It's a world of unnecessary complexity an intricate maze of twists and turns, and that is certainly true of today's enterprise networks with more and more demands on the infrastructure an increased attack surface and the need to fulfill security requirements for regulatory compliance security. Rules have become increasingly complex and though the wider use of virtualization mobile devices and more networked applications and users has opened up a host of opportunities to improve productivity. It has also led to complications and making sure the right people have access to the right resources while restricting the wrong people simply put with all these changes. It's become more complex to handle change scale and stay secure so much that when simple tasks such as security policy adjustments need to be made it leads to volumes of difficult to manage rules that segment traffic and servers inefficiently by their IP addresses, VLANs or subnets that are hard to map to security and business needs. This makes it hard to track and prevent unauthorized access and usage across the network policy changes that result in challenging are-architecture of the network and managing, what are now tons of IP based firewall rules and access control lists the remedy software-defined segmentation using Cisco trust. SiC technology already embedded in Cisco routers switches wireless devices and security technology like firewalls and even partner solutions it enables network segmentation and enforces security policies that map to business. Policy usage it groups business objectives into simple security groups as an example based on role or application versus mapping devices to IP addresses and it simplifies firewall rules and large volumes of access control lists leading to easier management and faster provisioning. It can also extend security by enforcing access policies across the extended Network for example when malware piggybacks on an authorized users connection trust SEC can restrict unauthorized lateral movement by enforcing appropriate business usage policies in addition because trust SEC works with Cisco identity services engine also known as ice the market-leading network access control policy platform. It further reduces complexity by simplifying policy management and providing enhanced context and visibility into connected users and devices an adaptable scalable network it's more than within Reachit's possible to leverage your network to provide better security. Cisco trust Sec is a key component of Cisco's threat centric security solutions for addressing the entire attack continuum before during and after by aligning business usage with security access policies controlling access to resources via segmentation and limiting the movement and impact of threats.