www.pipelinepub.com
Volume 20, Issue 7

Securing Today's Automated Enterprise

By: Srini Addepalli

The rapid adoption of automation and interconnected systems has transformed modern enterprises, offering efficiency and improved functionality. However, these advancements also introduce unique security challenges. This article explores the complex landscape, highlighting the increased attack surface and potential vulnerabilities in automated and interconnected environments. It then identifies the key characteristics of a comprehensive security solution for these interconnected systems, and highlights critical features and benefits organizations should consider when selecting a security approach for their evolving automated landscape.

The Security Challenges of Automation and Interconnected Systems

Automation and interconnection mean the use of technologies such as artificial intelligence, machine learning, cloud computing, internet of things, and edge computing to streamline processes, connect systems, and share data across different domains and platforms.

Communicating systems can be software entities such as micro services or hardware entities such as IoT devices. These communication systems can be housed in data centers or distributed over multiple geographic locations in Edges, Clouds, data centers, IoT networks, and others. Automation typically involves workflows where one system output is passed to another system for its processing. That is, an input to the front-end system can initiate chain of events (data flows) across multiple systems, which are possibly scattered across multiple locations, domains, and environments.

Communication systems can include containers, VMs, bare-metal services, public cloud services like IoT platforms, SaaS services, IoT devices, or third-party services. With various environments such as hypervisors, Kubernetes, serverless platforms, AI and ML platforms, or GenAI frameworks, any poor security configuration of hosting environments can affect both the performance and security of the automation systems.

Some components may not have the latest and safest software installed. For example, IoT systems may not be able to update software at all. This means that they need to be protected by security systems that restrict their access to only approved connections.

When human users interact with a front-end system, they must authenticate themselves on a demand basis and the system learns their identity. For services, there are different types of identities to be taken into account for any varied access controls. Identities and related credentials include certificates, API-keys, and JWTs with long lifetime. If credentials are compromised, attackers can move sideways more easily.

This means that while automation among connected systems helps businesses improve their operations, increases their efficiency, and helps them gain an advantage over rivals, it also creates serious security challenges.

Automation and interconnection increase the amount and diversity of devices, systems, and networks that cyberattacks can target. For example, a single hacked IoT device can endanger the whole network or enable access to confidential data in the cloud. Attackers also can use advanced and persistent threats to penetrate and control the processes of automated systems.

Automation and interconnection also create a diverse and dynamic environment that is difficult to monitor, manage, and secure. For example, different devices and systems may have different security protocols, standards, hosting environments and configurations, creating inconsistencies and gaps in the security posture.

Once they have breached an organization's network by exploiting the front-end system or even compromised third-party systems that share the same network as automated systems, malicious cyber actors often move laterally through the network, accessing more confidential data and vital systems.

Zero-Trust Architecture is Important

Traditional network security has relied on a layered strategy for defense; however, most enterprises mainly invest in protecting the network with perimeter security. When network users or components access the network from inside the boundary, they often have broad access to various corporate resources. If network users or components are compromised, bad actors can access resources from within the network. Since automated systems can perform actions in an automated way involving multiple interconnected systems, it’s important to ensure that security is built with a zero-trust mindset. Zero-trust security requires the following to address the security challenges comprehensively:

You must verify and authenticate the client systems or users, continuously monitor the user activity patterns in granting or rejecting accesses to destination services. Minimal access (or granular access) is another part of zero-trust ensuring that only required resources are accessible to the client systems based on their identity. Security posture collection of client or server system and the use of this information in making decisions to permit access to resources is another part of the zero-trust method of minimizing risks of lateral attacks. Security posture includes the health and patch status of both the client system and the environment it’s hosted on.

Data security posture and data protections are also essential to ensure that the data used by automation systems is not altered or exposed to malicious actors. Zero-trust of automation systems should include data protection such as encryption, backup for recovery in case of ransomware attacks, and data security posture such as malware detection on the files and folders.

Network segmentation is also a key part of zero-trust, especially in cases where the identity of systems can't be determined. It's advisable to isolate these systems in various network segments to provide segment specific access controls.

Finally, the ability to visualize all traffic flows, including data, analytics, anomaly detections, performance monitoring, threat hunting, and other observables is important to identify and isolate any threats.

Network Security Solution: SASE *and* Service Mesh

Networks are responsible for all the traffic between the systems that are connected. So, network level security plays an important role in safeguarding automation systems. SASE and service mesh technologies can help with securing the systems at the network level. Although other security components, such as Data Security Posture Management and Data Protections and Cloud security such as CNAPP are also important, this section only focuses on network security.

SASE and service mesh technologies are both ways to implement zero-trust security architecture at the network level. They can work together to protect automation systems from network security threats.

Zero-trust security needs a common set of features that SASE and service mesh have in common. Both authenticate the client users or services, obtain identity of the user initiating the traffic sessions, and apply identity aware access control to regulate the accesses. Both use modern authentication protocols and mechanisms such as OAUTH2, OIDC, and SAML-based authentication with MFA. They also authenticate services using client certificates, JWT, and API keys. Both provide granular access controls using various traffic parameters, including URLs, Paths, Query Parameters, Request Headers and many more. Both also integrate with posture management systems to ascertain the security posture of client and server services and use that information in access governance.

SASE and service mesh technologies can also accomplish threat detection and prevention using IDPS, malware detection using Anti-Malware technology, data loss prevention using DLP technology, and data security of the traffic going to cloud and SaaS Services. SASE also prevents the sessions to known bad sites by continuously collecting threat intelligence of external services. SASE does this by having NGFW (Next Generation Firewall), SWG (Secure Web Gateway), ZTNA (Zero-Trust Network Access), CASB (Cloud Access Security Broker), Anti-Malware, and DLP (Data Loss Prevention) functions to effectively identify threats and protect resources. SASE also utilizes WAAP (Web Application and API protection) technology to stop any API based threats.

SASE also offers network segmentation to divide the networks and secure the boundaries to prevent lateral attacks from spreading.

Furthermore, both SASE and service mesh technologies offer complete management and observability with AI, ML, and GenAI capabilities that help in analyzing flows across systems, detecting any anomalies, creating comprehensive reports, and providing closed loop automation to generate policies to block further attacks.

Even though both of them offer zero-trust security, their deployments are different. SASE is usually provided as a cloud service, more suitable for protecting communicating services that use WAN. SASE solutions are increasingly being deployed on-prem to secure services that go across different networks within data centers. Service mesh technologies are used to secure services within a Kubernetes cluster. Service mesh attaches the sidecar proxies to each microservice and controls the security functions from a central location. Due to these differences, both SASE and service mesh technologies are needed to provide comprehensive network security. Since internal technologies are similar, SASE providers will eventually provide deployment of security as service mesh technology vendors do today.

Conclusion

Automation is transforming how enterprises operate, providing more effectiveness and better functionality. But they also introduce new security challenges, such as larger attack areas, horizontal attack movements, attack diversity and complexity, and advanced and persistent attacks. To handle these challenges, enterprises need a complete and adaptable zero-trust security solution that can offer visibility and awareness, control and enforcement, and intelligence and automation for the entire automated and interconnected environment. SASE and service mesh are two networking technologies that can help in achieving zero-trust security needed by automation systems. By using a combined solution, enterprises can reduce risk and cost, increase effectiveness and productivity, and enhance innovation and competitiveness.