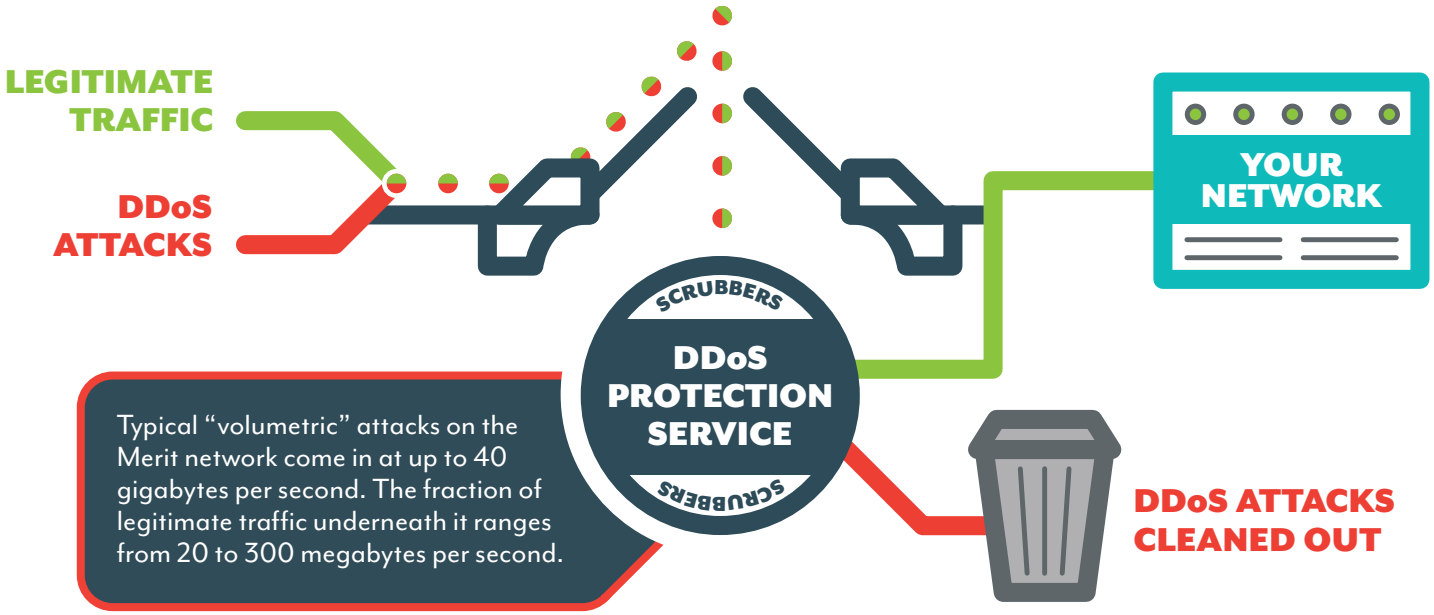
POISE UNDER PRESSURE

We'll Make Sure You're Not Blindsided by an Attack



DDoS ATTACKS STRIKE DAILY

A successful attack causes embarrassing downtime, incurs costs and damages reputations. Even more frightening, DDoS services are available on the dark web. And they're cheap. For public organizations shouldering high expectations of accountability, this is an unacceptable level of risk.

Merit Network's DDoS Protection Service ensures you are prepared in the face of a threat. That's because the Merit Support Center watches your perimeter for you. The instant a threat is detected, the drawbridge is raised. Traffic is rerouted to "scrubbers" that clean out the bad traffic. Legitimate traffic is sent on its way, safe and sound, to your network. Your network operates as normal.

What do you have to do as all this takes place? Nothing. And that's the point. We'll send alerts to keep you updated, and notify you when it's over. That's it. We take the problem out of your hands, so you can rest assured your defenses are tight.

merit
NETWORK. SECURITY. COMMUNITY.

MERIT DDoS PROTECTION SERVICE

UNDER ATTACK

The Merit Support Center (MSC) monitors traffic 24 hours a day. The network detection system establishes baselines for normal traffic activity, allowing it to spot attacks.

1. During an attack, the MSC notifies your designated IT points of contact and seeks authorization to launch defensive maneuvers, known as mitigation. Subscribers also can choose the "always on" option, in which case the MSC does not need your authorization to begin mitigation.
2. Traffic is rerouted to "scrubbers" that block and remove the bad traffic.
3. The clean traffic exits the scrubbers and heads to your network.
4. We monitor the situation until the event is over.

WHAT YOU SEE ON YOUR SIDE

1. Your points of contact receive notification of an attack.
2. Subscribers who've chosen the "always available" option are asked for authorization to mitigate. Subscribers who've selected the "always on" option are notified that mitigation is taking place.
3. You receive updates along the way, including when mitigation is complete.

PRICING

Pricing for Merit's DDoS protection is based on a small percentage of each member's bandwidth fees. This model works like that of shared insurance, pooling expenses and lowering costs for all Merit Members. Contact us to learn more.

DDoS: Distributed Denial of Service

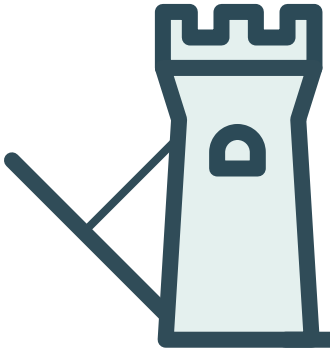
When launching a DDoS attack, hackers take advantage of vulnerabilities in the internet's architecture. They coordinate hosts to deploy hundreds of thousands of bots. This lets them inflate the attack and inundate a network with traffic. The bogus traffic clogs your network. Sites go down. Internet access is blocked. Employees can't access email and other critical cloud services.

Attackers may be motivated by anything from grudges to greed. Merit's many members in the education sector may be familiar with attacks launched on exam days. Our team also has seen online gaming feuds spill over into attacks on campuses.

Attacks have become more effective, sophisticated — and cheap. "DDoS attacks used to just be brute force, in your face, collateral damage," says Kevin Hayes, Merit's chief information security officer. But now criminals use them tactically: as diversions while they steal your intellectual property, for example.

rev 011721

"These attacks have been commercialized to the point where someone with almost no technical expertise whatsoever can go onto the dark web, pay some cryptocurrency and say, 'I would like an attack launched on this organization, or server, or IP address.'"
— Kevin Hayes, Chief Information Security Officer at Merit Network



Fortify Your Defenses Today.

Email our DDoS Protection Sales Team at sales@merit.edu and visit merit.edu/DDoS to learn more

merit
NETWORK. SECURITY. COMMUNITY.