SECURING THE MODERN WEALTH MANAGEMENT FIRM:

A Decision-Maker's Guide

A Practical Framework for Evaluating Security in a Distributed, High-Stakes Environment

in partnership with ▼

todyl

omega systems
technology managed

SECURING THE MODERN WEALTH MANAGEMENT FIRM:

A Decision-Maker's Guide

omega systems
technology managed

Table of Contents

93%

of firms experienced at least one cyber incident in the past year, highlighting how common security threats are

Executive Perspective:

When Security No Longer Matches the Threat

Most cybersecurity failures in financial services do not begin with sophisticated breaches. More often, they begin with security approaches built for a different era.

Investment advisers and wealth management firms now operate across distributed advisory teams, cloud-based applications, and a growing ecosystem of third-party platforms. Yet much of the industry still relies on network security models designed around a single office location – not a distributed workforce.

The result is a widening gap between how firms operate and how they are actually protected.

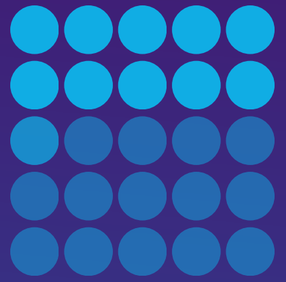
Omega Systems' **2025 Financial Services Cyber Resilience research** illustrates how widespread these incidents have become.

- 93% of financial services firms experienced at least one cyber incident in the past year
- Nearly one in five firms faced more than 25 attacks annually

The business implications extend beyond technical disruption. 88% of financial executives say a successful cyberattack would likely trigger investor withdrawals or loss of client confidence.

Executive Perspective

continued



42%

of financial executives cite staying current with evolving requirements as their biggest compliance roadblock

At the same time, compliance pressures continue to grow.

- 42% of regulated firms cite evolving regulatory requirements as their top challenge
- 54% still rely on spreadsheets or manual processes to benchmark security controls

This combination of rising cyber activity, expanding regulatory expectations, and distributed teams has pushed many firms to rethink how they approach security.

Secure Access Service Edge (SASE) has emerged as the leading response to this shift.

For wealth management firms – including registered investment advisers (RIAs), family offices, financial planning firms and others – evaluating SASE, the decision is not simply about adopting a new cybersecurity tool. It requires understanding how security approaches must evolve to support the way your firm operates today.

The following evaluation framework outlines **five stages many financial services firms use when assessing SASE solutions**.

Stage 1: Recognize the Gap

Between How You Work and How You're Protected

Traditional network security models have long been designed around a simple assumption: everyone works from a single office location, inside a defined and controllable network perimeter.

That assumption no longer reflects the reality of modern investment operations.

Advisors increasingly access systems from:

- Home offices
- Client locations
- Conferences and travel networks
- Shared branch environments

Meanwhile, core business platforms increasingly operate outside the firm's internal network:

- Microsoft 365 and collaboration platforms
- Cloud-based portfolio management systems
- SaaS CRM and analytics tools
- Custodian and third-party financial platforms

With work no longer confined to the network perimeter, security must be anchored to the user – not the office.

Recognize the Gap

continued

The result is a security environment where the traditional network perimeter no longer reflects where work actually occurs.

In addition to security limitations, many firms also find that traditional VPN infrastructure introduces latency, inconsistent connectivity, and operational friction for advisors accessing cloud platforms remotely.

If a VPN credential is stolen, it can act like a master key — giving an attacker access to far more than they should ever reach.

Traditional Security Model	Modern Wealth Management Environment
Office-centric workforce	*Distributed advisory teams*
Applications hosted internally	*Cloud and SaaS platforms*
Perimeter firewalls	*Identity-based access controls*
Network-level trust	*Continuous verification*

> Your advisors moved to the cloud.
> Your security may still be waiting at the front door.

Stage 2: Know the Threat

Today's attacks target identities, not networks

Most attacks targeting financial firms today are not traditional network intrusions.

They are **identity-based attacks** that exploit stolen credentials or compromised devices.

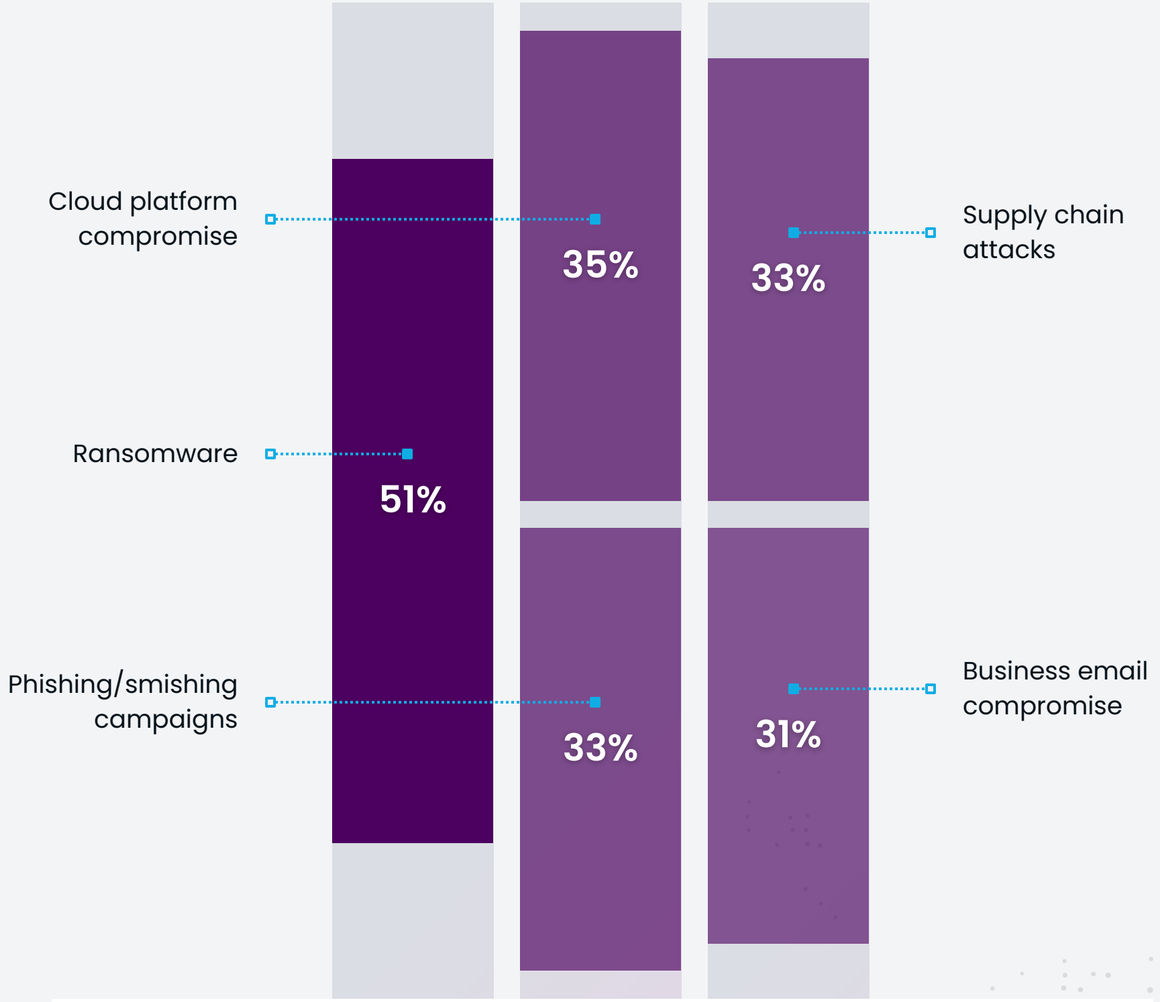
Among the threats RIAs and wealth managers report feeling least prepared to recover from include:

- Ransomware – 51%
- Cloud platform compromise – 35%
- Phishing or smishing campaigns – 33%
- Supply chain attacks – 33%
- Business email compromise – 31%

These attacks rarely require bypassing firewalls. Instead, attackers authenticate using legitimate credentials and operate inside the network as authorized users.

In traditional VPN environments, this often grants attackers wide-ranging network access, making a single compromised credential disproportionately impactful.

The 5 Threats Firms Fear They Can't Recover From



The common thread across all of these attacks is the same: once inside, traditional security models have little left to offer.

Stage 3: Understand What Changes

When Security Follows Your People, Not Your Office

Think of SASE as security that travels with your people rather than staying anchored to your office — wherever an employee logs in, the same controls, verification, and monitoring follow them. Secure Access Service Edge (SASE) represents a shift from location-based trust to **identity-based security**.

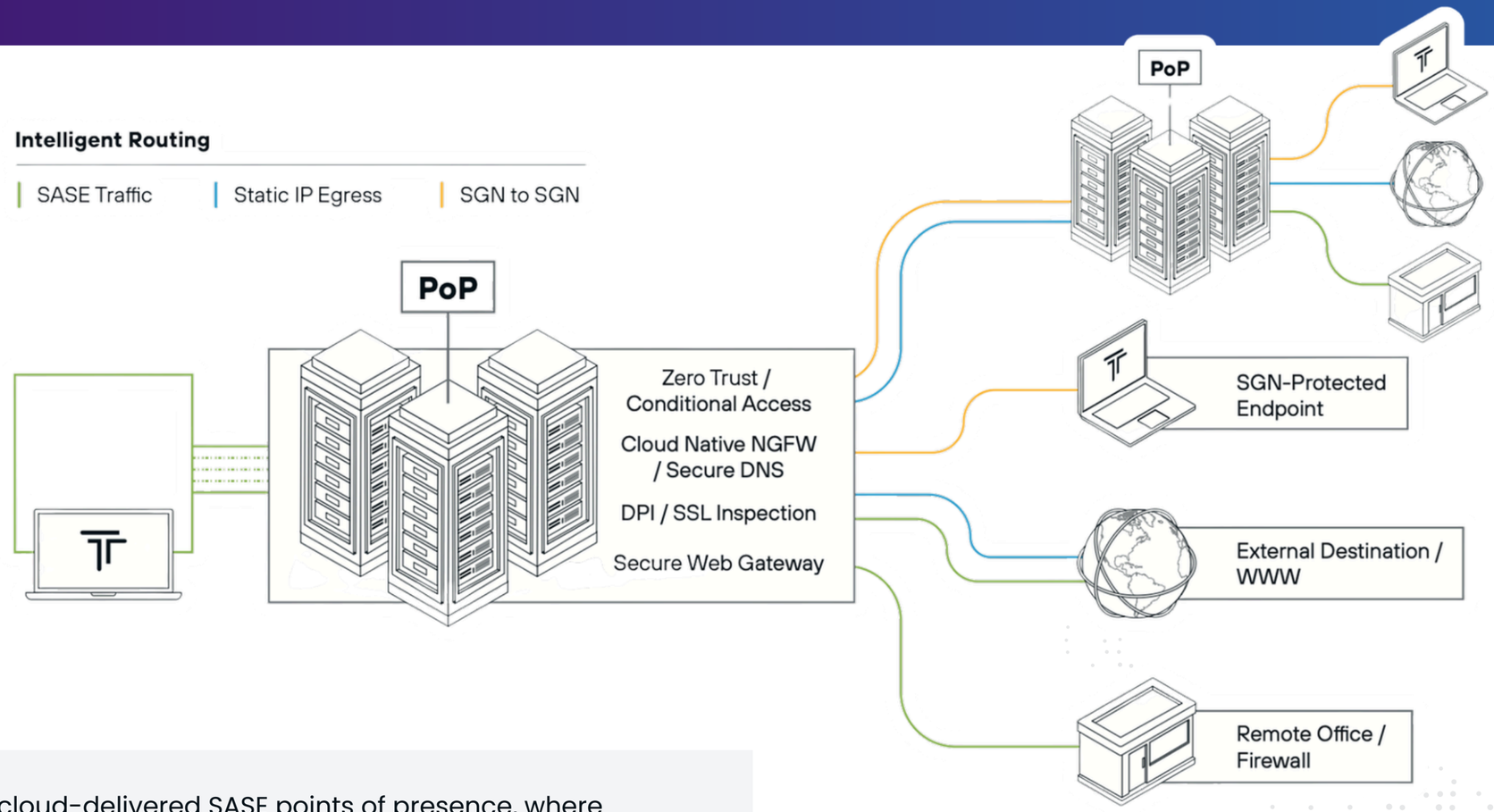


Figure 1. SASE Traffic Routing and Security Enforcement Architecture

> User and network traffic is routed through cloud-delivered SASE points of presence, where identity verification, security inspection, and policy enforcement occur before access is granted.

Understand What Changes

continued

Instead of granting users access to a network after connecting through a VPN, SASE platforms connect users directly to authorized applications while continuously verifying identity, device health, and access policies.

This security model reduces the risk of lateral movement inside the network while improving visibility into user activity.

By eliminating broad network-level access and replacing it with application-specific access, SASE ensures that even if credentials are compromised, attackers are unable to move freely across systems.

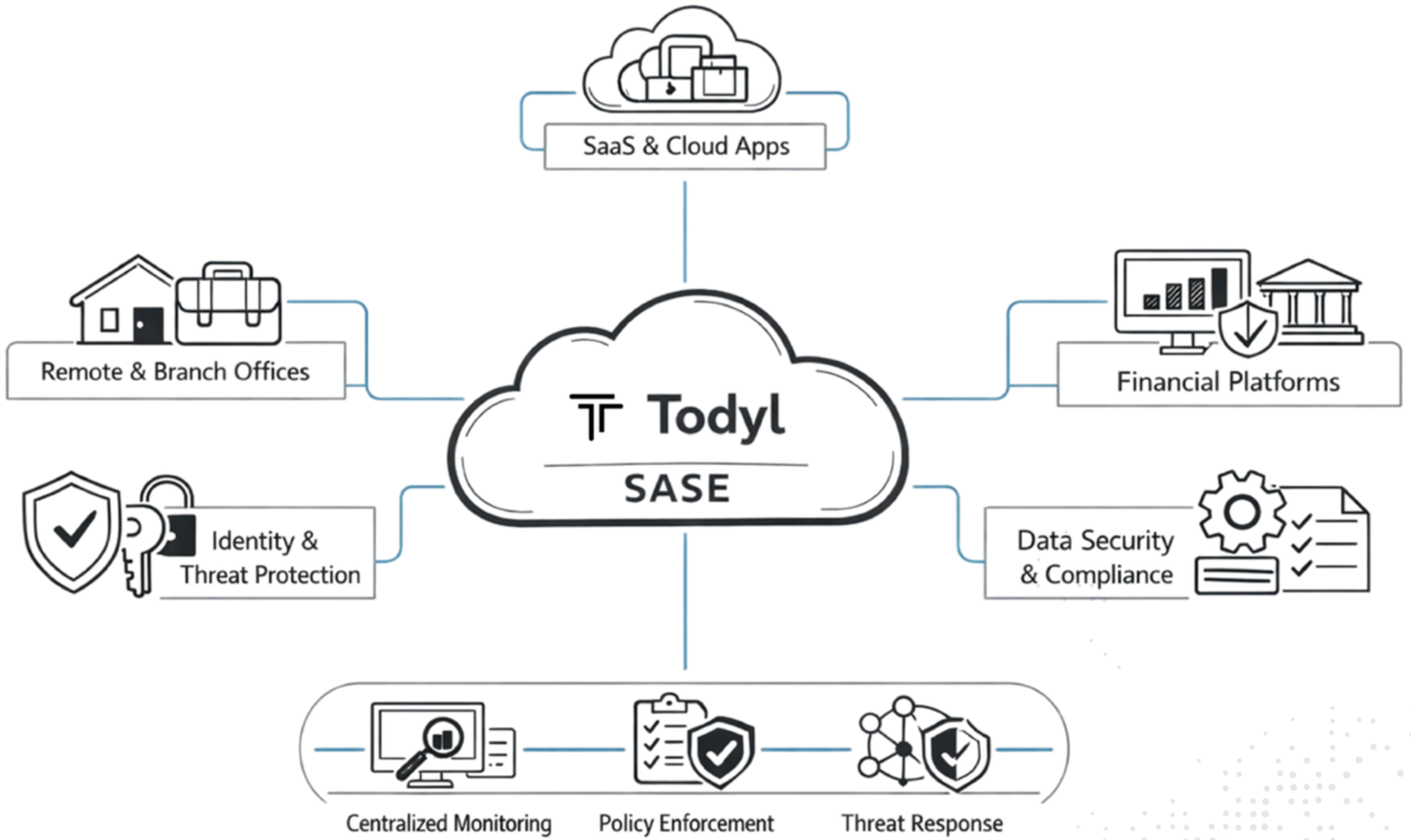
Traditional VPN Models	Identity-First SASE Models
Users connect to the network	Users connect directly to applications
Network-level access	Application-level access
Perimeter-based trust	Continuous identity verification
Multiple security tools	Consolidated security platform
Hardware appliances	Cloud-delivered security

> Unlike VPN-based access, where a single compromised credential can expose large portions of the network, SASE limits access to only what the user is explicitly authorized to use — significantly limiting what an attacker can reach, even if credentials are stolen.

Understand What Changes *continued*

The following illustrates how SASE platforms unify access, security, and monitoring across distributed environments.

Figure 2. Identity-First SASE Platform for Secure Access and Compliance



A unified SASE platform connects users to applications, financial systems, and data environments while enforcing identity-based security, monitoring, and compliance controls.

Understand What Changes

continued

A core component of the SASE model is Zero Trust Network Access (ZTNA), which restricts users to only the specific applications they are authorized to access, rather than exposing the broader network. This approach reduces lateral movement and limits the impact of compromised credentials or devices.

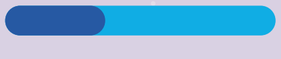
And for firms with compliance obligations, identity-first platforms also centralize access logs and monitoring data, strengthening both threat detection and audit-ready documentation.

But centralized visibility only matters if your team can act on it quickly — and for many firms, that remains the challenge. Omega's research shows that:

- 37% of firms say it would take a week or longer to detect and contain a breach
- 6% estimate detection could take a month or more

For an RIA's clients, investors, and regulators, a week-long window of undetected access is rarely a recoverable situation. Fragmented infrastructure often contributes to these delays. Security telemetry may be distributed across multiple systems, including VPN appliances, firewalls, cloud applications, and endpoint security tools.

SASE platforms consolidate these controls and monitoring capabilities into a unified architecture.



37%

of firms say it would take a week or longer to detect and contain a breach, indicating that many organizations face delays in identifying and responding to threats.

6%

of firms estimate detection could take a month or more, highlighting how extended timelines can further slow response and containment efforts.

Omega Systems'
2025 Financial Services
Cyber Resilience Report

Stage 4: Evaluate Your Options

Not Every Deployment Model Fits a Firm Your Size

Choosing SASE is one decision. How it gets implemented is another.

Many platforms were originally designed for large enterprises with dedicated internal security teams. Wealth management firms with 10–500 employees often require a different operational model.

Omega's research highlights the operational gap between internally managed environments and those supported by managed security partners.

Organizations relying solely on internal IT teams are 56% more likely to experience 25 or more attacks annually and report lower confidence in detecting advanced threats.

This has led many firms to adopt **managed SASE models** that combine cloud-native infrastructure with operational oversight.

Deployment Approach	Typical Characteristics
Enterprise SASE platforms	*Powerful but require dedicated security teams and longer deployment timelines*
DIY multi-vendor architecture	*Flexible but operationally complex*
Managed SASE platforms	*Provider deploys, monitors, and maintains security oversight*

> For mid-sized financial firms, architecture alone does not determine resilience. Operational oversight is equally important.

Evaluate Your Options

continued

Omega Systems partners with **Todyl**, a cloud-native security platform provider specializing in identity-first SASE architecture, to deliver managed deployment, monitoring, and policy management.

Through a unified, cloud-native platform designed for mid-market organizations, financial services firms can operate with the same caliber of security used by much larger institutions — without needing to build or staff an internal security team to run it.

It also improves the day-to-day user experience by removing reliance on unstable VPN connections, enabling more consistent and performant access to cloud-based applications.

Learn more about Todyl's underlying SASE platform here.

Stage 5: Ask the Right Questions

What to Evaluate Before Choosing a Security Platform

When evaluating SASE solutions, wealth management firms should focus on a few key questions.

Identity Verification

Does the platform verify both user identity and device security posture?

Network Exposure

Does this approach eliminate or reduce reliance on exposed VPN models?

User Experience

Does the platform reduce latency and eliminate reliance on manual VPN connectivity?

Application Segmentation

Can users access only the systems required for their role?

Deployment Timeline

Can implementation occur without major infrastructure redesign?

Visibility & Monitoring

Are activity logs centralized for investigation and compliance audits?

Operational Management

Who maintains policies, monitoring, and ongoing optimization?

> These criteria help firms determine whether a SASE platform strengthens operational resilience or introduces unnecessary complexity.

Close the Gap:

The Path to Security That Protects Your Firm, Clients and Reputation

Financial services firms now operate in an environment defined by continuous cyber activity, distributed work models, and expanding regulatory expectations.

Research shows that cyber incidents are widespread, detection timelines remain challenging, and many organizations still rely on manual compliance processes.

The traditional perimeter model was designed for centralized offices and internal networks. Wealth management firms today operate across cloud platforms, remote advisors, and interconnected third-party systems.

Secure Access Service Edge reflects the market's response to this shift. By moving from location-based trust to identity-based verification, SASE architectures align security controls with how firms operate today.

For wealth management firms seeking stronger protection, clearer visibility, and a seamless hybrid user experience, this is no longer a technology decision – it's an operational one. The firms that address it proactively will be better positioned to protect client trust, meet regulatory expectations and weather the next threat.

Explore SASE for Your Environment

If anything in this guide resonated with you, it's worth a conversation. Connect with the Omega Systems team to talk through what the right approach looks like for your firm.

omega systems
technology managed

About Omega Systems

Omega Systems is a trusted managed service provider (MSP) and managed security service provider (MSSP) supporting financial services and other regulated industries across the United States, including RIAs, family offices, private equity firms and other wealth management practices.

Founded in 2002, Omega combines managed IT services, cybersecurity operations, cloud infrastructure, and governance support to help financial firms strengthen operational resilience and maintain compliance in increasingly complex threat and regulatory environments.

Through its security operations capabilities and integrated technology solutions, Omega helps firms modernize their IT and security architecture while maintaining the visibility, control, and accountability required in regulated industries.

in partnership with

todyl

About Todyl

Todyl is a cloud-first security platform provider specializing in identity-first SASE architecture. Todyl's platform delivers secure, reliable access to the applications and systems your team depends on — from any location, on any device — without the complexity and risk exposure of traditional VPN infrastructure.

learn more at **www.omegasystemscorp.com**

call us at (866) 611-9998 and select #3