AT&T Cybersecurity

A report from AT&T Cybersecurity
and AT&T Chief Security Office

Published 01 June 2020

Tightly Control and Manage Access to Applications and Services with Zero Trust

A Perspective from the AT&T Chief Security Office (CSO)

AT&T
Business

Contents

Executive Summary

As businesses increasingly embrace mobile, cloud, and edge computing, network traffic patterns are changing. This is due to the expectation for anytime, anywhere access to the network and the emergence of technologies that require security to be delivered closer to individual users, devices, applications, and data. Enterprises are also wrestling with an increasingly large and complex attack surface, and security leaders are looking for ways to simplify processes and policy, consolidate security tools, and minimize risk while also being able to quickly adapt to the unforeseen threats that will arise with new technology.

In our journey to develop a dynamic model for resilient, flexible enterprise security, the AT&T Chief Security Office (CSO) recognizes the increasing importance of implementing effective network security controls based on Zero Trust (ZT) principles, as well as being able to tightly manage and control access to the business without creating friction that could hinder day–to–day operations.

We have also observed the waning effectiveness of legacy technologies to manage identity and access. For example, using source IP addresses are problematic because they were never designed to authenticate traffic. Authentication was handled by technologies at higher levels of the stack, typically the operating system (OS) and application layers. For network connectivity, this default results in an excessive amount of implicit trust that is unreasonable in today's digital environment.

This paper outlines the AT&T CSO's current point of view on how to most effectively manage access control today, considering the adoption of cloud and edge technologies and the realities of a remote workforce. Our point of view includes elements from several industry frameworks, including but not limited to Forrester's Zero Trust Model of information security, Gartner's frameworks for Continuously Adaptive Risk and Trust Assessment (CARTA) and Secure Access Services Edge (SASE), as well as research on software defined perimeters (SDPs).

We fundamentally believe that organizations can no longer assume everything "inside the network" is safe. Therefore, security professionals must treat all network traffic as untrusted until verified. This means strictly enforcing access controls and inspecting and logging all traffic. We also believe that an approach for managing and controlling access must be adaptable and scalable, able to evolve with the technologies of tomorrow, and serve dynamic access requirements without disrupting a plan for efficiency of a cybersecurity budget.

> Virtual networking is still maturing, and vendors are offering a large number of solutions to help deploy "next–generation" networks. Without going into the details of those solutions in this paper, we do believe network transformation (partial or whole) is a requirement for organizations that want to keep up with the demands of digital business.

Additionally, ZT principles cannot be superimposed on legacy network infrastructure and operations. A critical part of implementing ZT strategies includes rebuilding or refreshing the network with the intention of moving partially or completely to network virtualization (NV) or the cloud. Using NV and cloud services, security professionals can more easily make use of software–based technology to achieve more granular network segmentation and to centralize security controls. They can also take advantage of analytics, programmable orchestration and automation to quickly turn off and on network and security controls for applications, devices, users, and data as needed. This also helps provide that security is pervasively infused into the network fabric, thus making the network itself a tool that contributes to the overall security of the enterprise.*

Introduction

Like any security framework, ZT has evolved over the years, influenced by practitioners with real–life experiences and ongoing industry feedback. Though access control has always been a part of ZT, in 2019 Forrester "formalized" the requirement to "limit and strictly enforce access control" into a core, critical pillar of the framework — of equal importance to network security.

This move to emphasize the importance of managing and controlling access reflects a larger shift in the industry to distributed, pervasive security. Security professionals are realizing the need to push security to the edge and to focus as much on the entity requesting access as on the data or service the access is being requested for and why the request is being made. This is a direct result of the digital revolution we are seeing in business and perhaps most expressly, cloud adoption, the emergence of edge applications and compute, and the decentralization of the global workforce.

Whether beginning your journey or continuing down the path of migration to a ZT environment, there are several critical concepts related to access control that should be considered. The AT&T CSO has framed these concepts into 4 key areas (see figure 1):

1. **Visibility and inventory:** Identify and map the flow of sensitive data; create and maintain a comprehensive inventory of hardware devices, applications, and other software and hardware assets, including gaining visibility to all devices that access enterprise IT systems; catalogue information about the security posture of each; use this information to help establish trustworthiness
2. **Microsegmentation:** Isolate applications and devices closer to the workload, including setting up microperimeters by using software–defined perimeters (SDPs) or other edge controls, including next–generation firewalls (NGFWs), containers, native APIs of the cloud fabric, etc.

Forrester recommends taking the following steps to move closer to a ZT environment. However, a road map to ZT is not something to be taken lightly.

Zero Trust requires a rebuild or refresh with an eye to network virtualization versus simply overlaying ZT principals on a legacy network architecture.

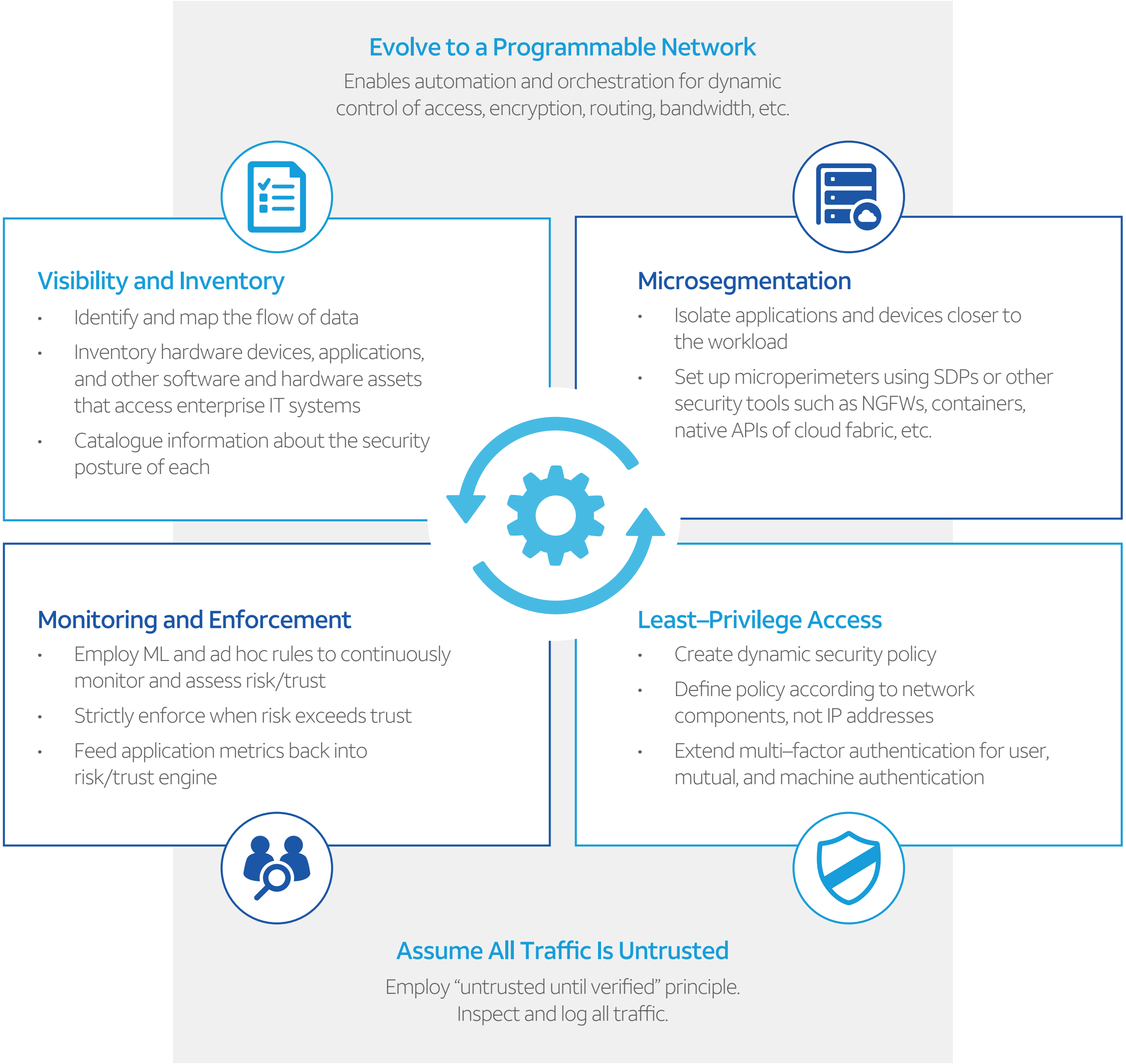
- Identify and map the flows of sensitive data
- Employ network segmentation with Zero Trust microperimeters
- Continuously monitor your ecosystem using analytics
- Embrace automation and orchestration

3. **Least–privilege access:** Exercise the principles of "least privilege access" by creating dynamic security policy and extending multi–factor authentication for user, machine, and mutual authentication
4. **Monitoring and enforcement:** Continuously monitor the acceptance of risk and trust for each entity (users, devices, and applications) by developing a risk/trust engine that makes use of machine learning (ML) and ad hoc rules to score all network flows and connections; strictly enforce policy; create a feedback loop to deliver application metrics and data back into the system to further inform risk/trust decision making

For optimal outcomes, each of the 4 areas above should be infused with the following:

- Treat all entities and network requests as untrusted until verified, and therefore inspect and log all traffic; continuously monitor interactions and adjust as needed
- Achieve ZT by embracing network function virtualization and/or cloud services to take advantage of analytics and programmable orchestration and automation systems, including technologies that can help manage the "spread" of today's network within a single console
- Use an enterprise configuration and operations management platform (open source or private) for policy–driven automation and orchestration of security and networking functions

Figure 1: Using Zero Trust to tightly control and manage access



Evolve to a Programmable Network

Enables automation and orchestration for dynamic control of access, encryption, routing, bandwidth, etc.

Visibility and Inventory

- Identify and map the flow of data
- Inventory hardware devices, applications, and other software and hardware assets that access enterprise IT systems
- Catalogue information about the security posture of each

Microsegmentation

- Isolate applications and devices closer to the workload
- Set up microperimeters using SDPs or other security tools such as NGFWs, containers, native APIs of cloud fabric, etc.

Monitoring and Enforcement

- Employ ML and ad hoc rules to continuously monitor and assess risk/trust
- Strictly enforce when risk exceeds trust
- Feed application metrics back into risk/trust engine

Least–Privilege Access

- Create dynamic security policy
- Define policy according to network components, not IP addresses
- Extend multi–factor authentication for user, mutual, and machine authentication

Assume All Traffic Is Untrusted

Employ "untrusted until verified" principle.
Inspect and log all traffic.

Inventory IT systems and use the information to establish trustworthiness

Every major cybersecurity framework, from the NIST CSF to the ISO/IEC 27000–series and beyond, calls for an organization to create and maintain an accurate inventory of devices connected to the network, including assets with the potential to store and process information, regardless of network connection status. Organizations can use this information to track a device as it moves through its lifecycle and provide that only the devices with the appropriate level of trustworthiness (whether corporate–managed or bring your own device, BYOD) can access network services.

Organizations should inventory personal and corporate–managed user applications and devices/assets, as well as those that are shared and commonly used, such as terminal servers, hosted virtual desktops (HVD), or virtual machines used by clients as desktops. However, simply gaining visibility is not enough. It is critical to capture multiple pieces of information about the security posture of each and identify each device/asset with fingerprinting technology.

Organizations can then use this information to establish the trustworthiness of a particular entity that is requesting access by cross–referencing its characteristics upon every individual login. Consider that ZT guidelines recommend establishing trustworthiness in 2 ways: 1) verify that the device/asset has been given access to the particular data, service, or application in the past, and 2) mandate that it currently meets the organization's security requirements (such as having the latest version of the operating system or encryption enabled). In addition, the device/asset should be identified as owned and managed by the organization or by an employee or other trusted and verified entity.

To further verify trustworthiness, organizations should score multiple attributes, including but not limited to the following for each device/asset:

- Certifications, geographic location, serial number, and operating system (OS) fingerprint
- Missing OS or application patches
- Trust score and user trust score, role or groups, place of residence, and user authentication model
- Manufacturer and trusted platform module (TPM) manufacturer and version
- Current location and IP address; whether or not the IP address is known and controlled by the organization
- Number of recent logins and last geographic login location

Mobile devices, in particular, can provide additional information which can be used as device authentication factors, such as the International Mobile Equipment Identity (IMEI), the unique number given to every single mobile phone. For example, in addition to relying on certificates, the AT&T CSO uses a strong device identifier natively provided by the mobile operating systems.

Because device access is typically associated with users and their roles or status, organizations should tightly manage all users in a database, including tracking their job category, role and responsibility, group membership, or affiliation. Supply chain affiliates, contractors, and others who need access to the network should also be tracked. Employee information should be integrated with HR systems and processes to ensure data is up–to–date, including accounting for job changes, company departures, and more.

All of these tools together help provide that only authenticated devices and users with the appropriate credentials, security risk profile, and trust score are authorized access as requested.

Isolate applications and devices closer to the workload

To limit malicious movement across hybrid networks and protect critical data and services, organizations should establish secure zones through the use of microsegmentation technologies. These include microperimeters or software–defined perimeters (SDPs) that can isolate devices and applications closer to the workload/service being protected. There are many other tools for microsegmentation, including next–generation firewalls (NGFWs), network overlays, software–defined network (SDN) integration, host–based agents, virtual appliances, containers, security groups, container–based clusters (such as Kubernetes and Swarm), or native APIs of the underlying cloud fabric.

The CSO views SDPs with identity–aware access control as one of the most practical solutions for microsegmentation because SDPs can significantly improve the security controls of an organization while also enabling the organization to provide anywhere, anytime access to applications and services from virtually any device. With SDPs, a user is not required to figure out the method of access based on the context of where they are, what time of day it is, or what type of device they are using — the network takes care of this.

Additionally, SDPs can provide several layers of protection, as follows.

- IT services are initially hidden from all users, and a named user cannot access a service until a sufficient level of trust is established — authenticate first and then connect.
- The level of trust is established at the time a user tries to connect, and decision to trust is based on identity and multiple contextual factors, such as device trust, user trust, location, and time of day.
- The level of access granted to a user is granular (providing “precision access”), and access is configured for least privilege, typically to a specific application or service based on the user’s identity and role.
- Trust broker, controller, or service validates the appropriate level of trust for both the user and device. This is then communicated to a gateway or agent that protects the service. Once this is achieved, an outbound connection is typically made from the gateway to the user (removing the need for inbound firewall rules). This can also significantly reduce an enterprise’s attack surface.

The AT&T CSO is closely following several emerging market models that predict the merging of network and security services into a powerful suite of solutions delivered via the cloud, as–a–service. For example, a suite of security services might include the following technologies: software–defined perimeter (SDP), secure web gateway (SWG), web application firewalls (WAF)/firewall–as–a–service (FWaaS), cloud application discovery, security groups within cloud environments, and more.

The combined benefits of such a solution include simplicity, scalability, flexibility, and enhanced security. In addition, a cloud access security broker (CASB) can provide an enforcement point between cloud service consumers and providers where the CASB aggregates and interjects an enterprise’s security policies as cloud–based resources. This is paired with SDP, WAF/FWaaS to deliver such things as: obfuscation, network access control (NAC), inspection, and dynamic brokering of least–privilege authorization. When combined with identity federation technologies, a CASB can also help manage the spread of shadow IT solutions.

Exercise least–privilege access policies

Automate and orchestrate authentication and authorization

A critical component of managing access to enterprise applications and services is the ability to take advantage of programmable orchestration and automation systems so teams can easily and rapidly manage the network and security controls for applications, devices, users, and data as needed, centralize security policy management, and support enforcement at scale for device deployment and configuration.

It also allows enterprises to centrally manage, automate, and orchestrate user and application authentication, device authentication, and trust scoring. Authentication of an entity should require an inspection of the multiple actions taken by both users and by applications. For example, device authentication should require a continuous evaluation of the security posture, condition, and state of the device to compute a "trust score" that is used in assessing whether or not that entity is allowed access. The application, device, and score combine to form an "agent." An organization's security policy is then applied to the agent in order to authorize a request or deny it. The rich information contained within the agent allows for very flexible, fine–grained access control and enforcement. Using an automation/orchestration platform, organizations can continuously adapt access control according to variable conditions.

Once a request is authorized, the platform (which should sit in the control plane) signals the data plane to accept the incoming request, and at the same time, configure encryption details. Transport encryption can be applied at the device level, application level, or both. At least one is required for confidentiality.

These authentication and authorization components, along with the aid of the control plane in coordinating encrypted channels, provide that every single flow on the network is authenticated as expected. Hosts and network devices will drop traffic if all of the components have not been applied to the traffic. Additionally, by logging each of the control plane events and actions, organizations can easily audit network traffic on a flow–by–flow or request–by–request basis.

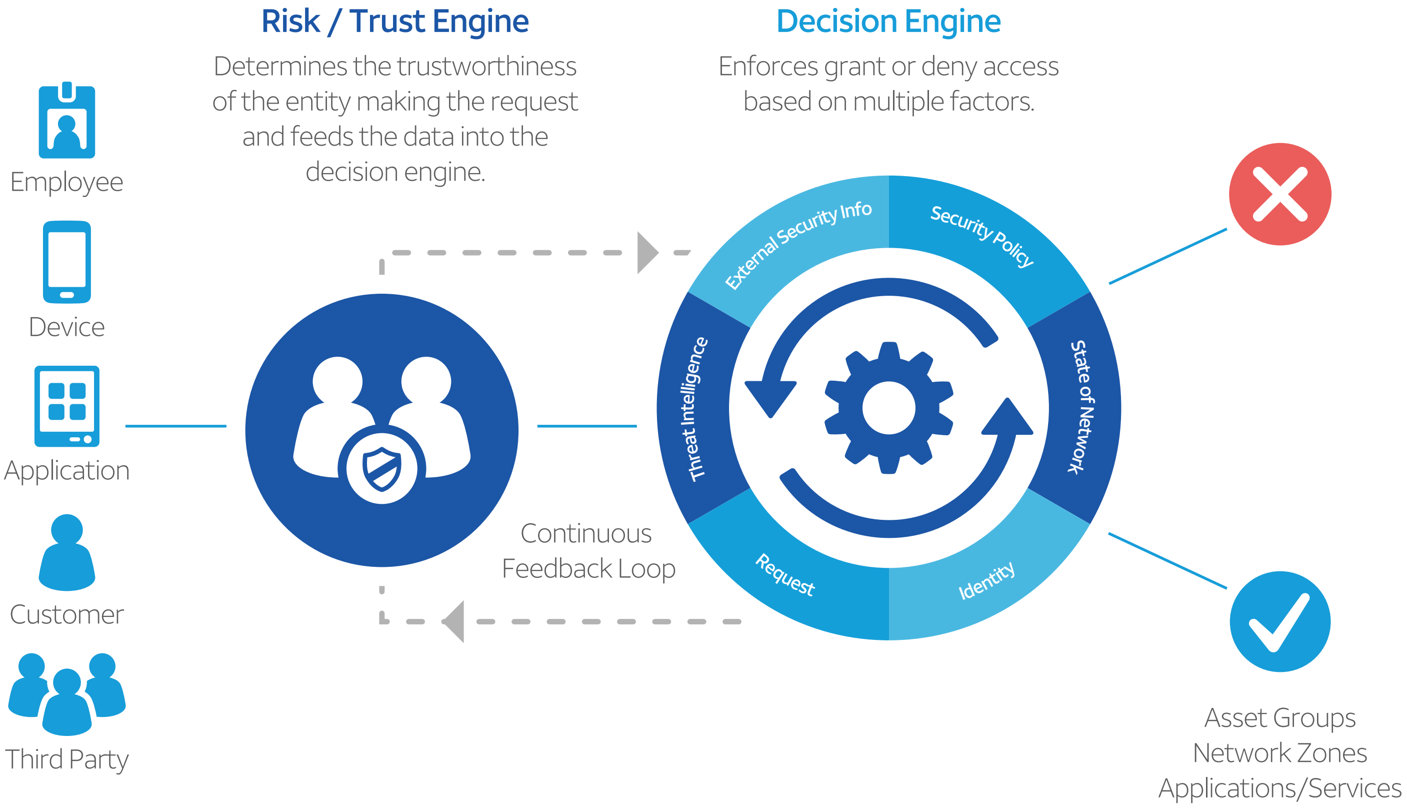
Define policy according to logical components; use security tags/labels

Over the years, IP addresses have become the de facto method used to verify identity, with security pros setting up policies on firewalls to authenticate access. However, this is an outdated and ineffective method in today's dynamic network environments. IP addresses are ephemeral in nature, and this is especially true for mobile users and source network address translation (SNAT), as well as in cloud–based and edge applications. In addition, entities can easily hide behind IP addresses with masquerading.

Instead of defining access policy by IP addresses or ranges of address, enterprises should define policy according to components in a network, such as network services, device classes, and user roles. In a virtualized or cloud network, security tags/labels can be used to define policy rules around those components, specifying which traffic is allowed to access specific network zones, devices and assets, or applications. For example, Kubernetes uses labels to identify pods (a group of containers that are deployed together on the same host) and define the rules that determine what traffic is allowed to access the pods.

Using these tools, enterprises can more tightly and dynamically manage access, even as network components change or evolve. Identity authentication can be specific to the entity making a request for an application or service, and authorization can be limited per data element or at minimum per request. For example, a decision engine that authorizes or denies access can be pre–loaded with policy and other inputs from a risk engine which determines the trustworthiness of the entity making the request. The decision engine then makes enforcement decisions based on its knowledge of the current state of the network, the identity, the policy, the device, the service, and external security reconnaissance. (See figure 2)

Figure 2: Dynamically manage and enforce access with a risk / trust engine



In concrete terms, a web service running on one server today might be on a different server tomorrow, or it may even move between servers automatically as directed by a workload scheduler. The policy definition needs to be divorced from these implementation details in order to be able to adapt to the dynamic nature of today's hybrid networks. Authorization should use multi–factor authentication (and more) for user, machine, and server/client.

It is also important to remember that an enterprise's access solutions and policies for controlling that access need to be aligned to day–to–day business operations. This helps to avoid disruption or friction for the users and machines that need to legitimately access applications, files, and services.

For tools that authorize access, enterprises should use multiple forms of authentication, including user, mutual (server and client), and machine authentication. Enterprises should also expand authentication protocols to include additional factors for both internal and external entities that need access to the network.

User authentication. The main authentication factors in use for today's Multi–Factor Authentication (MFA) processes are: 1) something you know, 2) something you have, and 3) something you are. In addition, security professionals should consider including additional authentication factors such as the location of the user or the state of the device.

Since authentication occurs at network layers 5–7, protocol–specific authentication mechanisms can be used, if available, for further authentication. A good example of such a protocol is HTTPS and its capabilities to support server and client certificates. For example, AT&T CSO makes extensive use of these Transport Layer Security (TLS) certificates and an internal Certificate Authority (CA). Organizations can also make use of push notification authentication, which sends the user an alert, typically on their mobile device, when authentication is taking place along with a one–time use token.

A web service running on one server today might be on a different server tomorrow, or it may even move between servers automatically as directed by a workload scheduler.

The policy definition needs to be divorced from these implementation details in order to be able to adapt to the dynamic nature of today's hybrid networks.

Authorize using multi–factor authentication (and more) for user, machine, and server/client.

Mutual authentication. Mutual authentication requires that both the server and the client prove their respective identities to each other before performing any communication–related functions. Identities are commonly proven with the use of a public or private key infrastructure, and since a majority of IT traffic is now HTTPS, organizations can use the existing and proven TLS client and server certificate method for authentication. In a web–based, mutual authentication process, communication can occur only if the client and the server trust each other's digital certificates. The certificate exchange is done through TLS protocol. This simply means that the server must be sure of the client's identity and the client must be sure of the server's identity.

The 3 commonly used layer 5–7 protocols all support mutual authentication.

- Transport Layer Security (TLS): Client and server certificates
- Internet Protocol Security (IPsec): Internet Key Exchange (IKE)/Security Associations (SA)
- SSH (Secure Shell/Secure Socket Shell): Server identity keys (known hosts) and client SSH keys

Machine authentication. Machine authentication is used to authorize machine interactions on both wired and wireless networks, enabling computers and other machines to interact and exchange information autonomously.

The processes of machine authentication can be performed by simple devices such as sensors and meters in infrastructure and through verification of a digital certificate or digital credentials. Digital certificates used in machine authorization are like a form of digital passport providing trusted identification for the purpose of securely exchanging information over the internet. Digital credentials are much like forms of machine–provided ID and passwords.

Continuously monitor, assess, and enforce trust and risk for the duration of an interaction

Monitoring and assessing the levels of risk and trust during an entity's interaction with the network is very challenging. Organizations can start with a simple approach of defining a set of static rules that score an entity's risk/trust. For example, a device that is missing the latest software patches would have its score reduced. Similarly, a user who continuously fails to authenticate would have their trust score reduced. However, a set of statically–defined rules will not meet the goal of defending against evolving or unexpected attacks.

Organizations should use additional internal and external contextual factors related to user and device, including assessing the risk of the data, application, or transaction being accessed. For example, trust/risk should be based on an assessment of the identity of the user making the request (including their job status, role, etc.), the application or service the request is being made for, the sensitivity of the data being handled, and any associated tags or labels. In addition, approaches like CARTA advocate for continuously monitoring and assessing the levels of risk and trust during an interaction and after extending access, which make sense in today's highly dynamic environments.

Continuous monitoring should be data driven, with information coming from security and non–security sources. It should be acquired at different frequencies, using a mix of short– and long–term assessments to determine an entity's risk posture. As an example, an organization might use a combination of physical, electrical, and temporal data to monitor and assess the status of authorized and unauthorized access to various components on a network. The metrics should be refreshed at various frequencies, computed hourly, daily, or weekly in accordance with the monitoring strategy. External factors should also be considered, with organizations using continuously updated threat intelligence that feeds information about evolving and new threats into the risk/trust engine. This important, external data provides the context needed to understand whether or not to change the risk posture of an entity based on the known adversary tactics, techniques, and procedures (TTPs) of evolving or new campaigns.

Advanced tools such as ML can be used to score an entity's risk in near–real time. For example, ML can derive a risk score by calculating observable facts from a subset of training data which includes raw observations that have been associated with trusted or untrusted entities. Learning from this data, ML can identify and ultimately predict behaviors that are then used to derive a computer–generated risk scoring function. A model that has sufficient accuracy can then be used to predict the risk of yet unseen requests in the network.

Finally, the application metrics derived from access interactions should be sent to a data lake as part of a closed loop feedback mechanism. By continuously feeding this data back into the system and standardizing a list of user actions that are common for most applications, the system can map application usage to a particular user's normal usage pattern, thus aiding in anomaly detection through ML.

Examples of actions include:

- Successful authentication
- Unsuccessful authentication
- Create object
- Read object
- Update object
- Delete object

- Manage other users
- Reset password
- User logged out / time out (useful for establishing normal usage patterns)

Examples of identity include:

- Source IP address
- Unique application ID
- Device certificate (server and client)
- Username or user ID
- Common or domain specific user ID

While ML is increasingly used to solve difficult computational problems, it does not remove the need for more explicit rules in the trust engine. Currently machine–learning–derived scoring models are largely limited to advisory action. An enterprise would need to augment the ML results with a customized scoring function. Trust engines, therefore, should use a mixture of ad hoc and ML scoring methods together to most effectively score an entity's trust or risk.

With the benefit of multiple data inputs and automation and orchestration, security professionals can quickly support enforcement by quickly making adjustments to policy requirements or individual controls as needed. Automation also reduces the amount of time a human must spend monitoring and evaluating. For example, the AT&T CSO uses ML and automated monitoring technologies to improve decision–making and provide security–related insight that would not otherwise be available through manual assessment and analysis. This ultimately improves the efficacy of human action. These tools help to dynamically calculate trust and risk throughout the interaction. If the acceptable level of trust drops or the risk increases to a threshold requiring a response, then the access should adapt accordingly.

Benefits of Using ZT to Manage and Control Access

- Automation and orchestration decrease deployment errors, enable Agile development and continuous integration/continuous deployment (CI/CD), and create open source opportunities that increase flexibility and speed.
- Programmable networks make it possible to automate network infrastructure, move traffic via closed–loop mechanisms, and increase network visibility.
- A composite risk engine enables risk–based assessments, drives collaboration communications within the business (learn and share), and delivers trusted connection to endpoints (users, devices, and applications presented by a single entity).
- Web–based applications and services allow application and system developers to focus on their core work, move a company into a web–enabled environment, and create a better user experience.
- Closed–looped security with automation and orchestration decreases manual intervention, creates a learning system, and improves the ability of security teams to address zero–day vulnerabilities.
- Network and security teams realize an increase in operational efficiencies and the ability to address attacks and security issues more quickly.
- Strong, multi–factor authentication aligned with ZT supports granular, user–based access that makes use of precise controlling as needed.

Summary

Building a ZT–based program that supports strict yet dynamic management and control of access is a challenging transition in which development, networking, and security teams will need to align more tightly than they are accustomed to. For most, this journey will be iterative. More importantly, there is no one–size–fits–all model for ZT. Every organization has unique business drivers and risk tolerance, alongside industry nuances, that need to be considered. Also, a framework for access control will evolve along with changes in an organization's IT systems, new technology advancement, and changes in the threat landscape.

As enterprises embark on this journey, there are additional challenges to consider. How do we identify a device? (In many cases, this may require a custom solution on certain devices, as there is no solution that will work on every device an enterprise is managing.) How do we enforce and track actions? What percentage of our processes should be automated? How do we provide for accuracy in the decision engine? What is the process to quickly resolve false positives, i.e. an entity being denied access? And no doubt, as identity and access management technologies continue to mature, the models we use to frame our processes will continue to evolve as well.

One thing we know for sure is that network and security transformation, including the transformation of managing and controlling access to the network, is no longer a "nice to have." These things are now critical to enterprises being able to move users, data, and applications virtually seamlessly across the business while also protecting the business from the known and yet–to–be identified security threats of emerging technologies. Tools of the past, specifically IP addresses, are no longer effective in managing that control. Instead, organizations need to build dynamic access control that makes use of software–defined solutions for networking and security controls that give enterprises the ability to quickly react to threats, adjust infrastructure and access as needed, and reconfigure security policy to support business resiliency.

AT&T Cybersecurity

AT&T Cybersecurity helps to reduce the complexity and cost of fighting cybercrime. Together, the power of the AT&T network, our SaaS–based solutions with advanced technologies including virtualization and actionable threat intelligence from AT&T Alien Labs™ and the Open Threat Exchange™, and our relationship with more than 40 best–of–breed vendors, all accelerate your response to cybersecurity threats. Our experienced consultants and SOC analysts help manage your network transformation to reduce cybersecurity risk and overcome the skills gap. Our mission is to be your trusted advisor on your journey to cybersecurity resiliency, making it safer for your business to innovate.

cybersecurity.att.com

About AT&T Chief Security Office

The AT&T Chief Security Office (CSO) establishes policy and requirements, as well as comprehensive programs, to ensure security is incorporated into every facet of AT&T's computing and networking environments. Our technical personnel work in partnership with other AT&T Business Units and Divisions to evaluate threats, determine protective measures, create response capabilities, and ensure compliance with best security practices.

Contributing Authors

Richard Bowman, Rodney Dilts, Steve Sekiguchi, Karthik Swarnam, Sam Tittes, and Markus Weber

References

Balaouras, S., Cunningham, C., & Cerrato, P. (2017). Five Steps to a Zero Trust Network. Forrester.

Balaouras, S. & Shey, H. (2017). Defend Your Digital Business from Cyberattacks Using Forrester's Zero Trust Model. Forrester.

Center for Internet Security®. (2017). CIS Controls™ V. 7.1. Retrieved from https://learn.cisecurity.org/cis-controls-download

Cunningham, C., Balaouras, S., Cyr, M., & Dostie, P. (2019). The Zero Trust eXtended Ecosystems: Networks. Forrester.

Kindness, A. (2019). Decode the New Networking Alphabet Soup. Forrester.

MacDonald, N. (2018). Zero Trust Is an Initial Step on the Roadmap to CARTA. Gartner.

MacDonald, N., & Firstbrook, P. (2016). Designing an Adaptive Security Architecture for Protection From Advanced Attacks. Gartner.

MacDonald, N. & Gaehtgens, F. (2017). Use a CARTA Strategic Approach to Embrace Digital Business Opportunities in an Era of Advanced Threats. Gartner.

MacDonald, N. & Skorupa, J. (2109). Market Trends: How to Win as WAN Edge and Security Converge Into the Secure Access Service Edge. Gartner.

Three Reasons Service Providers Need Programmable Networks Today. Retrieved from https://www.cisco.com/c/m/en_us/network-intelligence/service-provider/digital-transformation/programmable-networks.html

*The point of view expressed in this report reflects the AT&T CSO's perspective on best practices for security architecture and operations. It does not necessarily reflect technologies used in or the current architecture of AT&T's network.

AT&T
Business