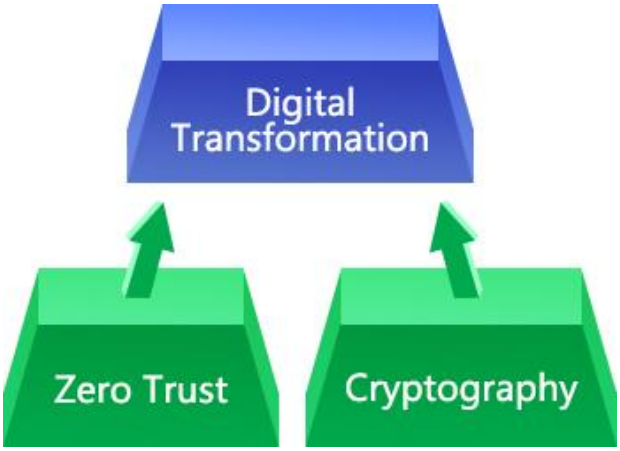
Digital Transformation, Cryptography, Zero Trust

The three words in the title of this article are the most popular words at present, and the author will talk about the relationship between them today. Zero trust is indeed one of the secrets to ensure the success of digital transformation. However, cryptography - refers to the technology, products and services that use a specific transformation method to encrypt, protect, and authenticate information. Digital transformation requires the dual guarantees of cryptography and zero trust to ensure the success of the transformation and ensure the normal operation after the transformation. Digital transformation without security protection will collapse at any time.



We all know that the world is promoting digital transformation at both the national level and the enterprise level, digital transformation has changed the way business is done, and even created a whole new type of business, using digital technologies such as cloud computing and big data to achieve the overall goal of improving efficiency and value, and creating value for customers. In this transformation, not only data is transferred to the cloud, but business is transferred to the cloud. Employees and devices are no longer limited to offices and office LANs, and the way to communicate with users is no longer phone calls and face-to-face visits, but to make full use of social media, email, and video conference etc. to achieve digital communication, provide customers with a better experience and create new value.

The traditional security protection solutions based on moats and fortresses are no longer useful in digital transformation because cloud services are not yours, your data is not on your own servers, and

your employees are not necessarily working in your office, if the network security measures do not keep up with these changes, it is possible to instantly return to the paper office era from the era of digital transformation at any time, or even back to the ancient era and unable to work normally because there are no paper documents. How to do?

The answer given by ZoTrus Technology is zero trust plus cryptographic technology. Digital transformation requires the double protection of zero trust and cryptographic technology. ZoTrus Technology provides five cloud services to ensure digital transformation security based on cryptographic technology and zero trust principles. The first cloud service is the Website Security Cloud Service. Because Web applications are the foundation of digital transformation, we must first consolidate the foundation and build a secure base. ZoTrus Website Security Cloud Service is a comprehensive web application security solution that integrates https encryption, cloud WAF protection and website trusted identity validation, it can effectively ensure the encrypted transmission security of confidential information of Web applications, anti-attack security and anti-identity counterfeiting security. Customers do not need to apply for an SSL certificate from a CA, but only need to perform CNAME domain name resolution twice and enable website https encryption and cloud WAF protection within 10 minutes, effectively ensuring the security of web systems.

Email is the second-largest traffic on the Internet and one of the key communication tools for digital transformation, but since email services have all moved to the cloud, email is no longer in your own mail server. To protect the security of emails containing a large amount of personal confidential information and business secrets, the principle of zero trust must be adopted. Zero trust to the emails that stored in cleartext in the cloud. Every email must be encrypted to ensure that each email is stored in ciphertext in the cloud. The second cloud service is Email Security Cloud Service, which is a full-lifecycle email security solution that realizes end-to-end encryption, it is an email security solution that integrates email encryption, digital signature, and digital postmark (timestamp), which can effectively eliminate email security issues such as email fraud, email leaks, and email identity spoofing, thereby ensuring the security of digital business communications.

Now, many business documents have also been managed on the cloud. How to ensure the security of the documents must also adopt the principle of zero trust. Zero trust to the documents that stored in cleartext in the cloud. Every document must be encrypted to ensure that every document is stored in

ciphertext in the cloud. The third cloud service is the Document Security Cloud Service. This is a solution that uses digital signature and encryption to ensure document security, it is also a cloud signature solution based on the principle of zero trust that only submit the HASH of the document to be signed to the cloud signing service system, never upload the original documents to the cloud which can effectively protect the security of document confidential information. Document encryption uses digital certificates to encrypt on the user's computer, which can effectively ensure that confidential documents will not be leaked, so that only authorized readers can seamlessly decrypt the encrypted documents. The digital signature, encryption and time stamp of electronic documents can effectively ensure the security and trusted of electronic documents.

The fourth cloud service is the Application Security Cloud Service, which is an innovative cloud service that uses digital signature and encryption to ensure the security of application software. It realizes the always verification for the digital signature of application software to ensure that the source of application software is trust, thereby ensuring the security of software operation. At the same time, for IoT devices that need to download updated software, a trusted https encrypted channel must be used to download the update package, and the digital signature and timestamp signature of the update package must be verified. Only software updates with trusted digital signature and timestamp signature are installed. It can effectively ensure the security of OTA upgrade of IoT devices and prevent attacks and extortion events in software upgrades.

The fifth cloud service is the Identity Trusted Cloud service, which is an identity validation and authentication service based on the principle of zero trust. Each individual has a trusted digital identity certificate, and any individual access to any resource must pass the digital signature verification. The identity of the website is proved by SSL certificate and its trusted identity is validated by the browser or APP. The Website Trusted Identity Validation Service launched today is one of the main products of the Identity Trusted Cloud Service, which realizes the trusted identity of the websites which are the largest traffic on the Internet.

The last thing worth mentioning is the ZT Browser. As the first product of ZoTrus Technology, it is not only a browser, not only a free SM2 SSL certificate supported browser, but also not only can significantly display the website's trusted identity, WAF protection and SM2 https encryption, more

importantly, it is a client software for "cloud-only" zero trust. Users need a client software that can locally store and manage confidential information, including encryption keys and other important data, and cannot store all data in the cloud, which must be "client plus cloud", so as to give full play to the computing power advantages of the "cloud" to achieve fully automatic encryption and digital signatures, and to allow the "client" to manage all important data in the hand, completely solving the problem of data security and privacy protection challenges that cannot be achieved by cloud-only, the integration of “client” and “cloud” jointly protect the security of digital transformation.

In short, digital transformation is must, but digital transformation without security is the root cause of disaster, and it has the risk of returning to ancient times at any time. Therefore, we must attach great importance to the construction of security measures for digital transformations. The most effective security protection is zero trust in individual identities, zero trust in website identities, zero trust in web traffic, zero trust in web connections, zero trust for cleartext emails, zero trust for unidentified documents and zero trust for unidentified application software, these zero trust security solutions must be implemented by cryptographic technology, and digital certificate can be used to realize digital signature, encryption, and timestamping services. Only in this way can the security of business systems be effectively protected, thus ensuring a successful digital transformation, and continued reliable operation.

Richard Wang

June 1, 2022
In Shenzhen, China