Securing the Post-AI World for Financial Services with Zero Trust

A strategic approach to cybersecurity in the age of AI

Solution Brief

Executive Summary: Navigating the dark forest

In a post-AI world, financial services must navigate a "dark forest" of hidden threats and uncertainties, where every interaction could pose a risk. Just as one would exercise extreme caution in a dangerous and unpredictable environment, financial services must approach AI security with vigilance. This brief outlines the steps financial services organizations can take to protect themselves as they enter this AI-driven landscape.

We'll explore how AI is reshaping the threat landscape, introducing new vulnerabilities such as AI-powered fraud and automated cyberattacks. Additionally, we'll highlight key trends and predictions, helping organizations anticipate AI's impact and strategically respond.

The best defense in this high-risk environment, where no entity—inside or outside the organization—can be trusted is zero trust. This brief provides a clear path for financial services organizations to begin their zero trust journey, offering actionable steps to ensure a secure and resilient AI future.

AI and the evolving threat landscape

AI is rapidly transforming the threat landscape, introducing complex risks that challenge traditional security models. Attacks have evolved and become more effective at scale, allowing victims to continue to operate while attackers threaten to expose their data. Although there are many AI mega trends and predictions, we're going to look at three trends for 2024-2025 that have been evolving at a faster rate.

2024-2025 Three Trends to Watch

Main sequence AI development

AI large language models (LLMs) have transformed how we think about generative AI by expanding its capabilities beyond narrow, task-specific outputs to more dynamic, context-aware solutions. But just like the real world, everything including AI will continue to evolve. These LLMs have grabbed us once it crossed the uncanny valley.

The uncanny valley refers to the unsettling feeling people experience when AI becomes almost—but not quite—indistinguishable from humans, creating a sense of discomfort due to its near-perfect imitation.

GenAI and ChatGPT in particular, crossed the uncanny valley once it hit 100 million users in two months, which is remarkable. Now that it has crossed the uncanny valley, there is more coming which may have more impact from a neurological perspective, from a pursuit of cognition perspective than just GenAI.

Encryption-less ransomware attacks

Previously encryption was used for ransomware, it drove the top agenda—steal your data, hold your operation ransom, and if you don't pay you can't run your business.

However, over time, ransomware attackers have realized that if you lower the amount of money you're seeking, and if you don't prevent your victim from doing business you'll get a higher yield. So for example, let's say they bring the ransom down from $10 million to $2 million and you go from a 5% chance of paying to a 70-80% chance of paying—it becomes a "better" ransomware business model at scale. This is encryption-less ransomware.

In encryption-less ransomware they take the data, they threaten you and in many cases will allow you to continue operations because they don't want to stop your business. By not disrupting the business, less reputational damages may occur. Attackers may also try to convince the victim to not disclose the ransom to the SEC/regulator because it's not material enough.

AI-powered ransomware attacks

AI-powered ransomware attacks are more effective at improving the yield, penetration and automation of the attacks. In this case, attackers leverage AI to automate and enhance the sophistication of cyberattacks, making them faster, more targeted and harder to detect.

Four ways financial services can navigate the evolving AI landscape

The use of enterprise AI is soaring, along with the risks. The four levels of corporate strategic consideration can guide financial services organizations in navigating the complexities of an ever-evolving post-AI world.

In 2024, the use of AI/ML tool usage grew by 594% and the use of ChatGPT grew to 634% (Zscaler ThreatLabz 2024 AI Security Report).

Policy & Ethics

Financial services must develop comprehensive policies that govern the ethical use of AI, ensuring compliance with regulation and fostering trust with customers. This involves creating a framework that addresses data privacy, algorithmic transparency, and bias mitigation, emphasizing responsible AI practices.

Core business

How does AI impact the core business? The Harvard Business Review did a study that showed a statistically meaningful difference in the performance of businesses that use AI versus those that don't in a given industry, and that that gap is continuing to widen.

So how are you going to bring AI into the business? Are you going to this with a partner or are you going to do things in a private sense? Are you going to own your own models? Are you going to partake in larger models? And what is the use case involved?

Organizations should evaluate how AI can enhance their core business operations, such as improving customer services, optimizing processing, and enabling data-driven decision-making.

Organizations should evaluate how AI can enhance their core business operations, such as improving customer services, optimizing processing, and enabling data-driven decision-making.
By identifying key areas where AI can add value, financial services organizations can create competitive advantages and drive innovation that aligns with strategic goals.

R&D and infrastructure

As AI tools come into the business, how do you deal with them? Investing in robust infrastructure that supports AI capabilities—such as cloud computing, big data analytics, and machine learning—will enable organizations to leverage emerging technologies and develop new solutions to meet changing customer needs.

Cybersecurity advantages

Financial institutions can enhance their cybersecurity posture by utilizing security solutions that leverage AI to identify and respond to threats in real-time.

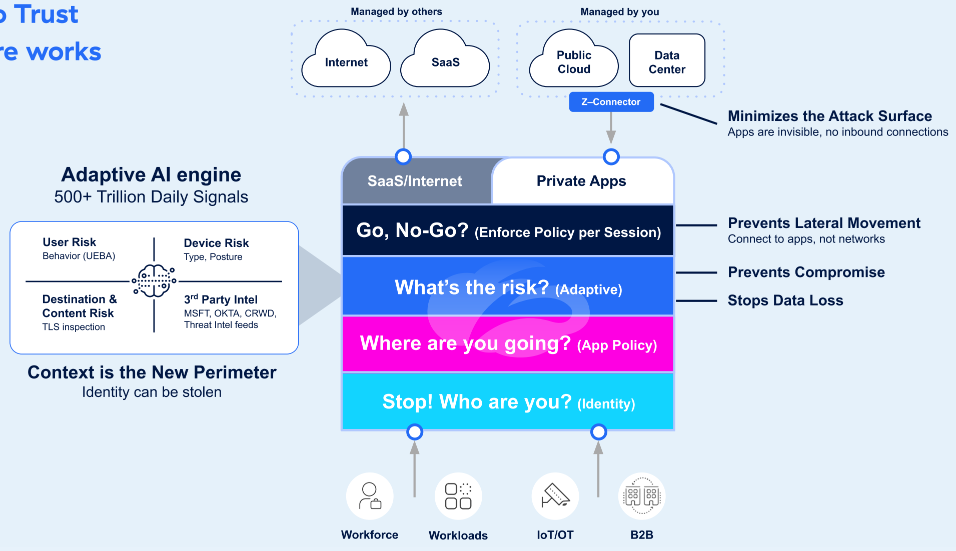
You should ask yourself, what are the advantages for AI and cybersecurity or potentially the threats? How is it going to be used against you? How can you prepare for that? By implementing AI-driven security measures, organizations can better protect sensitive data and assets, and ensure resilience against sophisticated threats.

The role of zero trust in reducing cyber risk

Even as enterprise AI usage accelerates, enterprises block **18.5%** of all AI transactions, a **577%** increase signaling rising security concerns. (Zscaler ThreatLabz 2024 AI Security Report) the best defense in this high-risk environment, where no entity—inside or outside the organization—can be trusted is zero trust.

Zero trust is the strategy that helps us navigate the dark forest by only allowing what the business needs when it needs it. Implementing a trust no one zero trust approach ensures that regardless of user, workload, device or another company you can significantly reduce cyber risk:

How a Zero Trust Architecture works


Managed by others
Internet
SaaS
Managed by you
Public Cloud
Data Center
Z-Connector
Minimizes the Attack Surface
Apps are invisible, no inbound connections
Adaptive AI engine
500+ Trillion Daily Signals
User Risk
Behavior (UEBA)
Device Risk
Type, Posture
Destination & Content Risk
TLS inspection
3rd Party Intel
MSFT, OKTA, CRWD, Threat Intel feeds
Context is the New Perimeter
Identity can be stolen
SaaS/Internet
Private Apps
Go, No-Go? (Enforce Policy per Session)
What's the risk? (Adaptive)
Where are you going? (App Policy)
Stop! Who are you? (Identity)
Prevents Lateral Movement
Connect to apps, not networks
Prevents Compromise
Stops Data Loss
Workforce
Workloads
IoT/OT
B2B

1. Authenticate identity: Stop! Who are you?

a. Who is connecting?
b. What are the attributes?
c. Where is the connection going?

2. Control app policy: Where are you trying to go?

a. Where are you trying to go? In this step, zero trust assesses risk using context, preventing compromise and data loss.

3. Adaptive contextual risk: What is the risk?

a. What is the risk? Prevent compromise and stop data loss by evaluating the user risk, device risk, destination, content risk, and third-party intel (Okta, CrowdStrike, etc.).

4. Enforce policy

a. Prevent lateral movement so you connect to apps, not networks
b. Enforce policy for both SaaS/internet connection based on a per-session, per-user basis
c. Private applications—minimize attack surface so that apps are invisible and no inbound connections can happen.

A zero trust journey

To secure your business against the growing number of cyberthreats powered by AI, embarking on a zero trust journey is essential. Implementing a zero trust journey should be seen as a gradual process, broken down into manageable steps that align with business priorities and security goals—ensuring your security evolves in a way that is both scalable and resilient.

1. Secure the workforce

a. Phase 1A—no network changes
  i. Cyber and data protection, digital experience, and quantify risk
b. Phase 1B—network simplification
  i. Zero trust branch office/internet café, advanced cyber and data protection strategy, and gain business insights

2. Secure workloads

a. Cyber and data protection for workloads
b. Zero trust workload networking and segmentation

3. Third-party access

a. Zero trust third-party app access
b. Zero trust third-party site connectivity

4. Secure devices (IoT/OT)

a. Cyber and data protection for IoT/OT
b. Zero trust IoT/OT connectivity

Conclusion

Zero trust offers the best defense in this fast-evolving landscape, where no entity—inside or outside the organization—can be inherently trusted. As technology and AI continue to evolve and eventually arrive concurrently, adopting a zero trust strategy ensures that only the right users and processes access what's needed, when it's needed—ensuring you can remain resilient and future-proof your organization.

Reduce your cyber risk, begin your zero trust journey by learning more at www.zscaler.com

Meet the Author

With 3+ decades as an entrepreneur, infosec expert and executive at companies like RSA, Arbor Networks, CA, McAfee, Cbyereason, and more, Sam is dedicated to empowering defenders in cyber conflict and fulfilling the promise of security, enabling a safe, reliable, connected world. Currently, Sam Curry is the Global VP, CISO at Zscaler and in his spare time he is a public speaker, hosts a podcast (On the Hook), sits on various boards and publications, and is an InfoSec mentor. Connect with me on LinkedIn.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com