Huawei Cloud White Paper for Zero Trust Capability Maturity

Issue 1.0

Date 2021-10-17

Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions

 and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://www.huawei.com/

Email: support@huawei.com

Introduction

The development of technologies, such as big data, cloud computing, and Internet of Things (IoT), is blurring enterprise network boundaries. Furthermore, a succession of external cyber attacks and internal threats (such as unauthorized access, misoperations, and data leakages) are emerging. Traditional boundary-based security protection methods are losing effectiveness. The zero trust model that adheres to the principle of "never trust, always verify" proves to be an effective solution and is gaining momentum in cyber security.

With an evolving zero trust capability, Huawei Cloud identifies that zero trust implementation is a systematic project and cannot be achieved by simply deploying a single network architecture or technical product. Instead, it requires long-term planning and construction, including specifying the strategic vision of zero trust, getting ready the required resources, and developing the roadmap. Therefore, we have built a zero trust capability maturity model based on the industry's zero trust architecture and our implementation experience to help enterprises identify their current maturity level of zero trust and provide guidance for their strategic planning of zero trust capability development.

This model translates the maturity assessment theory into a specific framework, which provides practical assessment guidance. The zero trust model framework is classified into 5 capability pillars, which are further divided into 20 core sub-domains. The framework measures zero trust capabilities from multiple dimensions (such as organization building and technologies & tools), and specifies quantifiable metrics to ensure comprehensive and accurate assessment.

Huawei Cloud continuously optimizes the maturity model based on practices and incubates internal zero trust applications into customer-oriented products and services. To date, Huawei Cloud has provided multiple zero trust products and solutions in multiple fields, such as identity security, network security, application security, and data security.

This white paper shares the zero trust capability maturity model implemented in Huawei Cloud with customers and the industry to explore how to assess zero trust capability maturity, and promote the industry's zero trust capability development. Huawei Cloud will continue to release zero trust products and services to improve its security protection capabilities and safeguard customers' business compliance and security.

Contents

1 Current State and Trends

Enterprise IT facilities are diversifying and service system access requirements are becoming increasingly complex as technologies like cloud computing and big data are extensively applied and services like remote office and mobile Internet are gaining popularity. Internal staff, supplier personnel, external partners, and others can access systems in multiple ways, and the interconnected systems are accessible to more devices, blurring the original network boundaries.

Furthermore, network security risks and threats are gaining complexity, and a succession of cyber attacks (such as APT attacks, ransomware, and unauthorized internal operations) are emerging, making it difficult for enterprises to defend against them and causing huge service losses. However, traditional boundary-based security protection methods have gradually become ineffective.

The zero trust model is one of the effective ways to solve the preceding problems. The term zero trust was first proposed by John Kindervag, chief analyst of Forrester, in 2010. After years of development and evolution, zero trust has become a new trend of cyber security development. The core idea is to stick to the principle of "never trust, always verify" and assume that there is no traditional network boundaries. All users, devices, and systems, whether in or outside the organization's network, need to be continuously authenticated and dynamically authorized before being granted the least privilege and fine-grained access to enterprise resources.

2 Key Points of Huawei Cloud Zero Trust Implementation

Huawei Cloud also faces security challenges similar to those in the industry. Therefore, it is urgent to implement zero trust to enhance security protection capabilities and safeguard its own services and customer services. However, zero trust cannot be implemented overnight but requires long-term planning and development efforts, including specifying the strategic vision for zero trust, required resources, and roadmap. A key planning task is to assess the maturity of zero trust capabilities so as to determine the current capability maturity level and development goals. To this end, a practical zero trust capability maturity model needs to be referenced.

The zero trust capability maturity model is an approach to assess an organization's zero trust capabilities, including a host of characteristics, attributes, indicators, or patterns that represent the capabilities. The maturity model usually uses a structured framework to define several evolving maturity phases from the initial level to the optimal level, and describes each phase based on maturity characteristics. The model can provide a reference benchmark for organizations to assess the current maturity level of their zero trust capabilities and set improvement targets.

3 Zero Trust Capability Maturity Model of Huawei Cloud

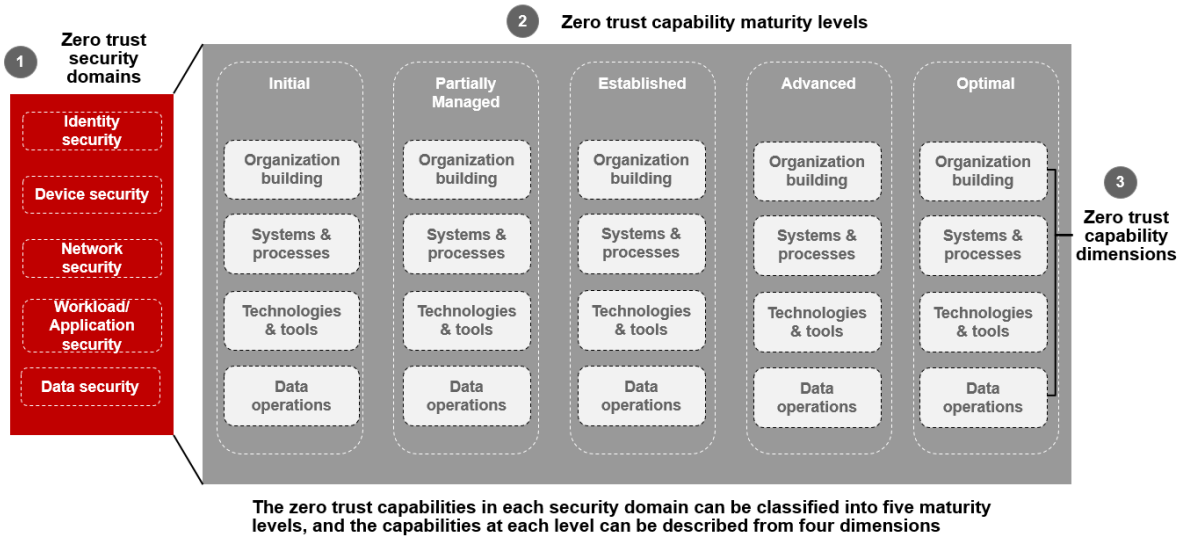
With references to the zero trust concept in the industry, Huawei Cloud has developed a zero trust capability maturity model based on its own understanding and practices in cyber security and privacy protection. This model aims to translate zero trust from the theoretical level to a specific framework to provide practical guidance for maturity assessment. Its features are represented in the following aspects:

- Assessment domains: Based on the industry's existing assessment domains, the zero trust capability maturity model further refines the key security domains of the five capability pillars, so as to perform more granular capability assessment.
- Capability dimensions: In addition to technical capabilities, the model also assesses management capabilities, such as organization building, systems & processes, and data operations, to measure the zero trust capabilities more comprehensively.

- Metrics: The model defines specific metrics for all key security domains, quantitatively assesses domain-specific and overall zero trust capability maturity levels, and helps develop future goals.

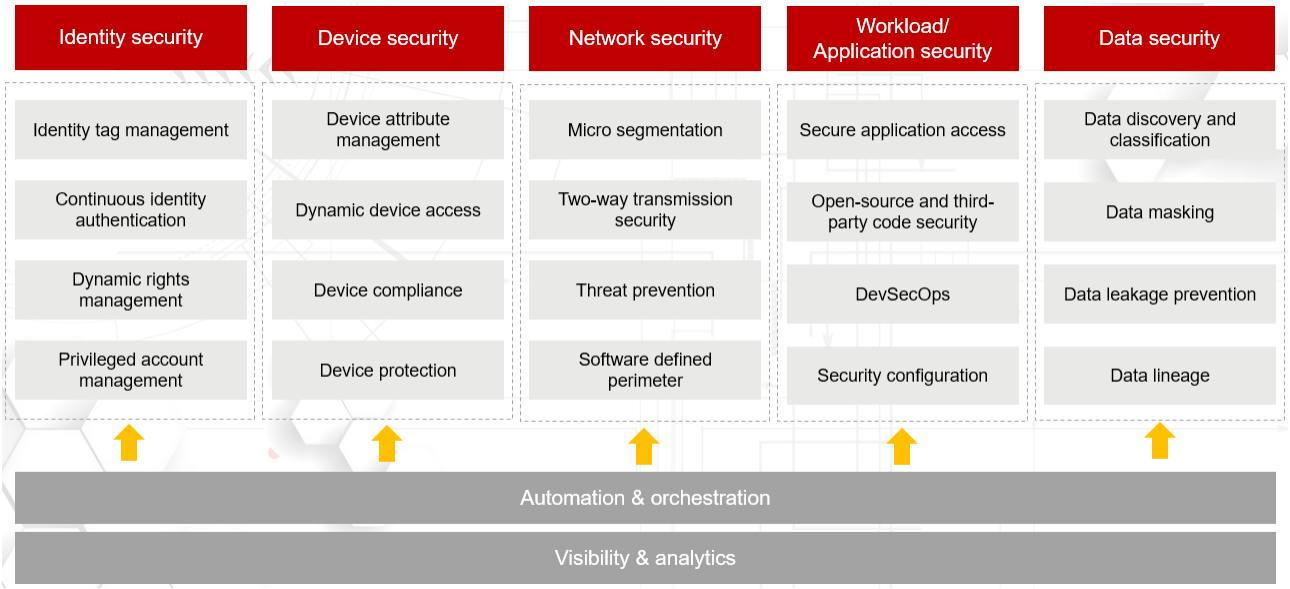
3.1 Maturity Model Architecture

The architecture of the zero trust maturity model can be divided into three parts: zero trust security domains, capability maturity levels, and capability dimensions. The following figure shows their relationships.



3.2 Zero Trust Security Domains

Based on the Forrester's Zero Trust eXtended (ZTX) framework and the US Department of Defense's Zero Trust Reference Architecture, the zero trust capability maturity model of Huawei Cloud is classified into five zero trust security domains: identity security, device security, network security, workload/application security, and data security. Automation, orchestration, visibility, and analytics will be the underpinning capabilities in the five domains. The 5 security domains are further classified into 20 key security sub-domains.



3.3 Zero Trust Capability Maturity

	Initial	Partially managed	Established	Advanced	Optimal
Organization building	Management roles and responsibilities not specified	Preliminarily managed by relevant personnel	Management positions and personnel specified, and responsibilities clearly defined	Positions/Staffing and responsibilities optimized	Same as the Advanced level
Systems & processes	No documented systems or processes in place	High-level policies and management requirements developed	Comprehensive and detailed management specifications and processes developed	Continuous optimization of systems & processes	Same as the Advanced level
Technologies & tools	Traditional security protection adopted without zero trust	Some zero trust capabilities available only in some domains	Relatively robust zero trust capabilities, but no automated policy adjustment	Dynamic policy adjustment through machine learning	Continuous optimization for adaptive policy adjustment
Data operations	No data statistics collection	Manual data statistics collection	General data operations metrics developed	Specific data operations metrics developed	Continuous optimization of data operations metrics

In addition, Huawei Cloud has designed an approach of measuring zero trust capability maturity to quantitatively measure the current zero trust maturity level and clearly indicate the future development path. This measurement approach can achieve:

- Quantitative scoring of zero trust capability maturity levels. The zero trust capability maturity level of each key security sub-domain can be quantitatively scored to identify the required maturity level of an enterprise.
- Visibility of zero trust capability maturity. The maturity scores of 20 zero trust sub-domains are globally displayed using radar charts and other means, thereby helping enterprises identify the weaknesses and strengths of current zero trust capabilities and plan the key domains for improvement.

3.4 Zero Trust Capability Dimensions

Zero trust capability dimensions indicate the capabilities required by each security domain, and can be classified into:

- Organization building: zero trust-related position setting, responsibility division, and personnel capability development of organizations;
- Systems & processes: establishment and implementation of zero trust management requirements, systems, and processes;
- Technologies & tools: technical means and products/tools required for implementing management requirements, systems, and processes;
- Data operations: establishment and optimization of data metrics to measure the effectiveness of zero trust management and technical capabilities.

4 Identity Security

One of the objectives to implement zero trust is to enable users (including employees, suppliers, and partners who may need to access organization resources) anywhere to gain the right access to the required organization resources. The core capabilities involved in identity security include: (1) identity tag management; (2) continuous identity authentication; (3) dynamic permission management; (4) privileged account management.

4.1 Identity Tag Management

In the zero trust architecture, identity tag management refers to the capabilities of user account and tag management throughout the lifecycle to ensure that the identity information of authenticated users is reliable and continuously updated. The capabilities at each level are as follows:

Initial: Organization building — Roles and responsibilities for user identity management are not defined. Systems & processes — Security management requirements related to user identity tags are not specified. Technologies & tools — The user identity lifecycle is not systematically managed, and users are identified only through accounts.

Partially managed: Organization building — User identities are preliminarily managed by relevant personnel. Systems & processes — Policies for account access permission management and requirements for identity authentication management have been developed. Technologies & tools — User identity tags (including accounts and some static tags) are managed in a unified manner.

Established: Organization building — Positions and personnel for user identity tag management have been specified, and management responsibilities have been clearly defined to plan and implement identity tag lifecycle management and user label policies. Systems & processes —

Comprehensive and detailed user identity tag management specifications and processes have been specified, including naming standards for different types of tags. Technologies & tools — A platform is used to automatically manage user identities, including static and dynamic user tags, and most tag policies are manually configured. Data operations — Data metrics for user account and tag management are preliminarily formulated to roughly measure the overall effectiveness of user identity management in organizations.

Advanced: Organization building and systems & processes — Same as the Established level. Technologies & tools — Machine learning is used to analyze user behavior, all identity tags are dynamically managed, and real-time visualization of tag status is implemented. Data operations — Specific data metrics are formulated to monitor the capability of automated user tag management, for example, the accuracy of user behavior tags.

Optimal: Organization building and systems & processes — Same as the Established level. Technologies & tools — AI is used to identify user behavior and trends and perform adaptive management of user identity tags. Data operations — Comprehensive and specific data metrics are formulated for user tag management to continuously optimize the metrics.

4.2 Continuous Identity Authentication

In the zero trust architecture, continuous identity authentication refers to the capabilities of continuously verifying users to ensure that they have valid identities before and during the use of required resources. The capabilities at each level are as follows:

Initial: Organization building — Roles and responsibilities for identity authentication management are not specified. Systems & processes — Security management requirements for identity authentication are not specified. Technologies & tools — User identities are authenticated simply using static passwords, and identity authentication of most systems is independent.

Partially managed: Organization building — User identities are preliminarily managed by relevant personnel. Systems & processes — Policies for account access permission management and requirements for identity authentication management have been developed. Technologies & tools — Unified identity authentication based on static passwords is basically implemented, single sign-on (SSO) is implemented in some systems, and two-factor authentication is used in vital systems.

Established: Organization building — Management positions and personnel for user identity authentication have been specified, and management responsibilities have been clearly defined to plan and implement identity authentication policies and rules. Systems & processes — Comprehensive and detailed identity authentication management specifications and processes have been developed, including the authentication policy change process. Technologies & tools — Unified identity authentication and SSO are fully implemented, multi-factor secondary authentication is performed based on environment situations, and some systems support federated authentication. Data operations — Identity authentication management metrics are preliminarily formulated to roughly measure the overall effectiveness of identity authentication management in organizations.

Advanced: Organization building — Positions/staffing and responsibilities for user identity and permission management are improved, and a professional operations team is established to plan and implement identity authentication policies and rules. Systems & processes — Identity authentication management specifications and processes are continuously optimized, including the risk calculation rule change process. Technologies & tools — No password policy is widely implemented, and identity authentication policies are dynamically adjusted based on comprehensive risk assessment in real time. Data operations — Specific data metrics (such as the accuracy of user risk attribute assessment and the accuracy of automated policy adjustment) are formulated for identity authentication management and automated adjustment verification.

Optimal: Organization building and systems & processes — Same as the Advanced level. Technologies & tools — AI is used for adaptive adjustment of user identity authentication policies. Data operations — Comprehensive and specific data metrics are formulated and continuously optimized for identity authentication management.

4.3 Dynamic Permission Management

In the zero trust architecture, dynamic permission management refers to the capabilities of assessing user identity risks in real time and allocating resources in line with the least privilege principle accordingly. The capabilities at each level are as follows:

Initial: Organization building — Roles and responsibilities for access permission management are not specified. Systems & processes — Security management requirements related to user permissions are not developed. Technologies & tools — Users are manually authorized based on requirements or experience.

Partially managed: Organization building — access permissions are preliminarily managed by relevant personnel. Systems & processes — Policies and requirements for account access permission management have been specified. Technologies & tools — A permission management platform is used to authorize users in vital systems according to the static role-based policy, which is updated on a regular basis.

Established: Organization building — Positions and personnel for access permission management have been specified, and management responsibilities have been clearly defined to plan and implement permission management rules and user authorization standards. Systems & processes — Comprehensive and detailed specifications and processes for account permission management have been specified, including the regular position permission review process. Technologies & tools — For vital systems, user access permissions are automatically adjusted based on role-specific authorization policies and major environment assessments. Data operations — Related metrics (such as the deployment rate of dynamic permission management and the success rate of automated authorization) are preliminarily formulated to measure the effectiveness of dynamic user permission management.

Advanced: Organization building — Positions/personnel and responsibilities related to user identity and permission management are improved, and a professional operations team is established to plan and implement dynamic permission management policies and rules. Systems & processes — Access permission management specifications and processes are continuously optimized, including the user risk calculation rule change process. Technologies & tools — Real-time status analysis is performed in terms of user behaviors, devices, networks, and accessed resource, comprehensive risks are calculated to dynamically adjust user access permissions. Data operations — Specific data metrics (such as the accuracy of user risk attribute assessment, accuracy of permission adjustment, and exception authorization rate) are formulated to monitor access permission management, automated detection, and authorization capabilities.

Optimal: Organization building and systems & processes — Same as the Advanced level. Technologies & tools — AI is used to analyze user behavior patterns for adaptive adjustment of access permissions. Data operations — Comprehensive and specific data metrics are formulated and continuously optimized for access permission management.

4.4 Privileged Account Management

In the zero trust architecture, privileged account management refers to the capabilities of preventing risks caused by credential leakage or privilege abuse to ensure the security of privileged identities and activities. The capabilities at each level are as follows:

Initial: Organization building — Roles and responsibilities for privileged account management are not specified. Systems & processes — Security management requirements for privileged

accounts are not specified. Technologies & tools — Privileged accounts are recorded manually and managed separately, and static passwords are used for authentication.

Partially managed: Organization building — Privileged accounts are preliminarily managed by relevant personnel. Systems & processes — Policies and requirements for privileged account management have been developed. Technologies & tools — A technical platform is deployed to manage privileged accounts of vital systems, periodically change keys, and record/detect/block account-related behaviors.

Established: Organization building — Positions and personnel for privileged account management have been specified, and management responsibilities have been clearly defined to plan and implement privileged account management principles and account activity control. Systems & processes — Comprehensive and detailed specifications and processes for privileged account management have been developed, including the regular activity log audit process. Technologies & tools — All privileged accounts are managed according to the least privilege principle for automated discovery of and manual response to privileged accounts, session isolation, and automated key rotation. Data operations — Related metrics (such as the privileged account management rate and key rotation coverage rate) are preliminarily formulated to measure the overall effectiveness of privileged account management.

Advanced: Organization building and systems & processes — Same as the Established level. Technologies & tools — Automated discovery of and response to privileged accounts, and dynamic permission adjustment according to the Just-In-Time (JIT) principle. Data operations — Specific data metrics (such as the automated identification rate, application scenario matching rate, and permission adjustment accuracy rate) are available for privileged account management and automated permission adjustment.

Optimal: Organization building and systems & processes — Same as the Established level. Technologies & tools — AI is used to adaptively adjust the access permissions of privileged accounts. Data operations — Comprehensive and specific data metrics are formulated and continuously optimized for privileged account management.

5 Device Security

Devices are an important part of the zero trust architecture. As devices having access to an organization's network are growing in number and type, the organization should continuously identify, verify, authorize, isolate, protect, fix, and control all devices and assume them to be untrusted by default. The core capabilities involved in device security include: (1) device attribute management; (2) dynamic device access; (3) device compliance; (4) device protection.

5.1 Device Attribute Management

In the zero trust architecture, device attribute management refers to the capabilities of continuously and automatically identifying, recording, and tracing different types of device assets and corresponding attributes in an organization so that dynamic device access control can be performed. The capabilities at each level are as follows:

Initial: Organization building — Roles and responsibilities for device management are not specified. Systems & processes — Device security management requirements are not developed. Technologies & tools — Device asset lists are manually maintained, and device attributes are not managed.

Partially managed: Organization building — Device assets and attributes are preliminarily managed by relevant personnel. Systems & processes — Policies and requirements for device asset and attribute management have been developed. Technologies & tools — An asset management system is used to maintain asset/attribute lists and automatically identify some assets and attributes.

Established: Organization building — Positions and personnel for device asset and attribute management have been specified, and management responsibilities have been clearly defined to plan and implement device asset/attribute inventory, review, update, and maintenance. Systems & processes — Comprehensive and detailed specifications and processes for device asset and attribute management have been developed, including requirements for defining device asset and attribute types and establishing, updating, and maintaining device asset lists. Technologies & tools — All device asset and attribute lists in organizations are automatically identified and managed in real time as well as in a visible manner, and identification policies are manually configured. Data operations — A few coarse metrics (such as the device management rate by category/quantity and attribute identification rate) are formulated to measure the effectiveness of device asset and attribute management in organizations.

Advanced: Organization building and systems & processes — Same as the Established level. Technologies & tools — Machine learning is used to analyze device features, dynamically manage device assets and attribute identification policies, and automatically manage asset and attribute lists. Data operations — Specific data metrics (such as the asset and attribute scanning frequency, scanning period, and identification accuracy) are formulated to measure the device asset and attribute discovery capability.

Optimal: Organization building and systems & processes — Same as the Established level. Technologies & tools — Device asset and attribute identification policies are continuously optimized, and the identification and management capabilities are continuously improved. Data operations — Specific data metrics are formulated and continuously optimized for device attribute management.

5.2 Dynamic Device Access

In the zero trust architecture, dynamic device access refers to the capabilities of continuously evaluating device attributes and contexts based on the Attribute Based Access Control (ABAC) model to dynamically authenticate and authorize devices. The capabilities at each level are as follows:

Initial: Organization building — Roles and responsibilities for device access control management are not specified. Systems & processes — Security management requirements for device access control are not specified. Technologies & tools — Access control is not implemented for devices.

Partially managed: Organization building — Device access control is preliminarily managed by relevant personnel. Systems & processes — Security management requirements for device access control have been developed. Technologies & tools — PCs, mobile devices, and other devices are authenticated using unique device IDs or certificates, and access control policies are manually updated and maintained if necessary.

Established: Organization building — Management positions and personnel for device access control have been specified, and management responsibilities have been clearly defined to plan and implement design, deployment, audit, and maintenance of dynamic access control policies. Systems & processes — Comprehensive and detailed specifications and processes for device access control have been developed, including the requirements for access control models, trust assessment algorithms, policy maintenance, and covered device types. Technologies & tools — Access control policies based on the ABAC model are developed to continuously assess the trust levels of all devices in organizations based on device attributes and contexts, and dynamically adjust access permissions. Data operations — A few coarse metrics (such as the rejection rate of unauthorized devices) are formulated to measure the effectiveness of device access control in organizations.

Advanced: Organization building — Positions/staffing/responsibilities for device access control have been optimized. Systems & processes — Management specifications and processes for device access control have been developed, including trust assessment algorithm requirements

and authorization policies. Technologies & tools — Machine learning algorithms are used to analyze device subject activities, automatically generate access control policies, and authenticate and authorize all devices that access organization resources. Data operations — Specific data metrics are formulated to measure the effectiveness of device access control policies (such metrics include the false acceptance rate (FAR), false rejection rate (FRR), and FAR/FRR change trend).

Optimal: Organization building and systems & processes — Same as the Advanced level. Technologies & tools — Trust algorithms in access control policies are generated in real time and continuously optimized, and authentication & authorization policies are adaptively adjusted. Data operations — Specific data metrics are formulated and continuously optimized for device access control.

5.3 Device Compliance

In the zero trust architecture, device compliance refers to the capabilities of automatically and continuously verifying the compliance of configuration policies on different types of devices and fixing devices that do not meet the configuration baseline. The capabilities at each level are as follows:

Initial: Organization building — Device compliance management roles and responsibilities are not specified. Systems & processes — Security management requirements for device compliance are not specified. Technologies & tools — Configuration policy check and fixing are manually performed for a single device type (such as PCs) as required.

Partially managed: Organization building — Device compliance is preliminarily managed by relevant personnel. Systems and processes — Policies and requirements for device compliance management have been developed. Technologies & tools — Tools are used to periodically check configuration policies for devices (such as PCs and laptops), and manual fixing is performed.

Established: Organization building — Positions and personnel for device compliance management have been specified, and management responsibilities have been clearly defined to plan and implement device configuration check, response, and fixing. Systems & processes — Comprehensive and detailed security management specifications and processes for device compliance have been developed, including requirements for the device check scope, policy application scope, check method, and check frequency. Technologies & tools — A unified platform is used to automatically check the configuration of all device types in organizations in real time, generate visualization reports, and automatically rectify some non-compliant items. Data operations — A few coarse metrics (such as the proportions of devices that follow or fail to follow policies) are formulated to measure the effectiveness of device compliance management in organizations.

Advanced: Organization building and systems & processes — Same as the Established level. Technologies & tools — Machine learning is used to analyze device configurations, and automatically generate policies for configuration check and fixing on all devices that access organization resources. Data operations — Specific data metrics (such as the number and proportion of devices with high-risk vulnerabilities and the configuration check accuracy rate) are officially formulated to measure the effectiveness of device compliance.

Optimal: Organization building and systems & processes — Same as the Established level. Technologies & tools — Machine learning algorithms are continuously optimized to improve the accuracy and timeliness of configuration check and fixing policies. Data operations — Specific data metrics are formulated and continuously optimized for device compliance management.

5.4 Device Protection

In the zero trust architecture, device protection refers to the capabilities of automatically and continuously implementing threat prevention, detection, and response mechanisms for different types of devices. The capabilities at each level are as follows:

Initial: Organization building — Roles and responsibilities for device protection are not specified. Systems & processes — Security management requirements for device protection are not specified. Technologies & tools — Anti-virus software and other measures are used to protect PCs and laptops, but no threat detection tool is deployed.

Partially managed: Organization building — Device protection is preliminarily managed by relevant personnel. Systems & processes — Management policies and requirements for device protection have been developed. Technologies & tools — Security hardening measures (such as certificate-based authentication and full-disk encryption) are adopted for PCs and laptops, and device threat detection tools are deployed but threat response and handling are manual.

Established: Organization building — Positions and personnel for device protection management have been specified, and management responsibilities have been clearly defined to plan and implement device hardening, threat detection, response, fixing, and others. Systems & processes — Comprehensive and detailed specifications and processes for device protection management have been developed, including requirements for the device protection scope, security hardening standard, and threat detection and response processes. Technologies & tools — A unified platform is deployed for registered devices in organizations to collect and analyze device threat information in real time and generate visualization reports, and the device threat and response tool is used to automatically complete some threat response and handling actions. Data operations — A few coarse metrics (such as the total number of device threat event alarms and the proportion of events at different levels) are formulated to measure the effectiveness of device protection in organizations.

Advanced: Organization building and systems & processes — Same as the Established level. Technologies & tools — Machine learning is used to analyze threat behaviors for all registered and unregistered devices, detect unknown threats, and perform automated response. Data operations — Specific data metrics (such as the unknown threat detection rate and event response and handling time) are formulated to measure the device protection capability.

Optimal: Organization building and systems & processes — Same as the Established level. Technologies & tools — An adaptive response process is initiated for all threat events to continuously optimize prediction, prevention, detection, and response capabilities for unknown threats. Data operations — Specific data metrics are formulated and continuously optimized for device protection management.

6 Network Security

Network security is one of the important parts of the zero trust architecture. As a data access and transmission channel, the network must provide necessary security protection and access control for data in transit. Network threat detection, response, fixing, and resource segmentation/isolation are the highlighted parts in zero trust network security. Core capabilities involved in network security include: (1) micro segmentation; (2) two-way transmission; (3) threat prevention; (4) dynamic network access.

6.1 Micro Segmentation

In the zero trust architecture, micro segmentation refers to the capabilities of isolating network and application resources by segment and classifying access object resources in a fine-grained manner. The capabilities at each level are as follows:

Initial: Organization building — Management roles and responsibilities for micro segmentation are not specified. Systems & processes — Management requirements for micro segmentation are not specified. Technologies & tools — Only internal and external network boundaries are distinguished, and internal networks are not segmented.

Partially managed: Organization building — Micro segmentation is preliminarily managed by relevant personnel. Systems & processes — Security management requirements for micro segmentation have been developed. Technologies & tools — Network topology diagrams are generated by collecting network node information, and micro segmentation is configured for key application services.

Established: Organization building — Positions and personnel for resource micro segmentation management have been specified, and management responsibilities have been clearly defined. Systems & processes — Comprehensive and detailed specifications and processes for resource micro segmentation have been developed, including requirements for micro segmentation policy management, O&M management, and security monitoring. Technologies & tools — Micro segmentation is implemented for all network resources; dependency diagrams are automatically generated based on application access relationships, and access control policies are adjusted based on static rules to implement micro segmentation for application/service resources. Data operations — Data metrics (such as the resource micro segmentation coverage) are preliminarily formulated to measure the effectiveness of key application/service protection.

Advanced: Organization building — Management positions/staffing/responsibilities for micro segmentation have been optimized, and a professional operations team is in place to establish and optimize the automation model of resource micro segmentation. Systems & processes — Management specifications and processes for resource micro segmentation are continuously optimized, including the automated change process of segmentation policies. Technologies & tools — Machine learning is used to analyze real-time context changes of networks and applications/services, automatically adjust micro segmentations for all of them, and visualize their real-time status. Data operations — Fine-grained data metrics are formulated for resource isolation protection.

Optimal: Organization building and systems & processes — Same as the Advanced level. Technologies & tools — AI is used to analyze real-time changes of the general environment and implement adaptive adjustment at the application level. Data operations — Comprehensive and specific data metrics are formulated and continuously optimized for network segment-based isolation management.

6.2 Two-Way Transmission Security

In the zero trust architecture, two-way transmission security refers to the capabilities of preserving the authenticity, integrity, and confidentiality of data in transit through two-way identity authentication and link encryption. The capabilities at each level are as follows:

Initial: Organization building — Management roles and responsibilities for network transmission security are not specified. Systems & processes — Management requirements for network transmission security are not developed. Technologies & tools — Transmission links are not encrypted.

Partially managed: Organization building — Network transmission security is preliminarily managed by relevant personnel. Systems & processes — Management requirements for network transmission encryption and authentication have been developed. Technologies & tools — A single encryption algorithm and one-way transmission protocol are used to protect network transmission links of external services.

Established: Organization building — Positions and personnel for network transmission security management have been specified, and management responsibilities have been clearly defined to

plan and implement two-way transmission security management. Systems & processes — Comprehensive and detailed specifications and processes for network transmission security management have been developed, including requirements for encryption algorithm selection. Technologies & tools — Hybrid encryption algorithms and two-way transmission protocols are used to protect network transmission links of both external services and internal key services. Data operations — Data metrics (such as the proportion of services supporting two-way transmission protocols and the transmission link encryption coverage) are preliminarily formulated.

Advanced: Organization building and systems & processes — Same as the Established level. Technologies & tools — Hybrid encryption algorithms and two-way transmission protocols are used to protect all network transmission links. Data operations — Specific data metrics are formulated to measure the overall effectiveness of transmission security management.

Optimal: Organization building and systems & processes — Same as the Established level. Technologies & tools — Encryption algorithms and transmission protocols are continuously optimized and updated to enhance network transmission protection. Data operations — Comprehensive and specific data metrics are formulated and continuously optimized for network transmission security management.

6.3 Threat Prevention

In the zero trust architecture, threat prevention refers to the capabilities of detecting and analyzing network activities to ensure quick network threat detection and response. The capabilities at each level are as follows:

Initial: Organization building — Roles and responsibilities for network threat prevention are not specified. Systems & processes — Management requirements for network threat prevention are not specified. Technologies & tools — No tool is deployed for network threat prevention.

Partially managed: Organization building — Network threat protection is preliminarily managed by relevant personnel. Systems & processes — Requirements for network threat protection management have been developed. Technologies & tools — Tools have been deployed, threat detection rules have been established, and tools can be used to detect and respond to known threats based on threat characteristics.

Established: Organization building — Management positions and personnel for network threat prevention have been specified, and responsibilities have been clearly defined to plan and implement threat detection, analysis, and response. Systems & processes — Comprehensive and detailed specifications and processes for network threat prevention management have been developed, including requirements for network threat detection and threat event response processes. Technologies & tools — A behavior analysis model has been established to automatically detect threats and isolate threat nodes by monitoring network activities in real time; however, unknown threats need to be further analyzed and addressed manually. Data operations — Data metrics (such as the threat false positive/negative rate) regarding threat detection and response capabilities have been preliminarily formulated.

Advanced: Organization building — Management positions/staffing/responsibilities for threat prevention have been optimized, and a professional security operations team is in place to establish and optimize automated threat analysis and fixing models. Systems and processes — Specifications and processes for threat prevention management have been continuously optimized, including threat detection and response processes. Technologies & tools — Machine learning is used to improve the network behavior analysis model, and isolation technologies (such as sandbox) and automated analysis/testing are used to implement automated detection, analysis, and fixing of unknown network threats. Data operations — Comprehensive and specific data metrics (such as the automated threat fixing rate) are officially formulated to measure threat detection and response capabilities.

Optimal: Organization building and systems & processes — Same as the Advanced level. Technologies & tools — The capabilities of detecting, analyzing, and responding to unknown network threats are optimized to continuously reduce their impact on networks. Data operations — Comprehensive and specific data metrics are formulated and continuously optimized for network threat detection and response management.

6.4 Software Defined Perimeter (SDP)

In the zero trust architecture, SDP refers to the capabilities of turning passive defense based on traditional static boundaries to proactive defense based on dynamic boundaries in order to effectively isolate enterprise applications from insecure networks. The capabilities at each level are as follows:

Initial: Organization building — Roles and responsibilities for network access control management are not specified. Systems & processes — Management requirements for network access control are not specified. Technologies & tools — No network access control is performed, or only traditional firewall policies are used for access control.

Partially managed: Organization building — Network access control is preliminarily managed by relevant personnel. Systems & processes — Management requirements for network access control are specified. Technologies & tools — Identity authentication is performed on network access requests to implement network access control.

Established: Organization building — Management positions and personnel for network access control have been specified, and management responsibilities have been clearly defined. Systems & processes — Comprehensive and detailed specifications and processes for network access control management have been developed. Technologies & tools — Application resources are visible only to authorized users; real-time verification is implemented based on multiple factors (such as identity authentication and network context) for continuous access control over network resources. Data operations — A few data metrics (such as the DDoS defense rate and resource invisibility coverage rate) are preliminarily formulated to measure the capability of dynamic access control over network resources.

Advanced: Organization building — Management positions and personnel for network access control have been optimized, and a professional security operations team is in place to establish and optimize the automatic adjustment mechanism of network access control policies. Systems & processes — Specifications and processes for network access control management are continuously optimized, including the automated access policy change process. Technologies & tools — Security control points are moved to edge sites; machine learning is used to assess the risk status and network identities of access endpoints and automatically allocate access resources. Data operations — Data metrics are continuously optimized to measure the capability of edge network access control.

Optimal: Organization building and systems & processes — Same as the Advanced level. Technologies & tools — They are continuously optimized to cover more SDP scenarios and implement adaptive network access control and response. Data operations — Data metrics are continuously optimized.

7 Workload/Application Security

Workload/Application security is an important part of the zero trust architecture. It is gaining importance as cloud computing thrives. Therefore, security protection must be enhanced to ensure the security of components (such as those at the application layer, computing containers, and VMs) to the greatest extent. Core capabilities involved in workload/application security include: (1) secure application access; (2) open-source and third-party code security; (3) DevSecOps; (4) security configuration.

7.1 Secure Application Access

In the zero trust architecture, secure application access refers to the capabilities of performing access control between applications or services through policy-based context-aware dynamic credentials. The capabilities at each level are as follows:

Initial: Organization building — Management roles and responsibilities for secure application access are not specified. Systems & processes — Management requirements for secure application access are not specified. Technologies & tools — Interaction between applications does not need to be authenticated, and access control is simply implemented through simple isolation measures.

Partially managed: Organization building — Secure application access is preliminarily managed by relevant personnel. Systems & processes — Management policies and requirements for secure application access have been developed. Technologies & tools — Identity authentication between key applications is implemented, and access credentials are manually managed and replaced.

Established: Organization building — Management positions and personnel for secure application access have been specified, and management responsibilities have been clearly defined to plan and implement inter-application access policies and credential management. Systems & processes — Comprehensive and detailed implementation specifications and operation guidelines for application access security management have been developed. Technologies & tools — Identity authentication is implemented among all applications, credentials are automatically managed and periodically replaced, and the operations and use of credentials are manually monitored and responded. Data operations — Data metrics (such as the automated credential management rate and inter-application authentication coverage rate) are preliminarily formulated for application access security management.

Advanced: Organization building — Management positions and staffing for secure application access have been optimized, and management responsibilities have also been optimized to plan and implement inter-application access policies and credential management. Systems & processes — Implementation specifications and operation guidelines for application access security management have been continuously optimized, including dynamic access policy management, based on the dynamically adjusted inter-application access policies of the organization. Technologies & tools — Dynamic authentication is performed for inter-application access based on the environment context, and automation tools are used to monitor the operations on and use of credentials in a visualized manner. Data operations — Specific data metrics (such as the accuracy of dynamic policies) are formulated to measure the capabilities of dynamic secure application access and automated credential management.

Optimal: Organization building and systems & processes — Same as the Advanced level. Technologies & tools — Big data and AI are used to analyze historical access information and adaptively adjust application authentication rules. Data operations — Comprehensive and specific data metrics are formulated and continuously optimized for secure application access capabilities.

7.2 Open-Source and Third-Party Code Security

In the zero trust architecture, open-source and third-party code security refers to the capabilities of ensuring the security of binaries, repositories, or source code that are used to build applications by performing multi-level automated security check. The capabilities at each level are as follows:

Initial: Organization building — Management roles and responsibilities for open-source and third-party code security are not specified. Systems & processes — Management requirements for open-source and third-party code security are not specified. Technologies & tools — Open-source or third-party code is not scanned, and executable files are scanned manually if necessary.

Partially managed: Organization building — Open-source and third-party code security is preliminarily managed by relevant personnel. Systems & processes — Management requirements for open-source and third-party code security have been developed. Technologies & tools — Source code security checks are performed on a regular basis manually and automatically (by using security scanning tools), and discovered vulnerabilities are fixed and validated.

Established: Organization building — Management positions and personnel for open-source and third-party code security have been specified, and management responsibilities have been clearly defined to plan and implement code review, code repository management, binary file verification, and more. Systems & processes — Comprehensive and detailed implementation specifications and operation guidelines for open-source and third-party code security management have been developed, including third-party code repository management specifications and binary file verification processes. Technologies & tools — Security scanning tools are used to verify source code, third-party repositories, and binary files, and vulnerabilities are fixed in real time. Data operations — Data metrics (such as the security check coverage rate of open-source and third-party code) are preliminarily formulated for open-source and third-party code security management.

Advanced: Organization building and systems & processes — Same as the Established level. Technologies & tools — Automated analysis tools are used to learn security requirements and historical issues so as to implement multi-level automated checks and visualized monitoring. Data operations — Specific data metrics (such as the vulnerability detection accuracy) are formulated for open-source and third-party code security to measure the automated security detection and monitoring capabilities of open-source and third-party code.

Optimal: Organization building and systems & processes — Same as the Established level. Technologies & tools — They are continuously optimized to accurately discover code vulnerabilities, and technologies (such as advanced association) are used to adaptively adjust remediation policies. Data operations — Data metrics are formulated and continuously optimized for open-source and third-party code security management.

7.3 DevSecOps

In the zero trust architecture, DevSecOps refers to the capabilities of prioritizing security in code development and implementing quick response and agile iteration from development to operation. The capabilities at each level are as follows:

Initial: Organization building — Management roles and responsibilities for DevSecOps are not specified. Systems & processes — DevSecOps management requirements are not specified. Technologies & tools — Some security activities (such as the security test before rollout) are performed if necessary in the DevSecOps lifecycle.

Partially managed: Organization building — DevSecOps is preliminarily managed by relevant personnel. Systems & processes — DevSecOps management requirements have been developed. Technologies & tools — Security activities (such as security design and secure coding) are implemented in some DevSecOps phases, especially security control performed in the requirement, design, and development phases.

Established: Organization building — DevSecOps management positions and personnel are specified, management responsibilities have been clearly defined, the security awareness of related roles is continuously raised, and security management in each DevSecOps phase is planned and implemented. Systems & processes — Comprehensive and detailed implementation specifications and operation guidelines for DevSecOps have been developed, including security design/test specifications and security deployment processes. Technologies & tools — Security activities have been fully integrated into each DevSecOps phase, and related tools/platforms (such as the code review tool and vulnerability scanning tool) have been introduced to execute

security activities. Data operations — Data metrics (such as the number of security defects in DevSecOps and defect rectification rate) for DevSecOps have been preliminarily formulated to measure the overall DevSecOps management capability in organizations.

Advanced: Organization building — DevSecOps management positions and responsibilities have been optimized, and security management in each DevSecOps phase has been continuously improved. Systems & processes — DevSecOps implementation specifications and process guidelines are continuously optimized based on the organization's new DevSecOps policy, including the security-policy-as-code process. Technologies & tools — Security-policy-as-code can be automatically optimized based on historical issues and security requirements learned, and visualized process monitoring is implemented. Data operations — Specific data metrics are formulated for DevSecOps to measure the effectiveness of security-policy-as-code and visualized monitoring capabilities.

Optimal: Organization building and systems & processes — Same as the Advanced level. Technologies & tools — Technologies, such as big data analytics and machine learning, are used to achieve adaptive correction. Data operations — Comprehensive data metrics throughout the DevSecOps lifecycle are formulated and continuously optimized.

7.4 Security Configuration

In the zero trust architecture, security configuration refers to the capabilities of performing version control over configuration files through the configuration policy as code, and implementing configuration security management of virtualization infrastructure in a more intelligent and efficient manner. The capabilities at each level are as follows:

Initial: Organization building — Management roles and responsibilities for configuration and image management are not specified. Systems & processes — Management requirements for security configuration and image security are not specified. Technologies & tools — No security control is performed via IT systems for configuration and image management.

Partially managed: Organization building — Security configuration and image security are preliminarily managed by relevant personnel. Systems & processes — Management requirements for configuration and image security have been developed. Technologies & tools — Regular security checks, audits, and monitoring are performed on images and configurations.

Established: Organization building — Management positions and personnel for security configuration and image security have been specified, and management responsibilities have been clearly defined to plan and implement security management of VM and container configurations, images, and runtime processes. Systems & processes — Comprehensive and detailed implementation specifications and operation guidelines for VM and container configurations and images have been developed, including security configuration management and image security management. Technologies & tools — Configuration-policy-as-code is implemented for some security configurations; automation tools are used to scan, monitor, and fix images. Data operations — Data metrics (such as the configuration-policy-as-code coverage rate) are preliminarily formulated for security configuration, image security, and runtime process security capabilities.

Advanced: Organization building and systems & processes — Same as the Established level. Technologies & tools — Security configuration is performed on the runtime infrastructure through the configuration policy as code; the real-time image status is monitored in a visualized manner by using the self-test tool, and alarms are automatically generated for process exceptions; process traffic of VMs can be detected and analyzed to identify VM escape vulnerabilities. Data operations — Specific data metrics are formulated to measure the effectiveness of configuration-policy-as-code and automated configuration and monitoring capabilities.

Optimal: Organization building and systems & processes — Same as the Established level. Technologies & tools — AI is used to predict, analyze, and identify potential configuration tampering or vulnerabilities, and adaptive fixing and continuous optimization are performed. Data operations — Comprehensive data metrics are formulated and continuously optimized for security configuration, image security, and runtime process security.

8 Data Security

In the zero trust architecture, data is a key object to be protected. Organizations should accurately identify and develop protection measures for sensitive data in the entire management environment to ensure that data is protected from unauthorized access or breaches during storage, transmission, and use. Core capabilities involved in data security include: (1) data discovery and classification; (2) data masking; (3) data leakage prevention; (4) data lineage.

8.1 Data Discovery and Classification

In the zero trust architecture, data discovery and classification refer to the capabilities of identifying, labeling, and classifying data to ensure that organizations can discover and protect different types of data in a timely and accurate manner. The capabilities at each level are as follows:

Initial: Organization building — Management roles and responsibilities for data classification are not specified. Systems & processes — Security management requirements for data classification and categorization are not developed. Technologies & tools — The organization's data is not identified or classified, and data of each system is managed by the corresponding owner.

Partially managed: Organization building — Data discovery and classification are preliminarily managed by relevant personnel. Systems & processes — Management policies and requirements for data classification have been developed. Technologies & tools — Data in key domains is identified and classified by tools.

Established: Organization building — Management positions and personnel for data discovery and classification have been specified, and management responsibilities have been clearly defined to plan and implement data discovery rules and classification/categorization standards. Systems & processes — Comprehensive and detailed management specifications and processes for data classification/categorization have been developed, including category label management and data level change processes. Technologies & tools — Tools are deployed for different types of data to automate identification, classification, and labeling, and the identification policies are manually configured. Data operations — Data metrics are preliminarily formulated for data identification and classification to roughly measure the overall effectiveness of data classification management in organizations.

Advanced: Organization building and systems & processes — Same as the Established level. Technologies & tools — Data labels and policies are managed in a unified manner, and machine learning is used to better manage data identification policies of vital systems. Data operations — Specific data metrics (such as the accuracy of machine learning and metadata integrity) are formulated to monitor the management capabilities of automated data identification, classification, and labeling.

Optimal: Organization building and systems & processes — Same as the Established level. Technologies & tools — AI and machine learning are used to improve the computing models for data identification and labeling. Data operations — Comprehensive and specific data metrics are formulated and continuously optimized for the management of data identification, classification, and labeling.

8.2 Data Masking

In the zero trust architecture, data masking refers to the capabilities of transforming sensitive information based on masking rules to reliably protect sensitive privacy data and ensure the security of data at rest, in transit, and in use. The capabilities at each level are as follows:

Initial: Organization building — Management roles and responsibilities for data masking are not specified. Systems & processes — Security management requirements for data masking are not specified. Technologies & tools — Data masking is not performed.

Partially managed: Organization building — Data masking is preliminarily managed by relevant personnel. Systems & processes — Data security management policies and data classification/masking management requirements have been developed. Systems & tools — Some application systems have independently implemented sensitive data masking.

Established: Organization building — Management positions and personnel for data masking have been specified, and management responsibilities have been clearly defined to plan and implement data classification and masking principles and standards. Systems & processes — Comprehensive and detailed security management specifications and processes for data masking have been developed, including the masking algorithm rollout process and masking method change process. Technologies & tools — Data masking is performed by a unified platform for all systems involving sensitive data, especially in cross-border transfers of personal data, and the masking policy is manually configured. Data operations — Data metrics (such as the number of data masking failures) are preliminarily formulated to roughly measure the overall effectiveness of data masking management in organizations.

Advanced: Organization building and systems & processes — Same as the Established level. Technologies & tools — Machine learning is used to learn data content and historical masking scenarios to automatically adjust masking policies for different scenarios and different types of data. Data operations — Specific data metrics are formulated to monitor the management capability of automated data masking based on classification labels.

Optimal: Organization building and systems & processes — Same as the Established level. Technologies & tools — AI and machine learning are used to optimize the technical models of scenario identification and automated masking policies. Data operations — Comprehensive and specific data metrics are formulated and continuously optimized for data masking management.

8.3 Data Leakage Prevention

In the zero trust architecture, data leakage prevention refers to the capabilities of automatically and continuously detecting, preventing, and responding to violations of organizational data security policies during the use, storage, and transmission of sensitive data to prevent accidental leakage of sensitive data. The capabilities at each level are as follows:

Initial: Organization building — Management roles and responsibilities for data leakage prevention are not specified. Systems & processes — Security management requirements for data leakage prevention are not specified. Technologies & tools — Data leakage prevention measures are not adopted, or only traditional (coarse-grained) methods, such as data encryption and post-event audit, are used for data leakage prevention.

Partially managed: Organization building — Data leakage prevention is preliminarily managed by relevant personnel. Systems & processes — Data security policies and data leakage prevention management requirements have been developed. Technologies & tools — In some scenarios, leakages of common types of data can be detected through single factors (such as keywords or data labels), visualized alarms can be generated, and manual response is made.

Established: Organization building — Management positions and personnel for data leakage prevention have been specified, and management responsibilities have been clearly defined.

Systems & processes — Comprehensive and detailed management specifications and processes for data leakage prevention have been developed. Technologies & tools — Leakages of complex types of data can be detected in service scenarios based on multiple factors (such as data behavior or content context), and measures can be automatically executed. Data operations — A few coarse data metrics (such as the number of sensitive data leakages per week or month) are formulated to roughly measure the overall effectiveness of data leakage prevention in organizations.

Advanced: Organization building — Same as the Established level. Systems & processes — Management specifications and processes for data leakage prevention are continuously optimized, such as sensitive data discovery policies. Technologies & tools — Machine learning algorithms are used to analyze the data status in each phase, generate data leakage detection rules, and apply them to all data leakage detection scenarios. Data operations — Specific data metrics (such as the sensitive word identification accuracy and the number of false positives/negatives) are formulated to track the capability of machine learning to detect sensitive data leakages and implement data visualization.

Optimal: Organization building — Same as the Established level. Systems & processes — Same as the Advanced level. Technologies & tools — Data leakage detection rules are continuously optimized to improve the detection accuracy. Data operations — Specific data metrics are formulated and continuously optimized for data leakage prevention management.

8.4 Data Lineage

In the zero trust architecture, data lineage refers to the capabilities of automatically tracing the real-time data location and processing throughout the lifecycle, improving data visibility and quality, and reducing data flow risks. The capabilities at each level are as follows:

Initial: Organization building — Management roles and responsibilities for data lineage analysis are not specified. Systems & processes — Security management requirements for data lineage analysis are not specified. Technologies & tools — A single type of data lineage diagram is manually drawn if necessary, and data flow risks are not identified (or seldom identified).

Partially managed: Organization building — Data lineage is preliminarily managed by relevant personnel. Systems & processes — Data security policies and data lineage management requirements have been developed. Technologies & tools — Tools are used to identify critical data assets and data lineage information, and data lineage risks are manually analyzed and visualized.

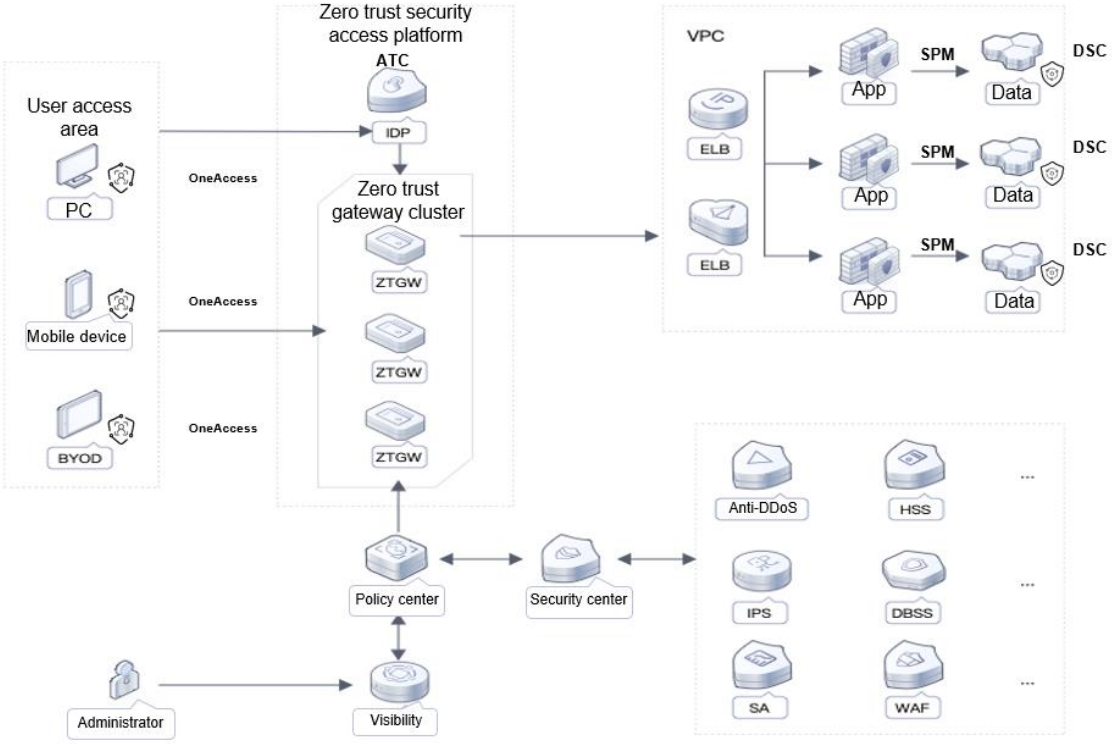
Established: Organization building — Management positions and personnel for data lineage have been specified, and management responsibilities have been clearly defined to plan and implement sensitive data flow identification, analysis, risk mitigation, and disposal. Systems & processes — Comprehensive and detailed management specifications and processes for data lineage have been developed, including requirements for data lineage analysis frequency and input sources. Technologies & tools — Policies are manually configured on the unified tool/platform to automatically discover data and related information, draw various data lineage diagrams, and identify and report risks. Data operations — A few coarse metrics are formulated to measure the effectiveness of data lineage in organizations.

Advanced: Organization building and systems & processes — Same as the Established level. Technologies & tools — The machine learning-based platform is used to automatically identify data lineage information, create risk assessment policies, collect data lineage information in real time, and reports risks. Data operations — Specific data metrics (such as the data lineage granularities by table, column, field, and field value) are formulated to measure the capabilities of machine learning algorithms and data lineage information identification.

Optimal: Organization building and systems & processes — Same as the Established level. Technologies & tools — Data lineage information discovery and risk assessment policies are continuously optimized, data lineage information is collected in real time, and risks are reported. Data operations — Specific data metrics are formulated and continuously optimized for data lineage management.

9 Zero Trust Practices of Huawei Cloud

The zero trust solution of Huawei Cloud highlights identity-centric security. It protects applications, data, and other resources through dynamic access control and fine-grained authorization, and builds end-to-end adaptive security capabilities for Huawei Cloud. The following figure shows the key capability structure.



Unified identity management (OneAccess): provides unified management and settings of users, organizations, user groups, applications, accounts, and credentials, and provides data synchronization, password policies, and user self-services to help enterprises and administrators manage user identities throughout the lifecycle.

Dynamic policy-based access control (ATC): performs deep learning based on device risks, access behaviors, native service alarms of other clouds, and reputation databases to build reliable, precise dynamic policies, and perform continuous authentication and dynamic fine-grained access control.

Application security topology (ATC): displays risks of all cloud application instances in a visualized manner, and builds a unified application security portal for invisibility to public networks. It automatically recommends required security services based on security solution experience and traffic characteristics.

Network micro segmentation (SPM): manages access control policies based on hosts, automatically delivers access control policies during service capacity expansion, visualizes access traffic between cloud service hosts, dynamically adjusts host policies, and detects, warns, and handles abnormal traffic.

Data security management (DSC): implements security visualization of tenant cloud data throughout the lifecycle, including collection security, transmission security, storage security, use security, exchange security, and destruction security; builds a unified data security portal to manage the status of each period.

Sensitive data identification (DSC): accurately identifies sensitive data in the database based on the sensitive data discovery policy, and protects full-stack sensitive data based on multiple preset and user-defined masking algorithms.

10 Conclusion

Against the backdrop that zero trust has become a new trend of cyber security development, this white paper is released to share the zero trust capability maturity model implemented in Huawei Cloud with customers and the industry, explore how to assess zero trust capability maturity, and promote the industry's zero trust capability development. Moreover, Huawei Cloud will continue to release high-quality zero trust products and services to improve its security protection capabilities and help customers ensure business compliance and security.

11 Appendix – Main Reference Sources

The reference sources include but are not limited to:

[1] DOD Zero Trust Reference Architecture

[2] NIST SP 800-207, Zero Trust Architecture

[3] Forrester: The Zero Trust eXtended Ecosystem

[4] Gartner: 2021 Strategic Roadmap for SASE Convergence

[5] Microsoft: Zero Trust Maturity Model

[6] CSA: Software-Defined Perimeter (SDP) Specification v1.0

[7] IDC Report: New Trends in China's Network Security Market — Zero Trust Market Research