Partner Email Campaigns

Agents and Technology Consultants partner with Thrive to leverage our technical expertise coupled with our NextGen managed services. Thrive is considered a trusted advisor that partners rely on to offer their clients NextGen Technology Services.

Thrive has developed a Partner Email Campaign program that allows our Partners to co-brand and leverage Thrive's collateral, email marketing campaigns and marketing automation platform.

For more information, contact your Thrive Rep. TODAY!

1 CHOOSE AN EMAIL

CLICK the links below to see email samples. Emails will be co-branded with your logo.

1. **Cyber Security Bundles**
2. **Endpoint Security & Response**

2 LIST

There are 2 options for lists. Please let Thrive Marketing know your choice.

1. Partner provides Thrive Marketing a list to be imported to Thrive's marketing automation platform. ****List cannot contain more than 100 contacts****
2. Campaign email will drafted by Thrive Marketing and sent to Partner. Partner can forward the email to their contacts and provide Thrive updates/feedback.

3 REPORTING

- **Responses** - Thrive Sales Rep. will forward any responses to Partner or if someone reaches out directly to the Partner they will let Thrive know.
- **Email Send** - Original email will be sent out again approximately 1 week after the first email is sent.
- **Open Report** - An Open Report will be generated after the first and second send and sent to the Partner and Thrive Rep.

Why Thrive?

Thrive is one of the largest and fastest growing providers of NextGen managed services in the U.S. With a team of 200+ engineers and 500+ technical certifications, Thrive is a proven technology partner that continuously drives business outcomes, innovation, and overall customer success through its traditional and NextGen managed services.

Thrive's Application Performance Platform and strategic services ensure each business application takes advantage of technology that enables peak performance, scale, and the highest level of security.

The demand for NextGen Cloud and security continues to grow rapidly and Thrive is well equipped with the highest levels of security, technical expertise and industry leading customer service for our clients.

Thrive has seen incredible growth within their customer base of 1,000+ companies and with new opportunities within their Cloud, Managed Security and Managed Services portfolio.

With the foundation of our services, and the Thrive Application Performance Platform, organizations are empowered to tap into best-of-breed technologies and best practices to run and manage their entire IT environment or individual components regardless of vertical or compliance drivers.

Thrive has an Industry leading automated self-service Managed Services Platform powered by ServiceNow delivering you the optimal customer experience.

Cold Calling Scripts

1 IT STRATEGY

Hi my name is_____

I am calling from _____ on behalf of Thrive, one of the largest and fastest growing managed security providers in the country.

Are you currently looking to make any adjustments to your current IT strategy? Specifically with regard to cyber security? Entering 2020, cyber security was the top issue on CIOs minds, Thrive can help you develop a technology roadmap to drive value for your business. Are you currently looking to make any adjustments to your current IT strategy? Specifically with regard to cyber security?

We'd love to set up a consultation call to understand your current IT landscape and how we may be able to help you reach your IT goals.

2 CYBER SECURITY

Hi my name is _____

I am calling from_____ on behalf of Thrive, one of the largest Managed Service and Security Providers in the United States with the ability to manage your entire IT environment with one of their main focuses is on cyber security. Are you confident in your organization's current security posture?

Thrive has had a tremendous amount of security focused engagements driven by COVID-19 as businesses look to understand where to invest, what has worked for them, and what has not. Their consulting team offers a Security Health Assessment to help uncover vulnerabilities within these businesses and develops a plan of action based on risk, effort & cost that prioritizes which areas to address first.

When are you available for brief call with Thrive's consulting team for you to learn more about their engagements and how your business may benefit from a security perspective.

3 Managed SIEMaaS

I am calling from_____ on behalf of Thrive, one of the largest Managed Service & Security Providers in the United States with the ability to manage your entire IT stack. One of their main focuses is on cyber security, are you confident in your organization's current security posture?

- How do you currently monitor for security threats, events and vulnerabilities?
- Is your company bound by any cyber security regulations?
- Has a recent security audit identified gaps in log monitoring or vulnerability management?
- Do partners or customers require your company adhere to their security guidelines?

Answer: These are the challenges Thrive solves on a daily basis. Thrive's managed security solutions and dedicated security engineers, can help your company meet it's security and compliance goals. Let's set up a call to talk about how Thrive can help you meet these goals today.

THRIVE℠

Points-of-Focus
Partner to Client

5 Things to Listen For

1 Client mentions any security issues or initiatives.

2 Has the client discussed moving to the cloud (DRaaS, O365, AWS, Azure, Hyperscale etc.)?

3 Client mentions compliance and regulatory requirements.

4 Client is expanding or outgrowing IT team, existing MSP or cloud provider.

5 Client has had outages, service issues, failed audits or major IT problems.

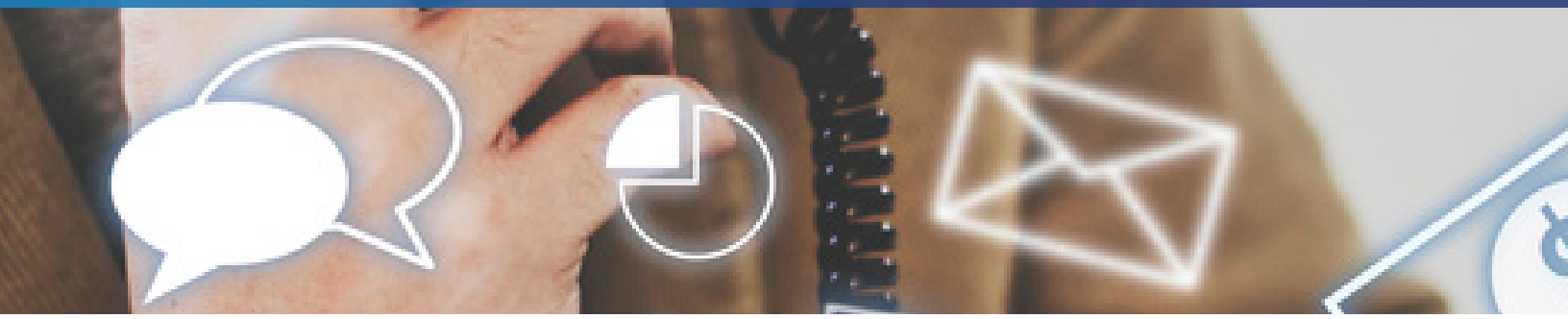
THRIVE℠

Points-of-Focus
Partner to Client

5 Questions to Ask

1. Have you validated and do you feel comfortable with your current security strategy?
2. Have you identified where you need to invest when it comes to IT?
3. How is your current cloud strategy helping you maximize your IT ROI?
4. Are you getting everything your company needs from how IT is setup in your organization?
5. Do you have any compliance or regulatory requirements to adhere to?

Voicemail Options



1 SERVICES OVERVIEW OPTION

Hello this is_____ calling on behalf of Thrive, one of the largest managed security providers in the country. With security being an evolving issue and main topic of concern for businesses of all sizes and verticals, I wanted to reach out and see if you had any interest in learning more about our services and how we may be able to help you reach your IT goals.

Feel free to give me a call back at _____and I can arrange a brief consultation call with the Thrive team to see if there may be a fit. Thank you.

2 SECURITY CONSULTATION OPTION

Hi this is _____ calling on behalf of Thrive, one of the largest managed security providers in the country. I wanted to reach out and offer you a consultation to learn a little about how Thrive can enhance your security posture and drive value for your business.

If you are interested you can reach me at _____and I will connect you with the Thrive team for an intro call to see if there is a fit. Thank you.

Cyber Security

SAMPLE CASE STUDY

THRIVE℠

Healthcare company is released from operation-stalling cryptolocker.

Thrive's NextGen Managed Services provide customers with a technology advantage on all aspects of digital infrastructure, including strategy, application performance, cloud, cyber security, networking, disaster recovery, and more.

Thrive's Cyber Security services leverage best-in-class security platforms from multiple security vendors to deliver a holistic end-user NextGen solution that helps prevent against both network-based and social-based attacks.

Why is your business a great fit for Thrive's Cyber Security Platform?

- Protect Sensitive Information
- Data & Security Breaches
- Protecting & Educating End Users
- Threats to End Users
- Thrive offers two cyber security Packages to meet your end-user security needs.

CHALLENGE

Password security and Multi-Factor Authentication are two of the best lines of defense for users to protect themselves against bad actors. After a weak default password without Multifactor Authentication allowed a hacker to gain access to the company's network, a large healthcare provider's data was encrypted and inaccessible; which halted their operations for nearly twenty-four hours across multiple locations. Ransomware was discovered by the Thrive team on upwards of twenty of the company's servers.

SOLUTION

Thrive's Cybersecurity Forensic Analysts took quick action to source the bad actor and work towards remediation. Utilizing best-of-breed tools, they were able to identify the IP addresses in which the attack was originating from and effectively block them from the network. Simultaneously, the Thrive team was able to configure restoration on the servers and perform back up measures. Within twenty-four hours of the original incident the first server was restored, and the remaining were all operational within four days.

RESULT

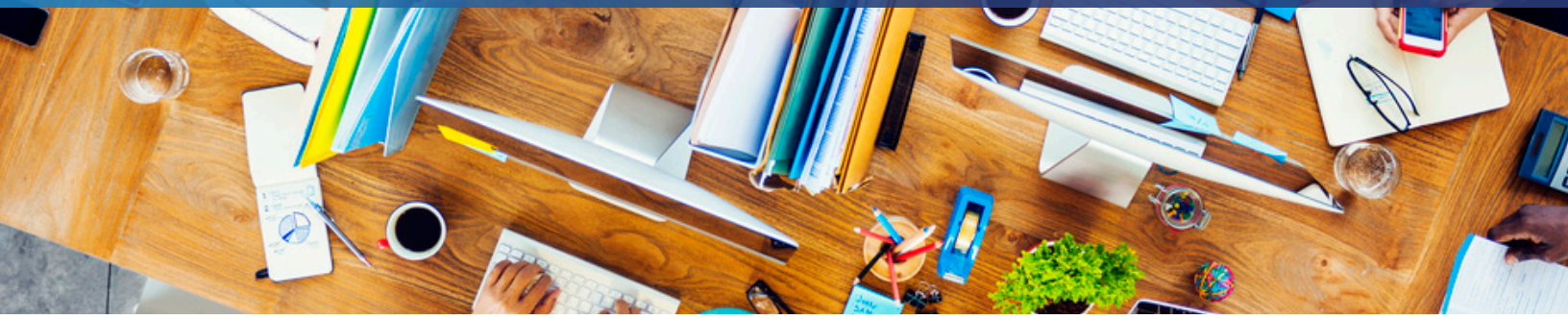
The immediate results of the remediation of the servers were that the healthcare provider became operational once again and able to serve their patients.

After the event was resolved the organization enlisted Thrive to perform a Security Health Assessment across their environment. Thrive's cybersecurity team was able to identify vulnerable target areas in the company's infrastructure and architect customized solutions. All of these being actionable items, the organization has been able to further leverage Thrive's services to strengthen their security framework to prevent future incidents .

How can Thrive help your business?

Thrive is a leading provider of NextGen Managed Services designed to drive business outcomes through application enablement and optimization. To learn more about our services, contact us at 866.205.2810 or info@thrivenetworks.com

Objections & Responses



1 New IT projects have been put on hold.

RESPONSE 1: We have seen some projects get delayed or canceled with other customers but the largest trend that we are seeing is companies who have had various cyber security impacts to their business and would like some assistance with strategy and/or in helping to protect their business. Have you seen any issues or blind spots in your cyber security strategy?

RESPONSE 2: We are seeing a couple trends with spending; companies have postponed or canceled Capital IT purchases but are embracing an Operational Expense model as a way to address COVID driven needs like cyber security.

2 I'm not having any security problems with {email, network, web etc} Security right now.

RESPONSE: It's only a matter of time before someone at your organization takes a risky action that puts the entire company's security at risk. Human error is involved in over 90% of data breaches, and you need a technology solution to provide a safeguard.

3 We're too {small, wrong vertical} to be the target of cyber attacks.

RESPONSE: Any company that relies on email, web services or has mobile employees can be hacked. The number, financial impact and complexity of cyber-attacks to small to mid-sized businesses have increased more than any other sector over the past year. We would like to sit down and discuss your options and weigh the risk vs. cost variables for you.

4 We plan to hire a security engineer and mange this in house.

RESPONSE: The talent gap for security people is larger than any other position within IT. ISC Squared said "The talent pool needs to increase by 62% to handle current openings and the problem is getting worse". Thrive has the people, expertise, tools, services and bench to help mid-sized businesses get around this problem.

5 We have network, firewall, endpoint and other security tools in place, that's good enough.

RESPONSE: Those are important layers of a strong cyber security posture but only a few pieces of the overall picture. Are you able to continuously monitor alerts, vulnerabilities, identify and handle advanced threats? Have you ever sat down with anyone to look at your strategy to ensure it is sound?

6 We're using a SIEM that works well for us.

RESPONSE: Our experience is that, SIEM's are difficult to install maintain and nearly impossible to monitor without a dedicated security team. Are you actually detecting threats and risks or just checking a box?