# Cisco Identity Services Engine (ISE)

## Visibility-Driven Segmentation

## Control access and contain threats within zones of trust

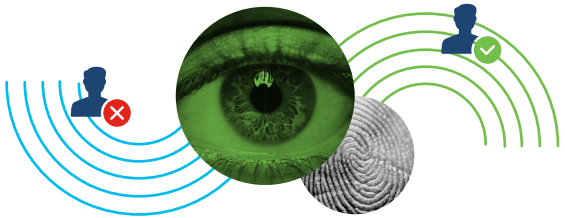
**You wake up to find out that another security incident has occurred. You're confused, and not sure how the attacker was able to get by your perimeter. But then you realize that you haven't had a perimeter for some time, as it has been pulled apart by cloud, mobility, and Internet of Things (IOT).**

Zero trust is a security concept that solves this dilemma by continually authorizing access, regardless of device location, and building "trust zones" to dynamic control policy enforcement. Segmenting the network into segmented zones of access has been an accepted practice in ensuring policies are adhered to and also to reduce risk. But this has rarely moved beyond practice, leaving organizations with partial network segmentation and partial protection.

Why? Because it has been slow to implement and impossible to continually ensure that the intent of the business is met and maintained as networks change. A main barrier to network segmentation has been a lack of visibility into the identity of devices, how they interact with each other, and ensuring that policies don't cause reachability issues that shut down critical business needs.

## Benefits

- **Boost productivity** by simplifying and automating policy enforcement
- **Increase flexibility** using automated device identity and classification to control access
- **Respond quickly** to threats and automat threat containment
- **Reduce** the attack surface within trusted zones of access



## Network segmentation to enable business outcomes

Cisco Identity Services Engine (ISE) overcomes these challenges and provides visibility-driven segmentation to extend zero trust in the workplace. With ISE you can control access and limit the lateral movement of threats, all while simplifying bring your own device (BYOD) and guest access. We build network segmentation and automate policy enforcement directly into the network, shutting down access closest to the resource to turn your network into the enforcer.

This is accomplished without the manual configuration complexity seen in legacy approaches that are tough to deploy, with a lengthy manual process, and near impossible to continually verify. With visibility-driven network segmentation in place, organizations are able to shrink the attack surface, limit the spread of malware, and enable rapid threat containment all while continually ensuring that this level of protection will not disrupt business outcomes.

**Network segmentation is within reach. Visit our webpage to learn how ISE can enable your network segmentation initiatives and read ESG's whitepaper, Removing Complexities Around Network Segmentation, to gain further insights into how you can simplify and embrace network segmentation.**

> "If you're searching for the best solution in the enterprise market in terms of security, access control granularity, and posture, then you need to have ISE [Identity Services Engine]!"
>
> Matteo Da Pozzo, senior network security consultant, Communication Valley Reply

Learn more at www.cisco.com/go/ise