THRIVE℠

DM ENTERPRISE GROUP

Is your Cyber ready to defend

Executives Decoding Cybersecurity

Thrive Overview

About Us

- Year Founded: **2000**
- Headquarters: **Foxborough, MA, US**
- Total Employees: **1,200+**
- Technical Resources: **700+**
- Technical Certifications: **900+**
- End-Users: **180,000+**
- Total Devices: **325,000+**
- Years of Technical Experience: **3000+**
- **SOC II Type 2 Certified**
- **ISO27001**
- **ISO9001**
- **Cyber Essentials Plus**
- **BS 10012**

Client Base

- 2,200+ customers worldwide
- Servicing SMBs to Enterprises, with a heavy concentration in the Mid-Market (100 to 5,000 employees)
- Diverse customer base with focus on:
  - Financial Services
  - Healthcare
  - Life Sciences
  - State and Local Government
  - Legal, Accounting & Professional Services

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
- Microsoft 365 Platform Services
- Global Network Management
- Professional Services
- Help desk & end user support

Key Differentiators

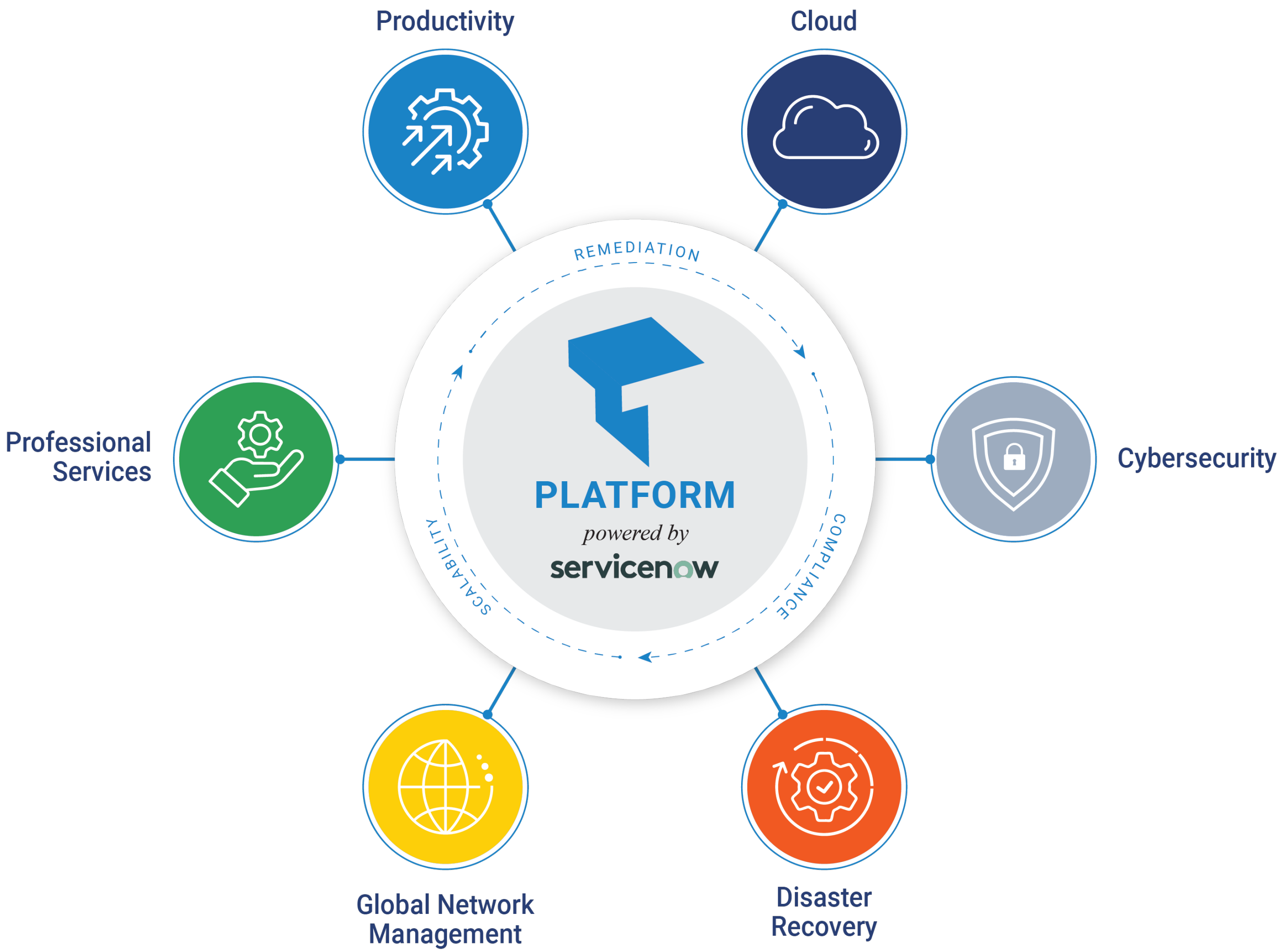
- Automation and orchestration Managed Services Platform built on ServiceNow that optimizes the client experience
- NextGen Platform of products, services & technologies
- Advanced cybersecurity services
- Dedicated technical service delivery team focused on your company and vertical
- Consultative approach 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

NextGen Managed Services

Thrive's NextGen Managed Services Platform is designed to optimize business application performance via secure, redundant Cloud-based infrastructure.



Thrive Office Locations

Thrive has **27** locations across the US, UK, Canada, Australia, and Asia

United States

- Foxborough, MA
- Austin, TX
- Baltimore, MD
- Birmingham, AL
- Boston, MA
- Charleston, SC
- Chicago, IL
- Greenwich, CT
- Jackson, MS
- Lakeland, FL
- Memphis, TN
- Miami, FL
- New York, NY
- Philadelphia, PA
- Portland, ME
- San Francisco, CA
- Sarasota, FL
- Washington, DC

Canada

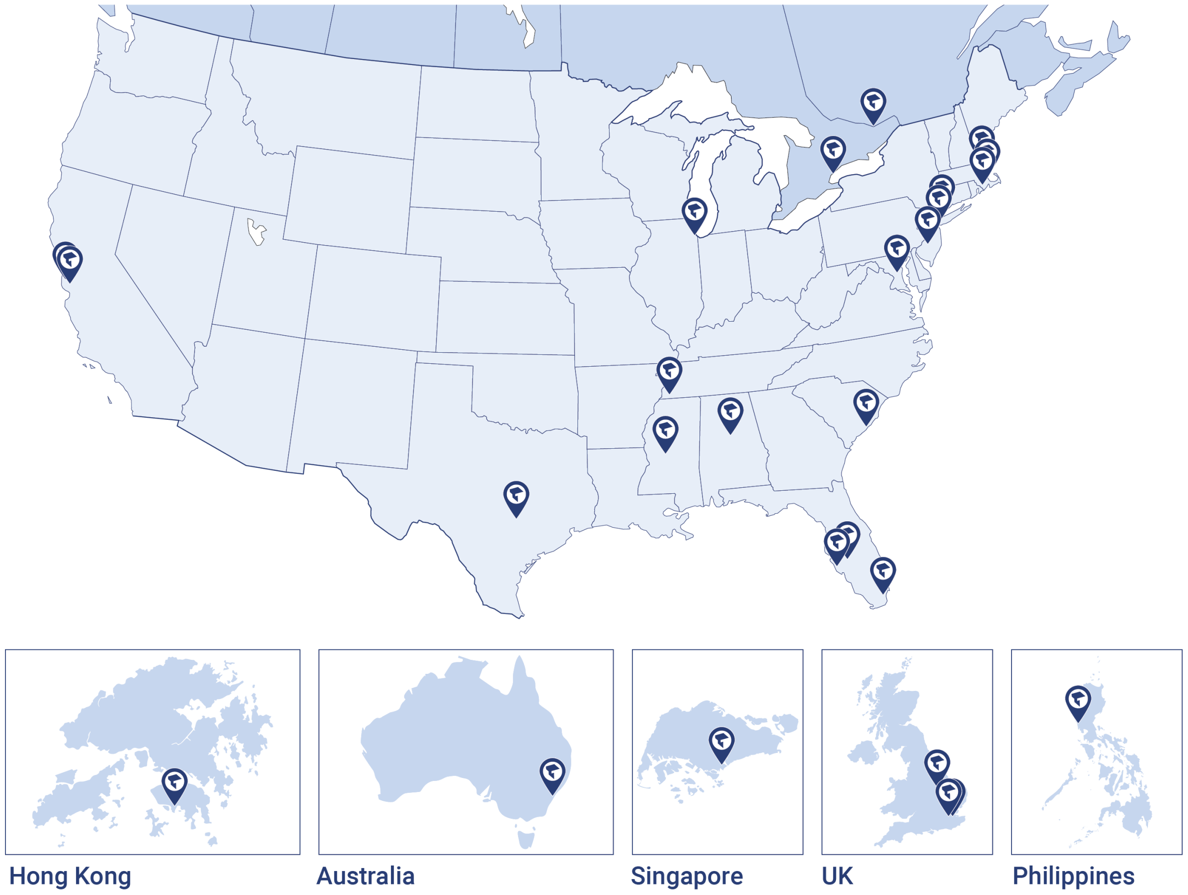
- Toronto
- Ottawa

Europe

- London, UK (3)

Asia Pacific

- Hong Kong
- Sydney, Australia
- Singapore
- Philippines



Cybersecurity for Executives:

Managing Organizational Risk

Key Questions

- Do you feel comfortable with your current security strategy?
  Do you have one?

- Have you identified where you need to invest when it comes to cybersecurity?

- If an event occurred today, have you defined next steps?
  Has the plan been tested?

- Do you have any compliance or regulatory requirements to adhere to?

- How are you continually validating the effectiveness of your cybersecurity strategy?

Key Questions (cont.)

- Is your organization addressing cybersecurity via a comprehensive approach?
- Is there a vehicle to correlate data generated by risk mitigating technologies?
- How quickly can you analyze data, make informed decisions, and execute changes to reduce organizational risk?
- Are the risk mitigating technologies you have deployed today integrated?
- Are you able to act quickly when threats occur?

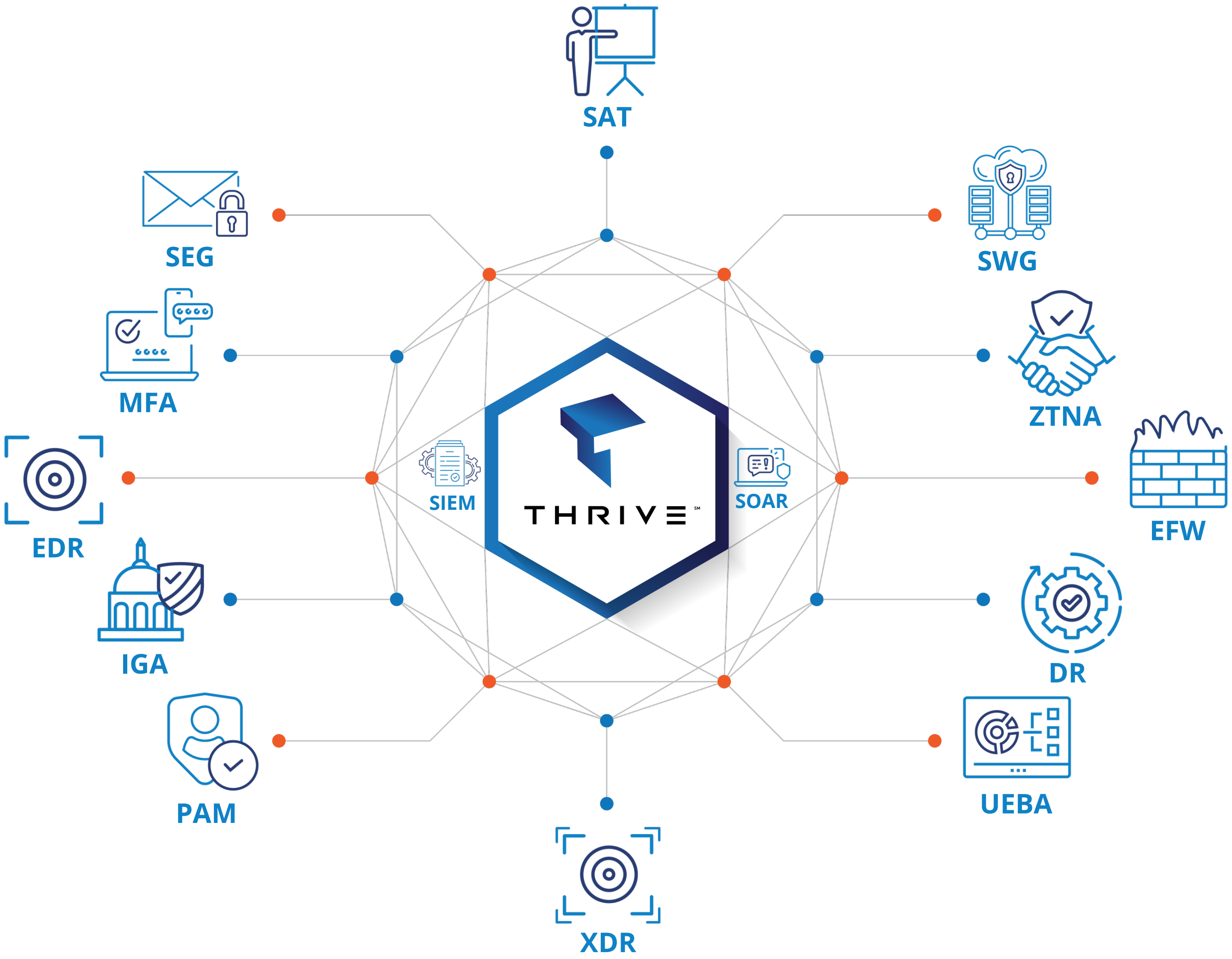
Cybersecurity for Executives:

CSMA & Cyber Risk Mitigation

Cybersecurity Mesh Architecture (CSMA)

Cybersecurity mesh, or cybersecurity mesh architecture (CSMA), is a collaborative ecosystem of tools and controls to secure a modern, distributed enterprise. It builds on a strategy of integrating composable, distributed security tools by centralizing the data and control plane to achieve more effective collaboration between tools. Outcomes include enhanced capabilities for detection, more efficient responses, consistent policy, posture and playbook management, and more adaptive and granular access control — all of which lead to better security.”

Thrive’s Cybersecurity Mesh Architecture (CSMA)



Gartner Key Findings

Cybersecurity Mesh Architecture (CSMA)

Cybersecurity Mesh Architecture (CSMA) is an emerging approach for architecting composable, distributed security controls to improve your overall security effectiveness. Security and risk management technical professionals can use this blueprint to start aligning their roadmap for security and IAM technologies that plug into a mesh.

1. Effective security and identity management requires a layered approach, but today's solutions are instead silos that operate with insufficient knowledge of other tools and leave gaps. These silos are time consuming to operate and monitor.
2. SOC teams are not armed with the right cybersecurity intelligence and integrated defense tools to stop and predict attacks.
3. Current cybersecurity deployments are unable to make contextualized enforcement decisions fast enough to meet business needs.
4. IT security organizations are overwhelmed when trying to stay ahead of new and more complex attacks and deploying the latest security tools to ever expanding infrastructure. Teams are struggling to enable automatic and predictive dynamic security decisions.

Why Thrive?

1 Effective security and identity management requires a layered approach, but today's solutions are instead siloes that operate with insufficient knowledge of other tools and leave gaps. These silos are time consuming to operate and monitor.

→ **Thrive reduces gaps by connecting siloed solutions with two-way integrations that pull data into the mesh and push actions out to a wide range of tools.**

2 SOC teams are not armed with the right cybersecurity intelligence and integrated defense tools to stop and predict attacks.

→ **Thrive's cybersecurity mesh includes threat intelligence and integrated defense tools to anticipate and prevent attacks.**

3 Current cybersecurity deployments are unable to make contextualized enforcement decisions fast enough to meet business needs.

→ **Using automation and orchestration, Thrive adds more context and faster connections between tools so that enforcement decisions align with the speed of business.**

4 IT security organizations are overwhelmed when trying to stay ahead of new and more complex attacks and deploying the latest security tools to ever expanding infrastructure. Teams are struggling to enable automatic and predictive dynamic security decisions.

→ **Thrive supports clients and their ever-changing threat surface by constantly evaluating and improving our people, processes, and the technologies that are connected through the cybersecurity mesh.**

Autonomous Penetration Testing

Autonomous penetration testing uses an automated tool to perform penetration testing on a network or system. This testing involves attempting to identify vulnerabilities in the target system by simulating attacks that a malicious actor might carry out.

Autonomous penetration testing tools work by scanning the target system for weaknesses, analyzing the results of the scan, and then attempting to exploit any vulnerabilities found.

Thrive provides a one-time Autonomous Penetration Test to identify areas of risk and provides both a Penetration Test Results report and Fix Actions report that outlines the steps required to eliminate the risk. A Thrive Consultant will review the test outputs with you to provide feedback and strategic recommendations.

Penetration Testing Benefits

- Find weaknesses in systems
- Determine the robustness of controls
- Support compliance with data privacy and security regulations (e.g., PCI DSS, HIPAA, GDPR)
- Provide qualitative and quantitative examples of current security posture and budget priorities for management

Key Takeaways

- Security Programs supported by policy & technology.
- Ongoing Validation
- CSMA Security Platforms will lead
- Policy weighs equally with technology
- Benefits of Outsourcing

> “By 2024, organizations adopting a cybersecurity mesh architecture will reduce the financial impact of security incidents by an average of 90%.”

Thank you