Data Sheet

Defense-in-Depth Managed Security Services

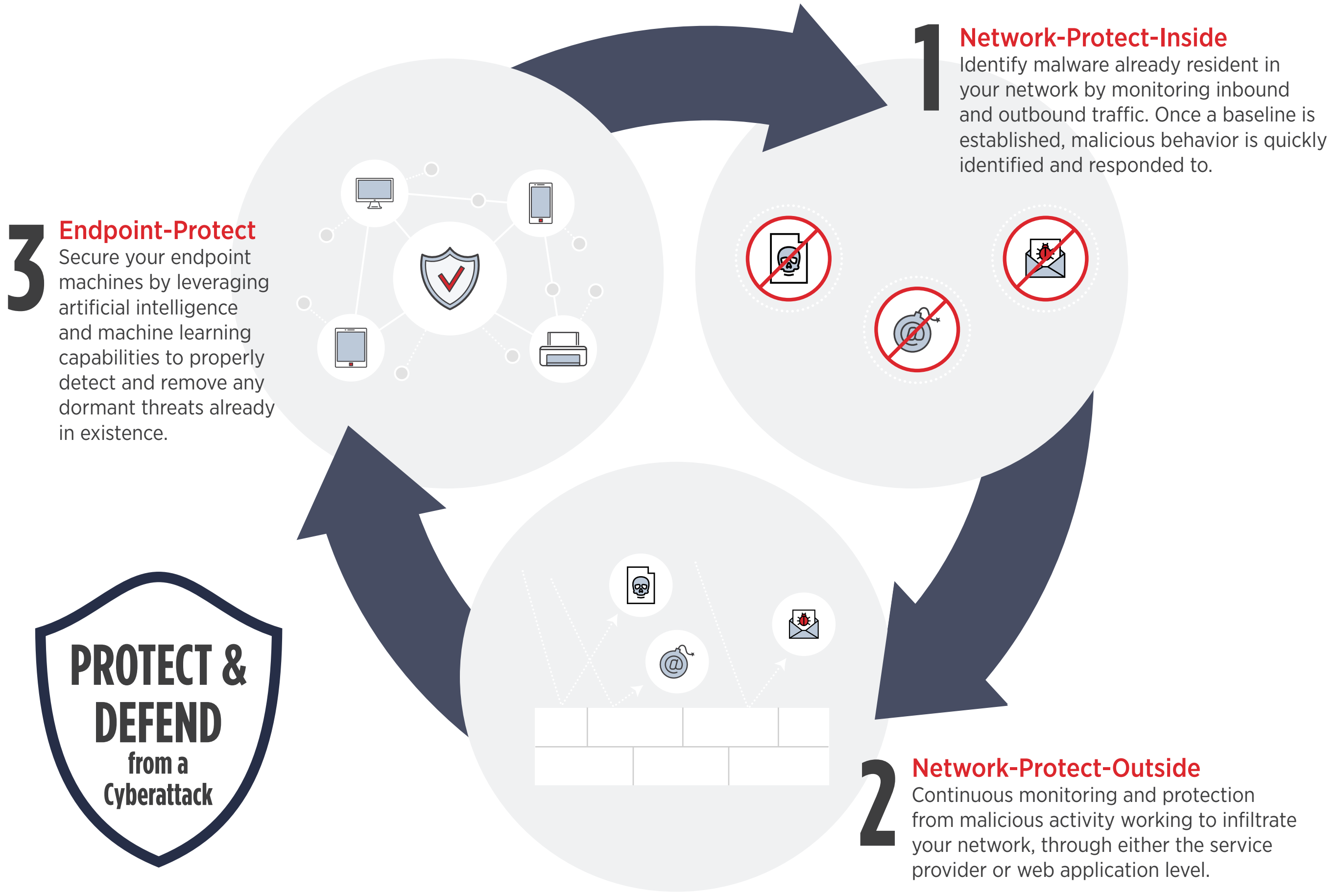
Defending your environment from a cyberattack takes significant effort. So much so, that many enterprise organizations employ expansive teams of subject matter experts and a variety of applications to meet and manage this challenge.

Smaller organizations don't have this luxury to defend their environment. Lack of resources makes mid-market organizations an easy target for cyberattacks.

Through our experience and training in protecting organizations' critical assets, The SCE Group has developed a model that solves for this challenge. Our Defense-in-Depth Managed Security Service delivers a comprehensive strategy to protect and defend your organization from a cyberattack.

This is accomplished by employing three key protection elements: Network-Protect-Inside, Network-Protect-Outside, and Endpoint-Protect.

The SCE Group Defense-in-Depth Managed Security Services model offers mid-market companies an advanced level of cybersecurity protection, without needing to employ your own cyber-defense team.



1 Network-Protect-Inside

Identify malware already resident in your network by monitoring inbound and outbound traffic. Once a baseline is established, malicious behavior is quickly identified and responded to.

2 Network-Protect-Outside

Continuous monitoring and protection from malicious activity working to infiltrate your network, through either the service provider or web application level.

3 Endpoint-Protect

Secure your endpoint machines by leveraging artificial intelligence and machine learning capabilities to properly detect and remove any dormant threats already in existence.

PROTECT & DEFEND from a Cyberattack

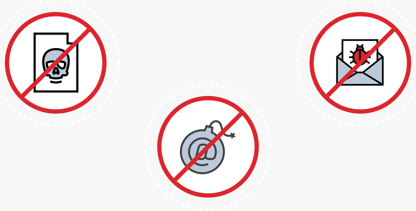
To learn more about how your organization can benefit from
The SCE Group's Defense-in-Depth Managed Security services,
please email us at communications@thescegroup.com.

THE SCE GROUP

Data Sheet

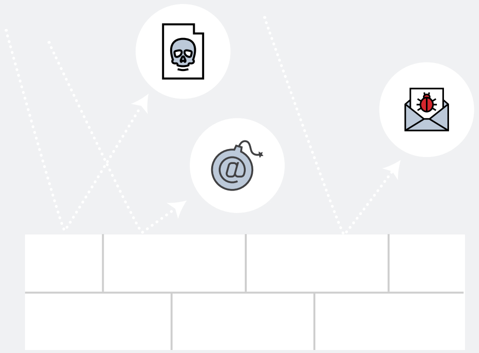
Defense-in-Depth Managed Security Services

HOW IT WORKS



STEP 1: Network-Protect-Inside

Before a network can be secure, you must identify malware that is already resident. This requires the monitoring of inbound and outbound traffic and measuring the results against normal business operations to form a baseline. Once a baseline is established, malicious behavior becomes easily identifiable and traceable. Identifying these malicious actors allows The SCE Group to quickly respond and enforce action, preventing their objective to compromise.



STEP 2: Network-Protect-Outside

Once you've identified and remediated the malicious behavior within your network, the next step is to monitor malicious activity that is working to infiltrate your network from the outside.

Malicious actors can shut down and compromise your network in various ways. At the network level they can flood routers and firewalls with an abundance of requests, thereby rendering complete device failure, allowing all traffic, including malicious traffic, to enter your environment. Application level attacks flood public-facing websites with an abundance of requests. This exercise is intended to take down the site to severely impact e-commerce activity and revenue.

To properly defend against outside agents, continuous monitoring and protection must be performed at the service provider and web application level. This ensures the malicious actors are identified and stopped well in advance of your environment.

STEP 3: Endpoint-Protect

After taking the steps to identify and protect ingress and egress traffic from your network, the final step would be to secure your endpoint machines. Endpoint machines are malware carriers, and threats lie in a dormant state, sitting resident and waiting to execute upon command. Antivirus software is not enough to identify these advanced threats. By leveraging artificial intelligence and machine learning, The SCE Group properly detects and removes threats before they can do harm.

To learn more about how your organization can benefit from
The SCE Group's Defense-in-Depth Managed Security services,
please email us at communications@thescegroup.com.

THE SCE GROUP