THRIVE℠

NextGen | PARTNER

Overview

As a leading provider of outsourced IT infrastructure, Thrive delivers NextGen managed services designed to optimize business performance, ensure scalability, and future-proof digital infrastructure operations.

Services

- Flexible and Powerful Platform that Delivers NextGen Managed Services that Optimize Business Performance, Enable Scalability, and Power Digital Infrastructure Operations
- Private, Public & Hybrid Cloud
- Cybersecurity
- Backup/Disaster Recovery
- Collaboration
- Global Network Management
- Professional Services
- Help Desk & End User Support

Key Differentiators

- Automation and Orchestration Managed Services Platform Built on ServiceNow that Optimizes the Client Experience
- NextGen Platform of Products, Services & Technologies
- Advanced Cybersecurity Services
- Dedicated Technical Service Delivery Team Focused on Your Company and Vertical
- Consultative Approach Using the Thrive5 Methodology

Leadership

- PE Backed By Court Square Capital (New York, NY) and M/C Partners (Boston, MA)
- Court Square portfolio companies include Ahead Technologies, DataBlue and Momentum Telecom
- M/C Partners portfolio companies Include: Zayo, Lightower, Involta, and Denovo
- Senior Management Has More than 100 Years of Technology Service Experience

Which Describes Your Approach to Cybersecurity?

REACTIVE

1. Have you had any challenges, or do you foresee making any changes to your cybersecurity program?
2. Have you identified where you need to invest when it comes to IT?
3. Do you have any compliance or regulatory requirements to adhere to?

PROACTIVE

1. Are you receiving any due diligence requests from vendors or customers?
2. Are you facing compliance challenges with cybersecurity insurance renewal?
3. Have you observed cybersecurity events taking place within your vertical or among your competitors?
4. Do you have assurance of your ability to predictably recover from a cybersecurity event?
5. Are you getting everything your company needs from how IT is setup in your organization?
6. Have you validated and do you feel comfortable with your current security strategy?
7. How is your current cloud strategy helping you maximize your IT ROI?

THOUGHT LEADER

1. Have you validated and do you feel comfortable with your current cybersecurity strategy? Do you have one?
2. Have you identified where you need to invest when it comes to IT?
3. Have you adopted a recognized cybersecurity framework?
4. Do you have any compliance or regulatory requirements?
5. How are you continually validating the effectiveness of your cybersecurity strategy?

How to Engage

5 Things to Listen For

- Client mentions any security issues or initiatives.
- Has the client discussed moving to the cloud (DRaaS, O365, AWS, Azure, Hyperscale etc.)?
- Client mentions compliance and regulatory requirements.
- Client is expanding or outgrowing IT team, existing MSP or cloud provider.
- Client has had outages, service issues, failed audits or major IT problems.

Cloud

- What is your cloud strategy?
- Can we have the cloud conversation?
- What applications do you currently have in the cloud (email, SaaS)?
- How old is your on-premises server infrastructure?
- When will you be faced with a refresh?
- How do you purchase hardware (OPEX or CAPEX)?
- Do you have any specific compliance needs?

Disaster Recovery

- What is your backup and disaster recovery plan?
- What's the impact on your business if you couldn't access your data?
- What would the impact be on your business if your applications were inaccessible?
- What is the productivity and financial impact to the business if your employees can't access your servers and applications?
- Is your current business continuity plan documented (do you have a runbook?) and do you test it?
- Have the needs of the business changed since you incorporated your business continuity plan and have ? you re-evaluated it?
- Do you currently back-up your 0365 environment

Cybersecurity

- Is there an adopted and implemented cybersecurity strategy?
- Have you identified necessary cybersecurity risk mitigation investments?
- Have you adopted a recognized cybersecurity framework (i.e. NIST, ISO, etc.)?
- Do you have any compliance or regulatory requirements to adhere to? Does your current security plan align/meet your regulatory requirements?
- How are you continually validating the effectiveness of your cybersecurity strategy?
- If a cyber event occurred today, have you already defined the next steps?
- Do you have a qualified cybersecurity advisor?
- Are all of your device logs centralized in one location?
- How confident are you with your current cybersecurity plan?
- How important is cybersecurity to your organization? Do you have full support from your executive team and board?
- Are you currently using an MSSP today? If so, which one(s) and for which services?
- If yes, how has your experience been?

CASE STUDY

Vertical: Healthcare

- **Number of Employees:** 1400
- **Business Challenge:** Company was being carved out of a larger organization and had to completely stand up all IT services and support
- **Services Provided:** Managed Server patching, Managed End User Patching, Managed Firewalls, 24x7 SIEM Performance Monitoring, Azure DR and Backup Management, End User Support
- **MRR:** $144,000

CASE STUDY

Vertical: Retail

- **Number of Employees:** 1000
- **Business Challenge:** Company was at a critical point with lack of Security controls and Data Center Infrastructure going end of life with no DR.
- **Services Provided:** Thrive is providing a complete Production environment on Thrive Cloud (Windows and AS400), DR for both Windows and AS400, 365 Email Security, Backups, and EDR for all Servers and Endpoints.
- **MRR:** $90,000 – 4 Year Term