



# Cisco Identity Services Engine

## Rapid Threat Containment

### Scrambling to react when you're under attack? We've got your back.

Fast cyber threat detection. The latest, standards-based threat intelligence. Automated, consistent responses. All of these are incredibly important in cybersecurity today, but there's more: The need for effective coordination among security staff, policies, processes and technologies. It all has to work together as a team. Does yours?

Though much progress has been made over the years, attackers still find ways to succeed. Then their success encourages new attacks, as attackers know that even the best defensive technology can be penetrated. They know about gaps between different technologies, and how responders can be overwhelmed with volumes of data that require thoughtful interpretation, insight, and ultimately a sound response decision.

Any defender hampered by uncoordinated technology, too many inconsistent interfaces, too few working integrations, and too much manual effort is simply outgunned. Worse, when pressured to act quickly, the stress takes its toll: Rushed-judgment, mistakes, or flat-out incorrect action. Burn-out isn't uncommon either.

If this sounds familiar, then imagine this: What if you had a simple, standards-based, bi-directional integration platform? One that would gather security telemetry and intelligence from products you already have, and bolster that data with standards-based threat feeds? It would include a growing alliance of technology partners, and an industry leader would test, validate and support everything. Wouldn't that be great?

It is. And it's already here. We call it Rapid Threat Containment, and it's only from Cisco.

### What do you gain with Rapid Threat Containment?



**Respond immediately.** Your network can automatically contain cyber threats, limit access, and remove devices as threat scores worsen.



**Improve operational quality.** Act correctly and confidently because we test, validate and support the product integrations.



**Reduce implementation complexity.** Our standards-based integration approach means less hassle and troubleshooting your team.



**Retain your cyber experts.** They don't enjoy manual work or making mistakes during high-pressure cyberattacks. Keep burnout at bay and they'll stay.

## With Cisco ISE, you can:



Grant and control the right level of network access



Improve your security posture and quickly contain breaches



Gain complete endpoint visibility with context



Streamline your access control policy management

## Licensing

Rapid Threat Containment use a combination of **Base**, **Plus**, and **Apex** licenses depending upon how you choose to integrate technologies and use them for intelligence and response automation.

Check out the [Cisco ISE Ordering Guide](#) for complete details.

## Learn More

To learn more, please visit <https://www.cisco.com/go/ise> or contact your account representative.

## Rapid Threat Containment, powered by Cisco ISE, delivers the automation you need

Cisco Identity Services Engine (ISE) is founded on the following innovations that discover and stop threats automatically:

- Cisco Platform Exchange Grid (pxGrid). This open, scalable, IETF standards-driven platform interconnects your Cisco and third-party security products for cross-product insight, input telemetry, and automated response actions.
- Network segmentation and enforcement. Intent-based network segmentation works through ISE and pxGrid to enable your network to be a threat container through built-in, adaptive segmentation policy. And with Cisco Stealthwatch and Firepower Management Center (FMC) it gathers their security intelligence, takes into account input from integrated Cisco Technology Partner products, and automatically drives the right containment commands back to FMC and ecosystem partner solutions.
- Cisco Technology Partners. The Cisco Security Technology Alliance (CSTA) is a security vendor ecosystem for open, multivendor product integrations for telemetry and intelligence input, and response command output. We fully test, validate, and support these integrations for accuracy and reliability
- Standards-based threat intelligence. ISE also supports the Common Vulnerability Scoring System (CVSS) and Structured Threat Information Expression (STIX) threat classification standards to make risk-informed access restrictions.

Ready to stop scrambling and improve your security operations?  
Learn more about [Cisco Rapid Threat Containment](#) today.

