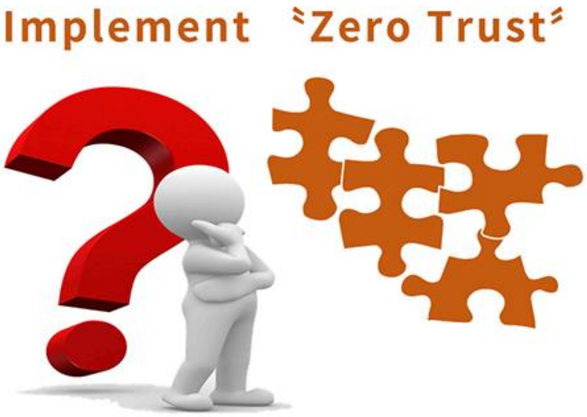
Zero Trust Implement, Where to Start?

According to Gartner analysts John Watts and Neil MacDonald, "Zero Trust" is an overused and widely misunderstood term by many organizations. Most organizations interested in Zero Trust are in the planning or strategic stage. Organizations looking to move to actual implementation should focus on two main projects: user-to-application segmentation (based on zero trust architecture) and workload-to-workload segmentation (identity-based segmentation).

The author also felt the same when talking about zero trust with many friends. Everyone thinks that zero trust is very important, but they really don’t know how to start. After all, this is a painful process to abandon the traditional security “castle and moat” solution. At the same time, the implementation of the "China Cryptography Law" has also made many government agencies do not know how to compliant with. How to overcome the problem of funding shortages and make progress in compliance with the Law. These two things that some readers may think are unrelated, can be combined and planned together, they are one thing! Because the protection requirements of the "Cryptography Law" for critical information infrastructure are the principle of zero trust, cryptography must be used to achieve information encryption and security authentication.



So, how to get started? How can one thing be done to satisfy both security application requirements? The author shares three insights here.

(1) Establish the concept of zero trust. Zero trust is a journey, not an overnight thing.

The first thing to note is that zero trust is a security concept, not a specific technology or a solution. We must first establish the concept of zero trust, fully aware that this is a trend and must be implemented. However, Zero Trust is a journey, not a wholesale replacement of infrastructure or business processes. Organizations should seek to gradually implement Zero Trust principles, process changes, and technology solutions to protect their highest-value data assets. Most government agencies and enterprises will continue to operate in a hybrid zero-trust and perimeter-based model indefinitely, while continuing to invest in ongoing IT modernization programs.

(2) Implement zero trust security, starting with base security.

To implement zero trust security, the network infrastructure can be left alone and start with base security. What is base security? The first is the https encryption of the Web application, which is the base security foundation. Whether it is an internal network or an external network system, https encryption must be implemented, because the HTTP cleartext transmission cannot guarantee the security of confidential information, and the intranet cleartext traffic is also insecure. According to statistics, 70% of security incidents start from the intranet. That is to say: all http traffic, whether it is browser access, mobile app access or system software API access, must be transformed into https encrypted traffic, and the server side must deploy an SSL certificate. The cost of this transformation is as low as a few hundred yuan/year/website, which not only meets the requirements of zero trust security transformation, but also meets the requirements of compliance transformation of the "Cryptography Law".

The second base security is email encryption. Cleartext emails are untrustworthy, and there is no way to guarantee that the identity of the email sender is trusted, that the content of the email will not be illegally tampered with and leaked. The second network traffic security of zero trust is to encrypt email traffic. Email certificates are used to achieve end-to-end encryption to ensure that emails are encrypted from the client, transmitted, and stored in the cloud, ensuring the security of emails throughout their life cycle. The cost of this transformation is also very low, only tens of yuan per email per year! It can not only meet the requirements of zero trust security transformation, but also meet the requirements of compliance transformation of the "Cryptography Law".

The third base security is code signing, not only the code signing of computer software, but also the digital signature of all remote upgrade codes. The OTA air upgrade system of equipment systems must be transformed to trust the code only with specific CA issued code signing certificate signature. Only in this way can the malicious attacks of equipment systems be effectively prevented.

The fourth base security is document signing. Never trust all electronic documents without digital signatures. All documents issued by government agency should have a trusted digital signature. Only in this way, the people will not be deceived, and all kinds of efforts to prevent telecommunications fraud can really achieve a multiplier effect.

The first of the above four base security transformation is the most important, and this is the top priority, because all kinds of government services and business activities have been moved to the Internet. If https encryption is not completely implemented, then individual privacy and business secrets cannot be guaranteed not to be illegally stolen and illegally tampered with. These security issues are not enough to rely on the law, and corresponding technical precautions must be taken to protect them.

(3) Realize strong identity authentication transformation, data encryption transformation, and network segmentation transformation based on identity certificate.

After completing the base security transformation, it can ensure that network traffic is encrypted, and applications and documents are secure and trusted. Next, we should start the transformation of the identity authentication system, completely close the authentication method of insecure username and password, and use identity certificate to realize strong identity authentication. An identity certificate is issued to each user, and the user must present the corresponding level of identity certificate and pass the authentication to access any resource. All devices must also have an identity certificate. This identity certificate can be an SSL certificate, because SSL certificates also have identity authentication attributes and can prove the server identity.

After completing the transformation of the identity authentication system, it is necessary to start the transformation of encrypting important data with an encrypting certificate. The confidential data is encrypted with a certificate and stored in the database. When the user obtains this data after passing the identity authentication, it is decrypted and encrypted with the user's public key and returned to the user, user can use his private key to decrypt it to get the original data. At the same time, when generating data, the timestamping service must be called to obtain timestamp signature data and store it together with the data, to prove that the generation time of the data is trusted, and the data time has not been tampered with.

Of course, network refinement and segmentation can also be performed simultaneously, the different applications are located on different network segments, so that authenticated users can obtain data more efficiently and quickly. However, the premise of network segmentation is to complete the base security transformation to meet the base security requirements of zero trust.

In a word, zero trust is a journey without end. We need to start from base security, and we need to use cryptographic technology to achieve zero trust base security. We need to move forward in this direction step by step. Only in this way can we finally reach the highest level of zero trust security.

Richard Wang

Dec. 22, 2021
In Shenzhen, China