



Secure & User-Friendly Download Center

Challenge

A leading cybersecurity solution provider wanted to replace their legacy download center. This system helped track product downloads while assigning stratified authorization access to customers based on product tier levels. The previous process featured excess integration points that were prone to human error and required additional manual steps to generate audit reports, decreasing overall usability.

The vendor wanted to implement a solution that would improve administrative reaction times, increase control over the download center, harness automation, and provide seamless integration compatible with existing software systems. The vendor also hoped to fortify the security of the entire process by embracing quantum-safe technology capable of combatting the advanced breach attempts of the future.

Solution

The Tectia Zero Trust Edition solution was implemented, extending Tectia's excellent backend security functionalities with a role-based hybrid privileged access management frontend. Tectia Zero Trust Edition relies on traditional public key authentication and ephemeral certificates, as well as the latest quantum-safe algorithms, for all-around protection. With this solution, roles can be assigned to end-users to ensure that the right customers are directed to the right product tier every time they log in to their account. This hybrid solution provides a modern and secure HTML5 user interface, allowing the customer to download any number of small or large installation files without having to write any code.

How Does it Work?

1. The vendor's customer clicks on a link that directs them to an OAuth account login page integrated to Tectia Zero Trust, where they input their credentials.
2. After being successfully authenticated, the customer gets mapped to roles according to their commercial contract, based on the vendor's CRM system.
3. Depending on the link initially used, the customer is either automatically directed to a product-specific download or a landing page. Using the SSH protocol under the hood, a connection is made to a backend Tectia utilizing built-in X.509v3 Public Key Infrastructure and ephemeral certificates.
4. Once authenticated and authorized, the customer gains access to a folder housing their product version, with access to a subfolder for downloading previous or recent versions.
5. The Tectia Zero Trust frontend is configured to support customer product downloads, with the concurrently running Tectia backend enabled for secure file interaction that, for this use case, is restricted to facilitate downloads only. Auditing can be conducted easily in realtime from Tectia Zero Trust.
6. From the vendor's perspective, components can be configured or integrated, when needed, to customize the solution's scalability and its compatibility with neighboring software programs – for example, another Tectia Zero Trust setup for administrative and CI/CD pipeline access or integration to a SIEM system.
7. From the customer's perspective, the authentication and authorization process is automated, simple, quick, and invisible – offering maximum security with minimal effort. Tectia Zero Trust is very user-friendly, which reduces the likelihood of human error – for example, the download link is persistent and human-readable. It can be bookmarked or shared publicly because authentication and authorization are verified separately when the link is accessed.

Since its implementation, Tectia Zero Trust has provided the vendor with enhanced security, easier integration, flexible scalability, reliable automation, and less room for human error. By reducing manual processes and harnessing a built-in security framework, the vendor has experienced increased operational efficiency while enabling a user-friendly interface customized according to the product tier the customer has purchased.

Results

Let's get to know each other

Want to learn more about how we help organizations protect themselves using temporary access credentials, passwordless authentication, and centralized privileged management? We'd love to hear from you.

[Request a Demo](#)

