

Defending Cisco: Our Computer Security Incident Response Team (CSIRT)

Our story to trust starts with protecting our own expansive global network.

Cybersecurity breaches can cost millions of dollars and inflict massive reputational damage. Cisco's Computer Security Incident Response Team (CSIRT) detects and responds to threats to our business operations at every touchpoint, making sure customers can safely access our solutions and services 24/7.



Costs of security failure

CSIRT works to prevent losses caused by unplanned expenses and reputational damage. Long-term brand damage especially can lead to significant annual revenue loss.¹

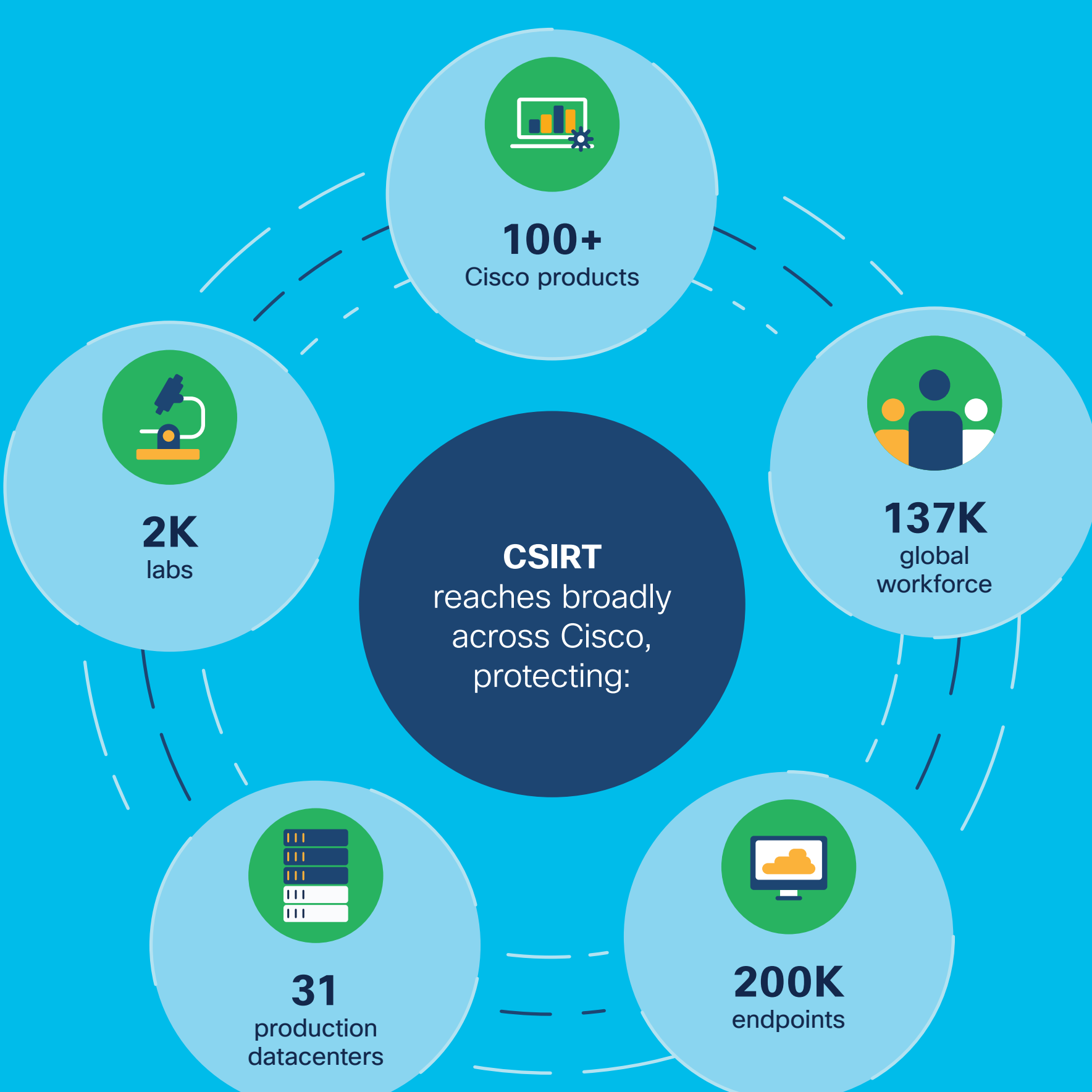


An integrated approach

CSIRT partners with various groups across the enterprise, including Security Operations, IT, and Cisco business leadership to mitigate cybersecurity threats across the entire organization. This teamed approach allows us not only to identify threats as they occur, but also prevent future breaches through trend analysis and ongoing development of new tools and architectures.



Our touchpoints



How we do it

Threat detection at the scale of the Cisco enterprise requires the scale of Cisco's integrated portfolio. CSIRT leverages dozens of Cisco industry tools and solutions to provide multiple layers of visibility and defense.



Big data, big reach

Cisco tools and solutions generate vast amounts of data. CSIRT manages this big data through a programmatic response, examining what threats are being targeted, how to detect them in real time, and how to respond most effectively.

