STRONG PROTECTION

FLEXIBLE LAYERS

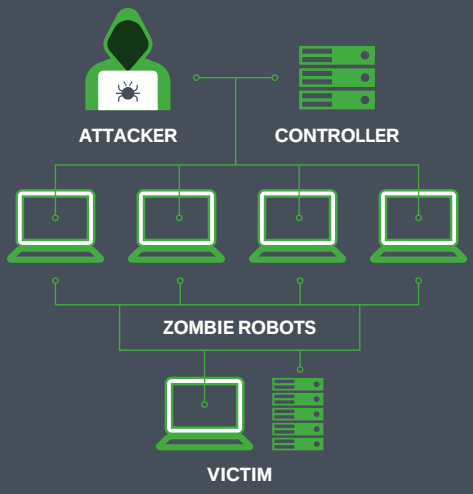
FAST DETECTION

DDoS

MITIGATION

ICN's premier network-based DDoS Mitigation service, delivers a strong cybersecurity layered defense against intruders. As DDoS attacks continue to rise in size, frequency, and complexity, organizations must take a layered approach to help aid in comprehensive protection.

WHAT IS A DISTRIBUTED DENIAL OF SERVICE (DDoS) ATTACK?



A Distributed Denial of Service attack happens when a malicious entity sends more traffic to your network than it can handle in an attempt to overload it. When this occurs, network equipment can fail into a state known as "hub mode" in an effort to maintain communication across the network. When this "hub mode" is enabled, all of the traffic on a network is blasted to every port, allowing an attacker to gather meta and packet data in an effort to map topology of your equipment.

Having a map of your network makes it easier for attackers to push forward with deeper penetration into the infrastructure, allowing them to breach data systems and steal information about your business and clients.

ICN

STRONG,
FLEXIBLE
& FAST

Grimes State Office Bldg.
400 East 14th Street | Des Moines, IA 50319

icn.iowa.gov
(800) 572-3940 / icn.css@iowa.gov

2018

2

ICN OFFERS TWO LEVELS OF DDoS MITIGATION SECURITY SERVICES

	Silver Plan Monitor & Detection Plan	Gold Plan Automatic Detection & Mitigation Plan
Design / The design consultation will include the development of customer requirements, an End User mitigation alert policy and appropriate response procedures.	●	●
Install / Our comprehensive installation includes a customer topology security review and provisioning of the attack-detection system. End User will maintain an ICN Internet connection.	●	●
Configure / Our solution includes provisioning the mitigation service and applying the security policy.	●	●
Administration / Our service includes the organization of administration passwords for the mitigation system(s).	●	●
Monitor / Our advanced monitoring system incorporates automatic detection of attacks. End User traffic is monitored continuously.	●	●
Maintenance and Support / Incorporates software and hardware upgrades to maintain the latest version.	●	●
Mitigate / Mitigation (filtering) of traffic begins after the system determines that a DDoS attack is underway.	*Event Fee**	●
Cleanse / Once mitigation begins, traffic is routed to ICN Cleansing Center. The traffic immediately undergoes the stages to remove the malicious activity. Once cleansing is complete, traffic will be forwarded from the ICN Cleansing Center to its original destination.	*Event Fee**	●

EMERGENCY DDoS SERVICES

ICN offers emergency DDoS services to those in need. Here is how our process works:

STEP 1 / End User will contact ICN identifying that they believe they are under a DDoS attack.

STEP 2 / Network flow monitoring will be set up and customer will be informed of findings.

STEP 3 / End User will give approval to begin mitigation and traffic will be routed to ICN Cleansing Center. Once attack subsides traffic will be pointed back directly to End User.

PREMIUM & PROFESSIONAL SUPPORT

Our premium and professional support team is at your service 24/7 to assist you with your security needs.

*Event (one calendar day) fee is a flat rate daily charge that provides coverage from the first day mitigation is implemented.