Cisco Identity Services Engine (ISE)

Automated Threat Containment

Don’t just block the threat, remove it

Imagine a burglar has broken into your house. As they approach your bedroom door, it slams shut, protecting you within. But this threat is still free to move throughout your house. Would you feel safe? Of course not! You would want them out of your home. But when protecting our networks, we often do just this. We detect, then block, but we do not remove the threat.

But what if your visibility and analytics solutions had an active arm of protection, shutting down access at the network device closest to the resource they are trying to connect to? What if detect and respond were one, breaking down the operational silo that malicious hackers are exploiting?

This is Rapid Threat Containment within Cisco ISE (Identity Services Engine). ISE breaks the silo between visibility and control. Teams are no longer swiveling from detection to remediation and are now automating their response to limit or remove access of a suspected endpoint, stopping the spread of highly impactful malware.

Benefits

- **Unify** visibility, detection, and enforcement
- **Reduce** mean time to repair of security incidents and breaches
- **Overcome** complexity within siloed security solutions
- **Accelerate** incident response with automated detection and containment
- **Increase return on investment (ROI)** on existing solutions, without added complexity

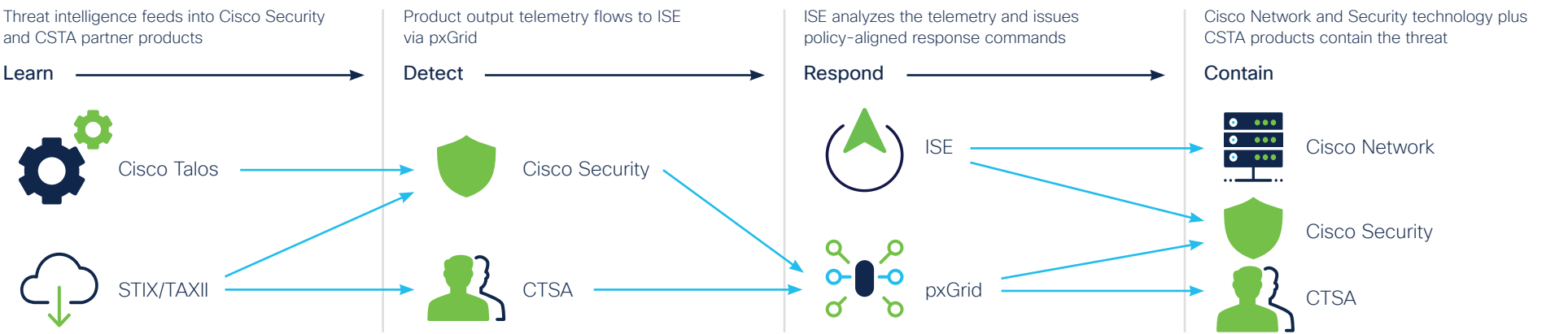
Integration is the key to automated threat containment

Integration between multiple solutions within a platform approach automates threat containment and removes complexity to save organizational resources, all while preventing security incidents from turning into breaches. But we have to do more than give customers an API. We need to look at validating solutions and simplify the workflow so customers can deploy advanced use cases to increase an organization's overall security posture.

ISE gains visibility and context from security intelligence and analytics solutions such as Cisco Stealthwatch® and third-party vendors, whether on-premises or in the cloud with our open and standard-based pxGrid and pxCloud* ecosystem. A unification of visibility and control results in automating threat containment to limit or remove access based on organizational risk tolerances. Suspected endpoints no longer remain in the network, moving laterally, infecting other endpoints, and causing havoc.

Integration with Cisco SecureX* brings an added layer of orchestration and automation. It allows for a true platform approach with multiple intelligence streams and workflows brought into a single view to unify visibility and control. The results are tremendous, with a drastic reduction of mean time to repair (MTTR) and increased ROI from existing solutions without any added complexity.

How Rapid Threat Containment Works



*Feature planned for release in the first half of CY 2020. Please contact sales for early access.

> “Cisco ISE integrates and shares information with the security portfolio enabling the frontline to make and informed decision on an asset. ISE can also be used as an automation point to quickly remediate a breach.”
>
> Ryan Bermel, Director of Security Solutions, 5thColumn

Take a look at Dynamic Visibility and Visibility-Driven Segmentation to learn about two key use cases provided by ISE to make Automated TC-NAC possible.

Learn more about ISE, please visit

www.cisco.com/go/ise

2163516 04/27