Cyber Security Bundle

Best-In-Class Security Products

Thrive's Cyber Security Bundle leverages best-in-class technologies to deliver a holistic end user security solution that helps prevent against ransomware, data exfiltration, and social engineering attacks.

With the recent increased shift to a remote workforce, ensuring endpoint and end user security becomes more challenging and requires a multi-layered approach. Thrive's Cyber Security Bundle addresses these challenges to provide protection against these threats to your end users and organization:

- Malware
- Social Engineering
- Phishing
- Ransomware

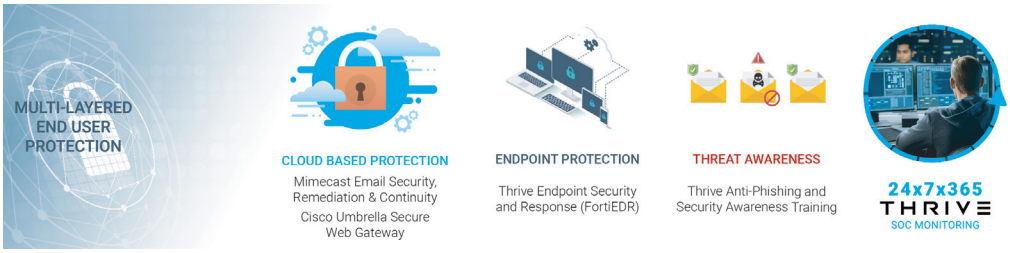
People are the weakest link in the security chain and human error is the leading cause of data breaches. As attacks become more widespread and sophisticated, end user protection and education are key security measures that can mitigate against costly data breaches that result in monetary loss, loss of productivity, and brand damage.

81% of all breaches come in from end users

The average time it takes for a company to recognize a data breach is **206** days

It's estimated that a ransomware attack occurs every **11** seconds

91% of all attacks launch aim at end users through a phishing attempt



The Thrive Advantage

- Managed Services Provider (MSP) - Unbundled managed services enable you to create a solution tailored to your exact needs, utilizing leading technology from Fortinet, Microsoft, Cisco, Mimecast, Qualys and more, ensuring that your business has Enterprise-grade security.
- Security Solutions - Thrive's Security Operations Centers are staffed by experienced CISSPs and security professionals with decades of experience protecting mission critical infrastructure.
- Security Operations Center (SOC) - 24x7x365 Monitoring and Management of industry-leading security technology.
- Consulting - Thrive addresses gaps that may exist in your organization by providing a variety of expert professional and consultative services with an agnostic approach to identifying and prioritizing risk.

Take the Next Step

To learn more about how Thrive can help your business, please visit thrivenextgen.com

Cyber Security Bundle

Component Descriptions

Endpoint Security & Response

Thrive's Endpoint Security and Response service provides Next Generation malware detection & protection for servers and workstations. FortiEDR is the only advanced endpoint protection platform that protects endpoints both pre- and post-infection and stops breaches and ransomware encryption in real time, automatically. It prevents malware infection with machine learning antivirus, detects and defuses potential threats in real time, and automates response and remediation procedures with customizable playbooks.

Secure Internet Gateway

Thrive's Secure Internet Gateway provides the first line of defense against threats on the Internet. Utilizing the Cisco Umbrella platform, the service delivers visibility into Internet activity across corporate network locations and blocks threats before they ever reach end points. As a Cloud-delivered, open platform, Umbrella integrates easily with existing security infrastructure and delivers live threat intelligence about current and emerging threats. By analyzing and learning from Internet activity patterns, Umbrella automatically uncovers attacker infrastructure staged for attacks, and proactively blocks requests to malicious destinations before a connection is even established.

Advanced Email Security

Mimecast Email Security, Remediation, and Continuity protects your email from evolving threats, keeping your email up and running during downtime, and reducing your time to recovery through Threat Remediation and mailbox restoration and recovery. Features include:

- Virus and spam protection
- DNS authentication and advanced reputation checks
- Multi-layered malware protection against known and zero-day threats
- URL re-writing with on-click scans to block malicious URLs in email and attachments
- Content Examination and Data Leak Prevention (DLP) for inbound and outbound mail

Anti-Phishing & Security Awareness Training

Thrive's Anti-Phishing and Security Awareness Training service provides ongoing security testing and training for your users to increase awareness of risks associated with phishing, spear phishing, malware, ransomware and social engineering attacks with targeted user campaigns and responsive training aimed at improving awareness of and avoiding security threats. Improving user awareness of these threats reduces risk of human error resulting in security breaches and ransomware.