THRIVE℠

SERVICE DESCRIPTION

Vulnerability Scanning and Management

Executive Summary

Thrive Vulnerability Scanning and Management Service Definition

Vulnerabilities in firmware and software code can provide hackers and criminals access to your critical systems and sensitive data and exploits can provide a launching pad for attacks inside and outside your organisation. Thrive Vulnerability Scanning and Management service is designed to meet the ever-growing need to assess and report on network and software vulnerabilities.

The service includes scanning, reporting, organisation and consultation of vulnerability mitigation. Client input regarding assets that need to be protected are highly considered on the delivery of our advisory and reporting services. The primary goals for the Vulnerability Scanning and Management Service are to greatly decrease the existing vulnerabilities that exist in Client's environment and provide an ongoing vulnerability management program to keep exploits to a minimum.

Services Scope

The service shall include:

- Installation of Thrive provided vulnerability scanning appliance and/or remote scanning agent
- Discovery and classification of hardware and software assets for scanning
- External scanning for up to 256 IP addresses
- Internal scanning of discovered systems
- Review with Thrive and Client team to review scanning results and assess risk to the organisation
- Guidance on high level remediation processes, including group policies, scripting, and network access policies
- Remediation of individual systems where applicable
- Thrive Vulnerability Management Dashboard

Thrive Scope of Work and Deliverables

- Thrive shall license and install vulnerability scanning tools within the Client internal network. The quantity of scanners required is dependent on the number of Client locations where devices to be scanned reside. Clients who have multiple sites connected through internal networking may be able to consolidate to a single scanner. Remote agents will be installed on user workstations that are not connected to an internal network if included in the Thrive Service Order.

- Thrive shall perform an automated discovery for hardware and software assets. The number of devices is determined by the vulnerability scanning tool. Any discrepancy between the quantities indicated on the attached Service Order and the Vulnerability Scanning tool will result in a billing adjustment to remediate the discrepancy.
- Thrive shall perform automated scanning to identify external and internal vulnerabilities of discovered systems.
- Thrive shall create and dedicated tenant and provide secure access to the Thrive Vulnerability Management Dashboard for visibility and co-management of vulnerabilities.
- Thrive shall provide vulnerability assessment documentation to review results and assess risk to the organisation. Review interval is dependent on the subscribed service (Monthly, Quarterly, or Annually)
- Remediation service is dependent on the impacted device and the management level Thrive has for the affected device, system, or platform.

Client Responsibilities

- Client shall provide the Thrive Security team with sufficient access to the network to install the vulnerability scanning tools.
- Client shall provide the compute resources to install the Thrive scanning tool appliance. The virtual appliance requires 1 CPU's, 4 GB of RAM, and 60GB of storage on a virtual machine. Alternately, Thrive can provide a cloud hosted scanner for an additional fee.
- Client shall be responsible for deployment of the remote scanning agents on subscribed servers and workstations. If Client subscribes to Thrive Managed Server and/or Thrive End User Support managed services, Thrive shall perform the remote scanning agent installation utilising existing Remote Monitoring and Management (RMM) tools in the agent deployment.
- Client shall provide Thrive a list of any devices to be excluded from scanning.
- Client shall actively participate with Thrive Security Engineers in the Vulnerability Management practice prior to and after service kickoff, including co-management of vulnerability status in the Thrive Vulnerability Management portal.
- Client shall be responsible for remediation of vulnerabilities on any device not contracted for and under active management by Thrive.
- Client shall accept risk of certain vulnerabilities as remediation for all items is not commercially reasonable. Thrive will work with Client and advise on situations where actual exploitation of vulnerabilities is highly unlikely.
- Client shall provide escalation contacts to Thrive for critical event notification.

Service Exclusions

Any service not explicitly included in the Vulnerability Management Definition above is considered optional and may be provided under separate agreement for an additional fee.