Prepared for

ELISITY

A Unified Architecture for Achieving Zero Trust Across all Network Domains

March 2021 EMA White Paper
By Shamus McGillicuddy

EMA
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Executive Summary

Network access and control is extremely siloed today. IT organizations use multiple technologies to manage and enforce policies. As enterprises pivot toward a zero trust security model, they will need to unify policy and enforcement across multiple technology domains. This white paper offers high-level guidance on how to get started.

The Trouble with Fragmented Trust

Most enterprises have a fragmented approach to network access policies and controls that can make any zero trust security initiative immensely complex. IT organizations should look for opportunities to unify zero trust networking with a solution that can apply policies and controls across domains.

Today's typical enterprise might have more than half a dozen solutions for managing trusted access on the network. For instance, many companies use software-defined networking (SDN) to segment workloads in the data center, a cloud-native networking solution for segmentation in the cloud, and traditional ACLs and VLANs in the corporate LAN and the Internet of Things (IoT) edge. Additionally, they might use a least-privileged access solution to manage the assets a user can connect to, a remote VPN solution for controlling network access for remote workers, and a software-defined WAN (SD-WAN) solution to control network access from branch offices.

This fragmentation can significantly undermine efforts to implement a consistent zero trust policy across all network domains. Each technology has its own policy engine, authentication mechanism, and access enforcement mechanism. Any effort to implement zero trust policies across multiple domains will require significant coordination across different technologies. In fact, 27% of zero trust networking projects are significantly undermined by a lack of integration across multiple zero trust solutions.[1] The same business requirements might drive policy design across all of these silos, so one policy engine would certainly be better than five or six.

Organizational fragmentation is also a major issue. Different groups in the technology organization will own different technologies. Security, network operations, cloud operations, DevOps, OT, application architects, and enterprise architects each have their own tools and technologies for implementing segmentation and access control within the domains they manage. Coordinating across these domains will require unprecedented levels of collaboration among groups that do not get along. For instance, 29% of zero trust networking initiatives are significantly undermined by conflicts between network teams and security teams.

[1] Unless otherwise noted, all data cited in this paper was originally published by EMA in the October 2020 research report, "Enterprise Zero Trust Networking Strategies: Secure Remote Access and Network Segmentation."

Moreover, edge devices are introducing more complexity and fragmentation. For instance, client devices usually have an associated user, so identity-based policy offers a foundation for establishing trust. However, most enterprises have thousands of operational technology (OT) and IoT devices connecting to their networks, and none of them has a user association. OT and IoT device policies are more likely to be tied to function, where access policy is defined as narrowly as possible.

With so many silos and fragmented solutions, it can be hard to know where to start with zero trust. In fact, 31% of zero trust projects are particularly challenged by project complexity. These individuals have told EMA that they don't know how to set their zero trust project priorities and scope.

How Enterprises are Unifying Trust for Edge Access

Move Away from Implicit Trust

Today, 42% of zero trust networking practitioners say it's critical for authentication and authorization to be based on multiple factors, not just identity. Identity is a critical component, but enterprises must go further by using context, environment, behavior, and more to establish trust. Identity should no longer be the linchpin of policy. For instance, after a user authenticates on a device, that device can be lost, stolen, infected, or otherwise compromised by malicious activity.

Furthermore, most enterprises are dealing with devices that have no user identity associated with them. EMA research found that 76% of enterprises have IoT devices connecting to their corporate networks today, and 47% of them were forced to invest in new authentication and access control technology to establish trust for those IoT devices.[2] Also, 44% of enterprises say access to IoT and OT is a major driver of their zero trust networking strategies.

In the early days of IoT, many enterprises managed trust by creating large IoT VLANs for all unmanaged devices. Unfortunately, today's enterprises need a more granular approach to trust. IoT and OT devices have specific assets that they should or should not be able to access. In a hospital, IP-connected security cameras and medical imaging systems with patient data must have different levels of trust. Remote access and administration requirements for these different classes of IoT assets demand granular segmentation and differentiated policy. Otherwise, a compromised IP camera could become a "jump box" that a malicious actor uses to access patient data that only a medical device should be able to connect to.

[2] EMA, "Network Management Megatrends 2020," April 2020.

Define and Manage a Unified Policy for Zero Trust Access

In recent years, EMA research found that IT organizations want access policy to be unified. In 2018, more than 40% of enterprises expressed interest in unifying secure remote access and SD-WAN management.[3] In conversations with EMA analysts, IT executives have expressed a need for a unified policy framework from the data center network out to the WAN edge, the cloud edge, and more.

From the top down, IT organizations need to look at how they can build a unified, multifactor policy model that can be applied to edge access control universally. The trust model should be based on what's important to one's business.

Zero trust policies should be able to consider location—whether a user, device, application, or data are inside a corporate site or connecting from elsewhere. They should also consider geo-segmentation, identifying regions and nations from which access should be disallowed or limited. Different locations should factor into what kinds of behaviors are acceptable. For instance, a CEO should have one level of access when connected the network from his corporate office, another level of access when connected from his home, and a third level of access when he's traveling.

The type of device and that device's role should also be a major component of zero trust policy. The role a device plays should influence what kind of trust is conferred. In a factory, HVAC controls, physical security systems, and manufacturing systems should all have different trust profiles. In a branch or campus, video conference systems should have different trust profiles than building automation and control systems, badge access systems, or third-party-managed multifunction printers.

Other factors that require continuous monitoring should also be considered. For instance, behavior can be used to refine trust policies. If a factory's HVAC system makes a suspicious communication request to access sensitive resources that only the manufacturing system should access, that HVAC system should be isolated from the network and SecOps should be alerted. Security state should also be monitored. The policy engine should review and monitor the state of antivirus and anti-malware systems and verify that the correct firmware version is installed on the device.

[3] EMA, "Enterprise Wide-Area Network Transformation," December 2018.

Continuously monitor the network and the behavior of edge devices

Forty-four percent of zero trust networking practitioners say they must continuously monitor the network to optimize access policies, and 56% say it is critical that zero trust access controls be able to challenge users and devices to reauthenticate, based on observed behavior and other changes in policy.

Thus, any zero trust system must have a monitoring capability. Monitoring should be integrated into the zero trust platform. Authentication requests, traffic flows, changes in network state, threat feeds, and more can all play a role in policy decisions. In fact, 98% of zero trust networking initiatives have or plan to have a dynamic policy engine that can evolve based on new business conditions and observed activity. EMA's research has found that successful zero trust networking initiatives are more likely to have a dynamic policy engine in place that can respond to changes in the network.

However, a zero trust platform should have analytics in place to respond to indicators of change. This will enable a system to challenge reauthentication if something suspicious happens. The smarter a platform is with monitoring data, the better the trust model will work.

Move Toward a Unified Zero Trust Data Plane

Enterprises are investigating a wide variety of technologies for implementing zero trust. For remote access control, they are considering legacy VPNs, secure access service edge (SASE), and software-defined perimeters. On the segmentation side, they're looking at legacy VLANs and ACLs, host-based or hypervisor-based segmentation, and appliance-based solutions.

EMA recommends that enterprises look for ways to unify their zero trust data planes, much as they need to unify their policy and control. This may require an overlay topology that works everywhere. One must look for ways to unify how one enforces policy on the data plane, from the remote edge to the data center. Companies must break down silos by choosing a solution that covers as many use cases and as many aspects of the business as possible.

If there are gaps that can't be filled with a unified solution, enterprises need to integrate. For instance, 49% of enterprises say it's critical to integrate remote access control and network segmentation.

EMA Perspective

Network access and segmentation technologies are too fragmented within today's enterprises. Multiple groups are involved in edge access, and they use siloed technologies for policy and enforcement.

When embarking on a zero trust initiative, the IT organization should unify technology and create a cross-domain approach to edge access. This will require a reduced reliance on identity for conferring trust, a unified policy model that can be tailored to the unique needs of a business, a dynamic policy engine that monitors the network and responds to observed activity, and a unified enforcement architecture.

About Elisity

Elisity is solving the challenge of securing access to enterprise assets and enterprise data in the complex modern world of blurring enterprise boundaries, the proliferation of cloud, connected devices, and mobile workforces. Elisity provides unified policy and identity-based access solutions powered by AI. The Elisity team is made up of experienced entrepreneurs with deep technical backgrounds in enterprise networking and security with the world's largest and most security-conscious organizations.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at **www.enterprisemanagement.com** You can also follow EMA on **Twitter** or **LinkedIn**

1995 North 57th Court, Suite 120, Boulder, CO 80301 +1 303.543.9500 **www.enterprisemanagement.com** 4079.033121