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.
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.

How Rapid Threat Containment Works

1. Threat intelligence feeds into Cisco Security and CSTA partner products.
2. Product output telemetry flows to ISE via pxGrid.
3. ISE analyzes the telemetry and issues policy-aligned response commands.
4. Cisco Network and Security technology plus CSTA products contain the threat.