (JIT) ephemeral (short-lived) certificates that are compatible with either X.509v3 Public Key Infrastructure (PKI) or, alternatively, OpenSSH Certificates.

User authentication and authorization, within the Zero Trust certificate-based architecture, are delegated to a central authority - the high-availability Zero Trust module. When a legitimate user wishes to initiate a secure connection, the user's client first contacts the Zero Trust module and authenticates within it. If authorized by the Zero Trust module, the client obtains a server-specific short-lived certificate. Then, the client can use the certificate to access the Tectia Server, which identifies the user from information in the certificate. After that, all is clear for the secure session to commence.



Your SSH server estate before Tectia Zero Trust Edition - SSH keys are scattered around your estate without clear ownership.


User
SSH Client (ephemeral certificate)
Service account
SSH Client (ephemeral certificate)
Role database
SSH Server
User
SSH Client (ephemeral certificate)
Zero Trust module
SSH Server
User
SSH Client (ephemeral certificate)
Audit logs
SSH Server
User
SSH Client (ephemeral certificate)

Your SSH server estate after implementing Tectia Zero Trust Edition with the Zero Trust module.

Tectia Zero Trust Edition utilizes **role-based access control (RBAC)**, which means that the user's access rights depend on the role the user currently has, rather than their identity. This type of access control allows dynamic addition and removal of access; both changes are instantly reflected in the entire environment, as Tectia Zero Trust Edition syncs with the Identity and Access Management (IAM) system in use.

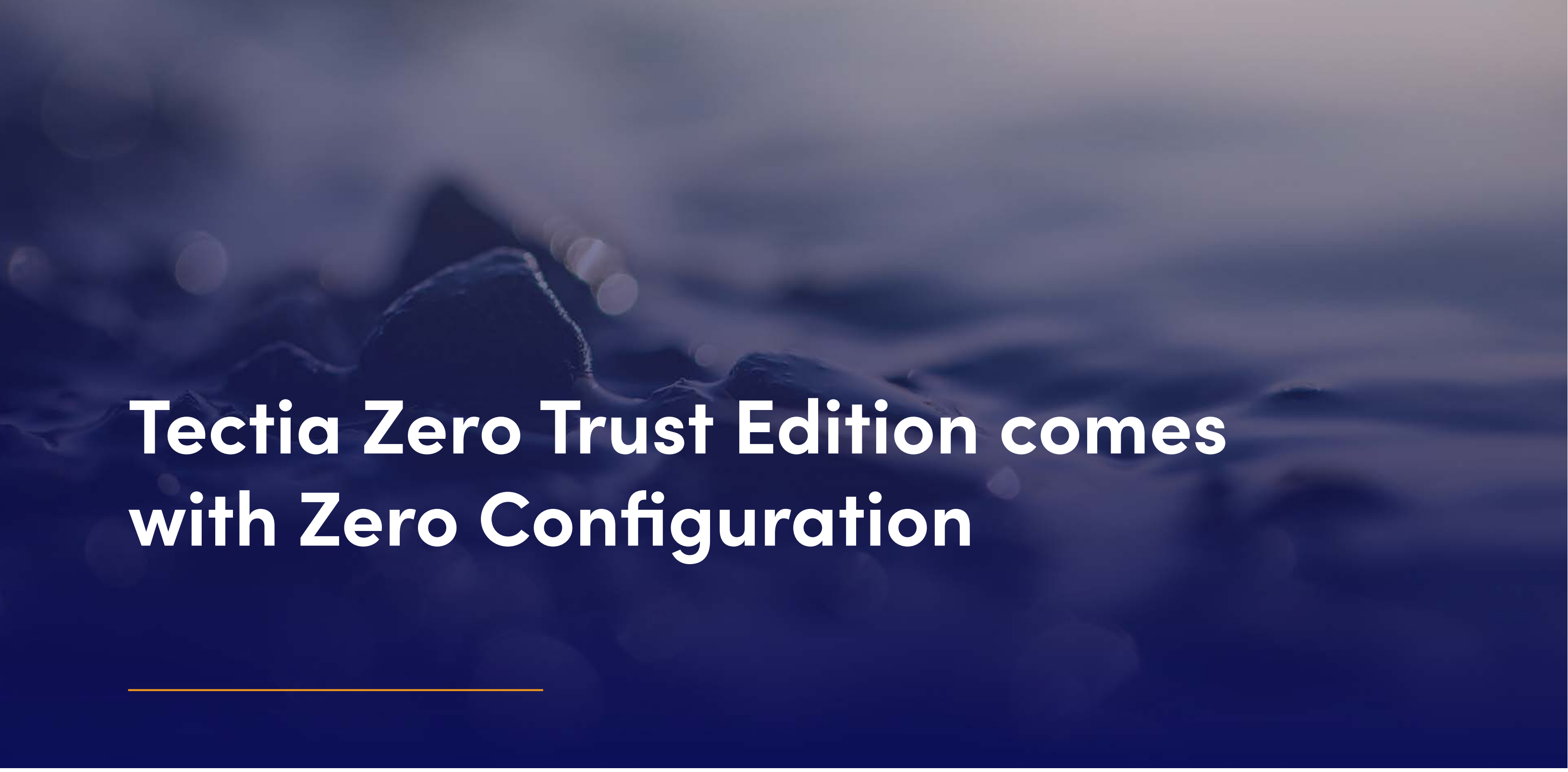
The benefits are obvious. In addition to implementing defense in depth, Tectia Zero Trust Edition also significantly simplifies credentials management.

For example, when an employee is transferred to another department, it is enough to remove or demote the old access rights and add any new rights to the Zero Trust module. Compare this to having to separately remove or add dozens or even hundreds of keys in a large server base.

It is equally important that the individual Secure Shell users/clients never possess private keys corresponding to their short-lived certificates. This way, the users cannot mishandle or share secrets they do not have.

Access and auditing logs are also easy to create, since the Zero Trust module is always logging all Secure Shell connections and can integrate with SIEM solutions.

Additionally, users have no means to erase their trails. Entire sessions can be recorded, searched, and re-played as a video, helping an auditor to get an exact picture of what happened at any point in time. Thanks to the fact that the full audit trail allows full accountability on who did what and the users no longer have access to the credentials, even shared accounts can be still used safely on target servers. Login-as-self is also supported if the environment has user-specific regular and/or privileged target accounts.



Tectia Zero Trust Edition comes with Zero Configuration

Tectia Server configuration itself can be immutable, even if the authorized target accounts in Zero Trust module change over time with new use cases.

Tectia Zero Trust Edition is officially supported for Tectia Server version 6.4.18 and above, but Tectia X.509v3 certificates will work with any Tectia Server version.

Zero Trust is the paradigm of the future. Fortunately for our Tectia users, the new Tectia Zero Trust Edition upgrade will provide them with the benefits of Zero Trust: role-based access control (RBAC), simple centralized credentials management, and easy logging and auditing support.

With this upgrade already available and other significant upgrades, your Tectia estate is indeed future-proof!

Learn more about Tectia Zero Trust at the SSH website →

SSH

Finland

SSH Communication Security Oyj
Karvaamokuja 2 B 00380 Helsinki
www.ssh.com
+358 20 500 7000
info.fi@ssh.com

USA

SSH Communication Security, INC.
434 W 33rd Street, Suite 842
New York, NY, 10001 USA
www.ssh.com
+1 781 247 2100
info.fi@ssh.com

Hong Kong

SSH Communication Security LTD.
35/F Central Plaza, 18 Harbour Road
Wan Chai
Hong Kong
www.ssh.com
+852 2593 1182
info.fi@ssh.com