cisco SECURE

cisco The bridge to possible

Cisco Secure DDoS Edge Protection

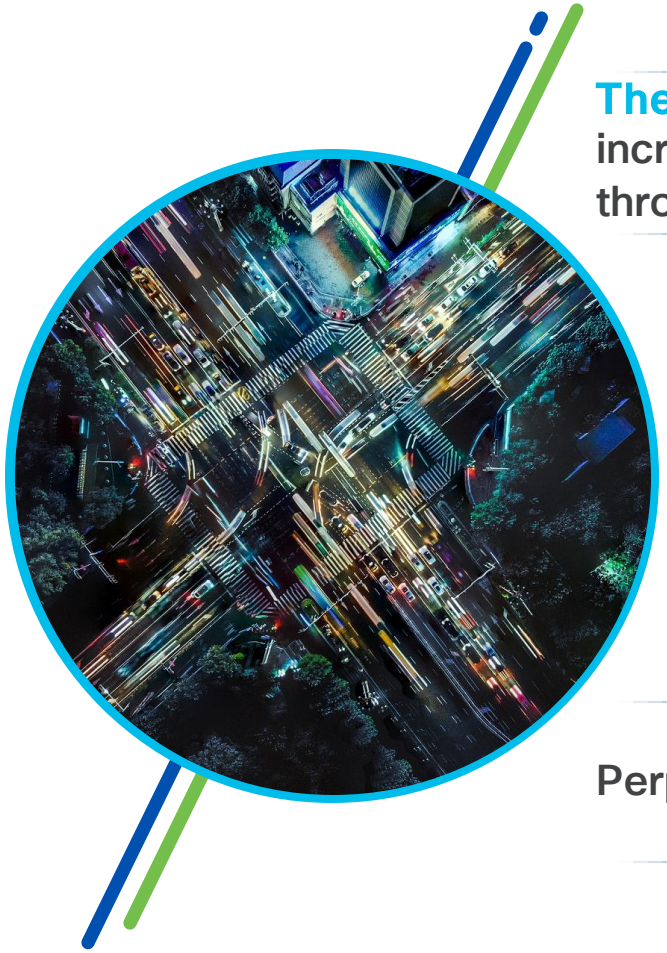
Use Your Routers as the First Line of Defense Against DDoS Attacks

July 27, 2023

Agenda

- Why there is a need to rethink DDoS protection
- Our approach to transforming DDoS defenses
- Seeing the solution in action
- Panel discussion

DDoS attacks have never posed a greater threat than now



The number of DDoS attacks is growing faster than Internet traffic: attacks increased by 150% in 2022[1] and are expected to reach over 15.4 million through 2023[2], while Internet traffic is growing at a CAGR of 30%[3].

Communication service providers are not only **the target of DDoS attacks** themselves, but also **conduits for attacks on other networks**.

The growth of more **distributed and edge networks** combined with the **proliferation of connected devices** increases opportunities for DDoS attacks.

Perpetrators use increasingly **sophisticated methods** to cripple networks.

Sources – 1: Radware | 2: Cisco | 3: Telegeography

DDoS attacks can have a long-lasting negative impact on your business

Direct financial impact

- Service disruptions can lead to lost revenues.
- Missed SLAs can result in penalties.
- Cybercriminals use DDoS for extortion.

Customer churn

- Poor quality of experience encourages customers to move to competition.

Brand damage

- Negative publicity can cause reputational damage.
- A tarnished brand reduces shareholder confidence.

Fines

- Regulators can impose hefty fines on organizations with inadequate security measures.

Boosting DDoS defenses with traditional solutions is challenging

- Scaling traditional DDoS defense across **more distributed networks**, carrying exponentially growing volumes of traffic, is cost prohibitive.
- Traditional DDoS defense negatively impacts the performance of **low-latency applications** on the edge.
- Protecting networks is becoming increasingly difficult due to the **dynamic, multi-vector nature** of today's threats.

Transform DDoS defenses for your distributed networks with Cisco Secure DDoS Edge Protection

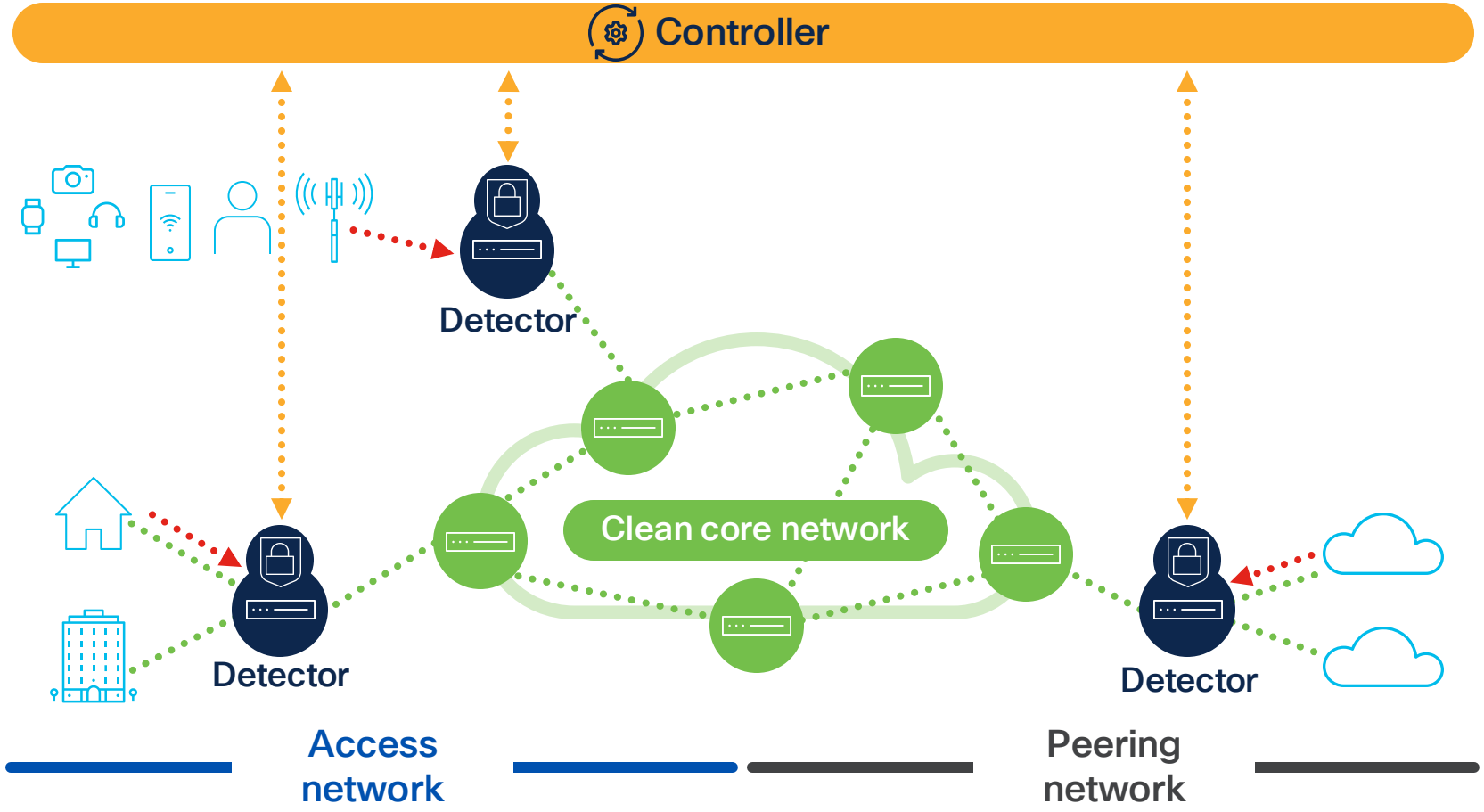
Keep attack traffic off your network by using your routers as the first line of defense

Use your routers as the first line of defense against DDoS attacks

Real-time on-box autonomous attack detection and mitigation	Protects quality of experience and the performance of low-latency applications
Software that requires no additional equipment, rack space, power, or cooling	Makes the solution cost-effective and scalable
Unsupervised machine learning algorithms	Ensures the flow of legitimate traffic while preventing malicious traffic from flooding the network
Automation, zero touch, and a central interface management function	Offers both ease of management and complete control

Scale your DDoS capabilities simply and cost-effectively as you scale your networks

Cisco Secure DDoS Edge Protection detects and mitigates DDoS attacks on your routers in real-time



Detectors

Containers that run on IOS XR routers

- Act as a **distributed defense system** for hyperscale networks at the edge
- Collect telemetry and use autonomous machine learning to detect attacks
- Address attacks by pushing access control list updates for mitigation

Controller

Management of up to 60,000 detectors

- Receives alerts from all routers' detectors to **scale defenses network-wide** when an attack occurs
- Offers information about **real-time and historical attack forensics** to support threat intelligence analyses
- Supports both manual decision-making and letting the system mitigate attacks automatically
- UI for solution operations and APIs for integration with other systems

Real-time on-box autonomous attack detection and mitigation

Protects the performance of low-latency applications and quality of experience

Real-time on-box autonomous attack detection and mitigation

A router is equipped with a detector – a containerized application that **detects and mitigates attacks on-box at line rate**, with zero impact on the throughput performance of the router.

The detector uses patented algorithms and information received from the router's hardware to **characterize attacks**, including those in tunneled traffic (GTP), and generates an **alert to the controller** when it identifies an attack.

Thanks to optimized system interaction with the centralized controller that can manage a fleet of tens of thousands of detectors, **spotting anomalies across distributed networks** is highly efficient and effective.

Software that requires no additional equipment, rack space, power, or cooling

Makes the solution cost-effective and scalable

Software that requires no additional equipment, rack space, power, or cooling

Detectors can be deployed in **every router in the network**, offering a distributed defense system for hyperscale networks at the edge.

The solution leverages IOS XR to **deliver telemetry five times more efficiently than traditional solutions**, aggregating data from edge devices.

The centralized controller receives reports from all routers' detectors to **scale defenses when an attack occurs** and deliver network-wide visibility, detector fleet control, and attack lifecycle management.

DDoS defense delivered at over **80% lower cost** compared to traditional solutions* with an opportunity to apply these savings to further expand DDoS defense coverage.

** based on an illustrative analysis to cover 900 access aggregation sites with Cisco Secure DDoS Edge Protection*

Unsupervised machine learning algorithms

Ensures the flow of legitimate traffic while preventing malicious traffic from flooding the network

Unsupervised machine learning algorithms

The solution uses advanced spatial analysis to provide **granular detection of known and zero-day attacks**.

Once it spots a threat, its unsupervised learning algorithm **compares the parameters of suspected attack traffic with those of normal traffic**, while characterizing the attack vector, source and destination of the malicious traffic.

The solution ensures that **only attacking traffic is blocked**. Legitimate traffic is able to pass through the router during an attack, protecting quality of experience for end users.

Automation, zero touch, and a central interface management function

Offers ease of management with complete control

Automation, zero touch, and a central interface management function

A centralized controller manages a fleet of **up to 60,000 detectors**, configuring their profiles and security settings.

Using information from detectors, the controller **characterizes threats in real-time** and adapts to threats during an attack, **updating the mitigation** if attack vectors change.

The controller offers information about **real-time attack forensics and threat intelligence analyses** and provides real-time and historical reporting of incidents.

The controller is fully **automated and autonomous while allowing manual intervention.** This makes mitigation faster and optimizes the use of security resources and expertise.

Use cases of Cisco Secure DDOS Edge Protection

Mobile access

Protect the performance of low-latency applications

The challenge

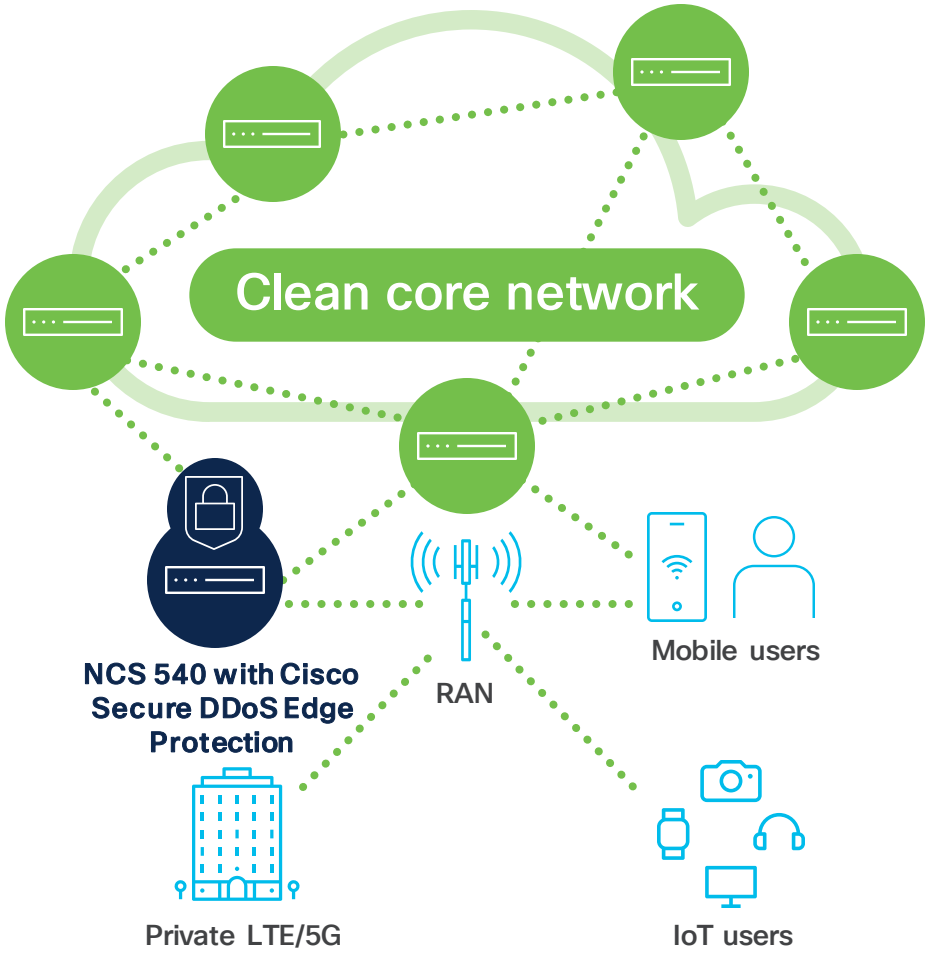
- The proliferation of mobile and IoT devices creates new opportunities for cyber criminals to launch DDoS attacks.
- Traditional DDoS solutions can only detect attacks once the traffic exits the encrypted GTP-U tunnel – when it is too late.
- Backhauling mobile and IoT traffic to scrubbing centers is expensive and negatively impacts the performance of low-latency applications on the edge.

How our solution addresses it

- Sees inside the GTP tunnel and detects and mitigates DDoS attacks at the earliest opportunity.
- Protects the network from attacks originating from end-user equipment.
- Eliminates the need for traffic gating at UPF and scrubbing.

The outcome

- Complementing traditional DDoS solutions with Cisco Secure DDoS Edge Protection helps ensure the performance of low-latency mobile and IoT applications (sub-10-ms).



cisco SECURE

Peering

Ensure the availability of services despite constantly evolving threats

The challenge

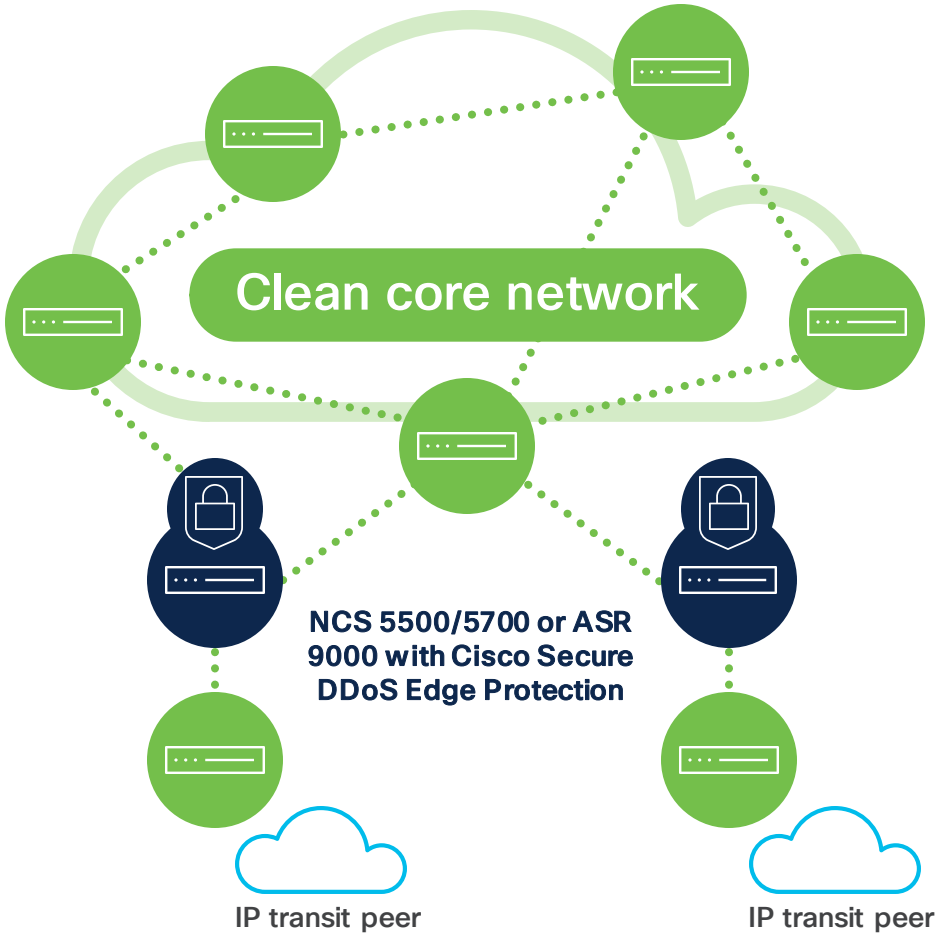
- Protecting peering against DDoS attacks is complex because of the volume of traffic handled by peering nodes and the range of protocols that perpetrators can exploit to target different services.
- Current approaches using static misuse lists are unable to identify zero-day attacks and protect the network against constantly evolving threats.
- Growing node traffic volumes make traditional DDoS solutions cost-prohibitive.

How our solution addresses it

- Gives full visibility over threats by characterizing attacks in real-time.
- Dynamically adapts the mitigation as attack vectors change.
- Offers scalable and cost-effective protection for peering by tackling threats at the edge of the network.

The outcome

- Protects peering from attacks and ensures the availability of services, as the volume of traffic handled by peering nodes grows and new threats emerge.



Broadband

Improve customer retention by ensuring quality of experience and protect the network

The challenge

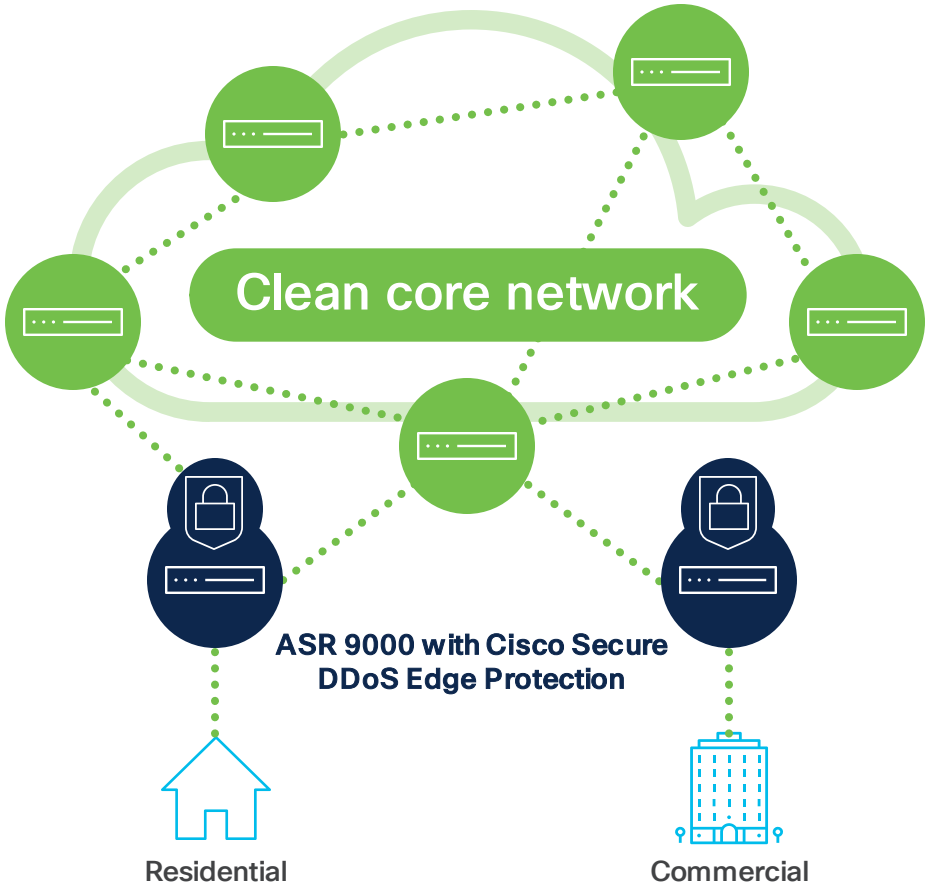
- New super-fast fiber-to-the-home networks increase opportunities for perpetrators to exploit high-bandwidth CPE and different end-user devices.
- The development of more distributed broadband architectures increases the risks of DDoS attacks using local internet break-outs.
- Users expect flawless connectivity for gaming, content streaming and collaboration, so quality of experience is critical for customer retention and a competitive differentiator.

How our solution addresses it

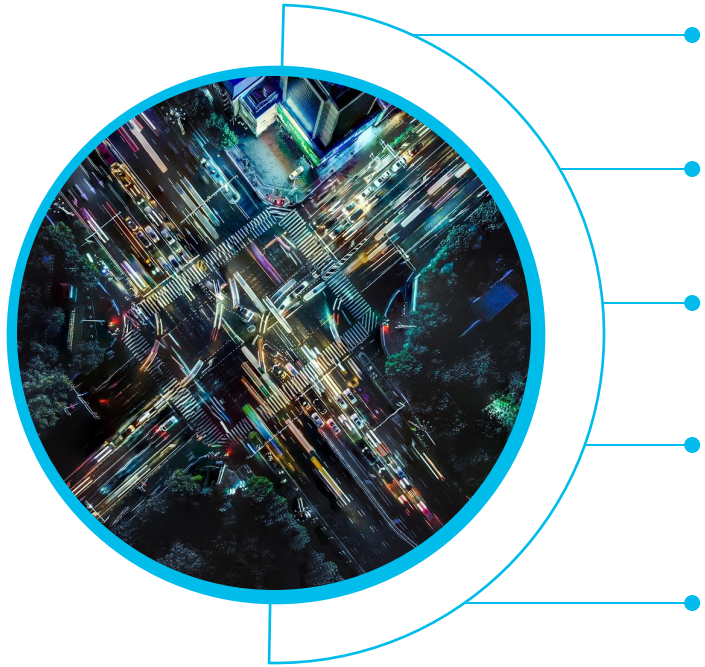
- Characterizes attacks emerging at Internet breakouts in real-time, and dynamically adapts the mitigation as attack vectors change.
- Mitigates attacks aimed leveraging CPE and end-user devices close to the source and prevents threats from spreading into the rest of the network.

The outcome

- Ensure flawless experience for residential and business customers and prevent attrition, as services at the edge become more important and broadband networks continue to grow at breakneck speed.



What sets Cisco Secure DDoS Edge Protection apart



- True on-box DDoS protection: **a world first**
- DDoS protection efficacy: **99.49%**
- Time to attack mitigation: **less than 10 seconds**
- Validated number of multi-vector attacks: **500**
- **20** years of DDoS defense experience combined with Cisco's unparalleled routing expertise

Seeing the solution in action

Panel Discussion

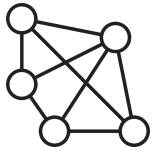
- Erich Pletsch, Sr. manager, business development
- Mike Geller, Distinguished architect
- Jim Cubbage, Product manager, security
- Nitin Singla, Lead product manager, security and provider connectivity
- Michel Brouns, Go-to-market lead, new service provider offers

To wrap up...

Transform DDoS defenses with Cisco Secure DDoS Edge Protection

Real time on-box autonomous zero-day and known attack detection and mitigation with 99.49% efficacy and less than 10 seconds to attack mitigation

Cost-effective and scalable with no need for additional equipment, power or cooling – supporting your sustainability goals



Pervasive protection across mobile access, peering nodes, and broadband networks

Experience the solution with a demonstration and lab test

cisco SECURE


cisco SECURE