zscaler | CXO REvolutionaries

Five Steps for Financial Services to Win at Cyber

Editor's note: The following is based on material presented at a recent Wall Street Cybersecurity Summit.

Knowing you would like to implement zero trust and implementing it are two different things. Zero trust is not a plug-and-play solution; it's a journey that requires validating every connection – user to app, app to app, or process to process. Financial services firms rely on zero trust to secure everything from online banking to internal trading systems and claims processing apps.

Legacy castle-and-moat security products (VPNs, firewalls) were never designed for the cloud and are unable to adequately protect financial institutions, customers, and partners. As leading financial organizations work to achieve digital transformation, they require a proven zero trust platform that will reduce business risk, lower cost/complexity, and increase productivity.

Zscaler, a leading cloud security provider, enables a zero trust approach helping companies to obscure their attack surface, prevent lateral movement, and provide direct access to resources on a per-session basis – without putting users or applications on the corporate network.

In short, never trust, always verify.

Many of the challenges associated with a large initiative like zero trust in financial services are not technical issues, but stem from driving organizational change. There are significant interpersonal and organizational components that must be carefully considered. Over the course of my career, which included technology leadership positions in financial services, I have had the opportunity to work on many "big word projects" ranging from AI to cloud, and of course, zero trust. What follows are some of my top tips for ensuring financial services companies win at cyber by successfully influencing key stakeholders.

How to win at cyber in five easy steps

1. **Organizational Partnership**
   Zero trust is a team sport. Successfully transforming a financial institution's security posture requires you to align with key stakeholders early. Each department plays a critical role:

   - The **Chief Technology Officer (CTO)** is often focused on the infrastructure: design, maintenance, configuration, execution & technology strategy

   - The **Chief Information Security Officer (CISO)** knows and owns the security strategy and ensures regulatory compliance.

   - The **Chief Information Officer (CIO)** is focused on day-to-day operations and how zero trust approaches improve application security as well as the overall end-user experience, whether it's for mobile banking apps or e-payment platforms.

   - The risk leader, like a **Chief Risk Officer (CRO)**, confirms the technology group is covering all the risks to the organization and end-consumer

Bringing the CTO and CISO together on a common goal of zero trust and then inviting the risk leader along on the journey is a huge step in your success. Establishing a rhythm of these leaders with the CIO brings it all together. These roles might be slightly different in your organization, but understanding each stakeholder's responsibilities, motivations, and goals and connecting them before the project begins is key.

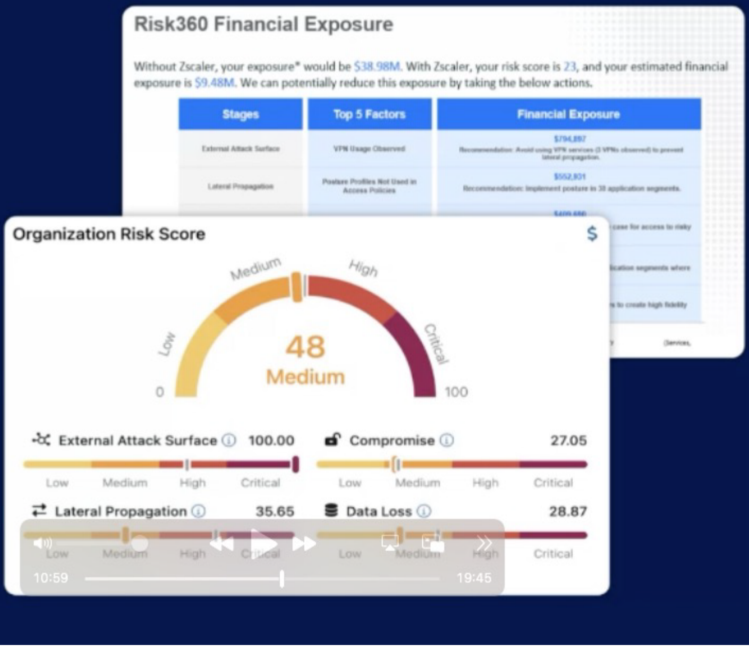
2. **Communication and board-level metricss**
   Once key leaders are aligned behind your zero trust initiative, you need the backing of your board. The board doesn't need to hear all the technical jargon but wants to understand how zero trust will mitigate risk such as regulatory fines, data breaches, or reputational damage.

   For example, regularly presenting a comprehensive risk score that reflects the organization's exposure to threats – and tying that score to business impacts like operational disruption or customer data loss — is invaluable in financial services. Once you've established this score, continue to revisit it along each phase of your initiative to demonstrate maturity backed by real-world data from your environment.

Communication and Board Level Metrics – AI and Risk 360 can help

CLEAR COMMUNICATION of how the organization is improving its cyber risk position

COMPARE to industry peers with an always CURRENT view of the cyber risk



Risk360 Financial Exposure

Without Zscaler, your exposure* would be $38.98M. With Zscaler, your risk score is 23, and your estimated financial exposure is $9.48M. We can potentially reduce this exposure by taking the below actions.

Stages	Top 5 Factors	Financial Exposure
External Attack Surface	VPN Usage Observed	$794,897 Recommendation: Avoid using VPN services (3 VPNs observed) to prevent lateral propagation.
Lateral Propagation	Posture Profiles Not Used in Access Policies	$552,931 Recommendation: Implement posture in 38 application segments.

Organization Risk Score

External Attack Surface 100.00

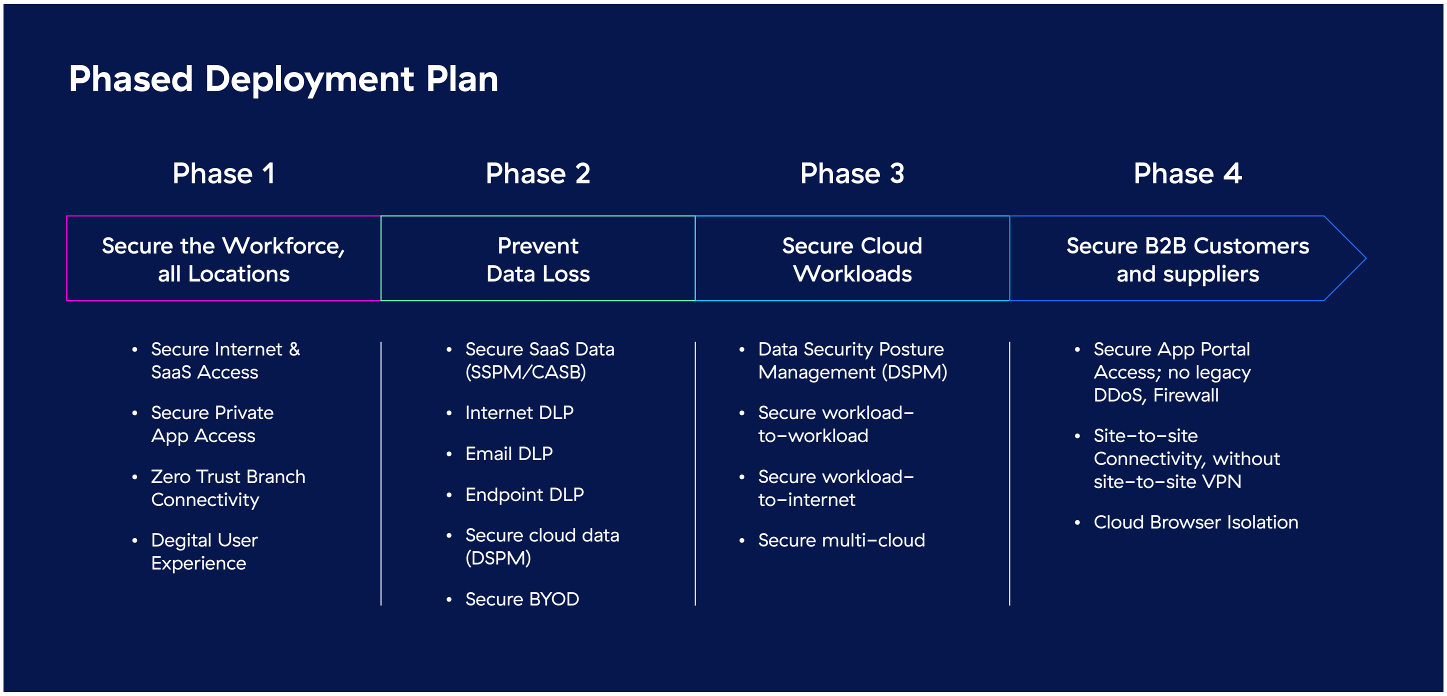
Compromise 27.05

Lateral Propagation 35.65

Data Loss 28.87

3. **Phased deployment plan**
   At Zscaler, we believe your approach to zero trust should be gradual, broken down into manageable initiatives. This is even more relevant in financial services, where hybrid IT environments, third-party vendors and sensitive data make digital transformations complex. It's no accident we speak about zero trust as a journey, one that rarely unfolds along a straight line. Transformation initiatives often begin in response to a stimulus — implementing a VPN replacement or incorporating a new acquisition into existing IT systems, for example — and then maturing over time.

One thing is critical, though: developing a plan that incorporates individual use cases into an overarching strategy for deployment. The sample plan I've created below almost certainly won't map perfectly to your organization's needs, but it is an example of a phased deployment that takes care to avoid the feeling of needing to "accomplish" zero trust overnight.



Phased Deployment Plan

Phase 1	Phase 2	Phase 3	Phase 4
Secure the Workforce, all Locations	Prevent Data Loss	Secure Cloud Workloads	Secure B2B Customers and suppliers
• Secure Internet & SaaS Access • Secure Private App Access • Zero Trust Branch Connectivity • Degital User Experience	• Secure SaaS Data (SSPM/CASB) • Internet DLP • Email DLP • Endpoint DLP • Secure cloud data (DSPM) • Secure BYOD	• Data Security Posture Management (DSPM) • Secure workload–to–workload • Secure workload–to–internet • Secure multi–cloud	• Secure App Portal Access; no legacy DDoS, Firewall • Site–to–site Connectivity, without site–to–site VPN • Cloud Browser Isolation

4. **Pragmatic technical deliverables**

Throughout my career I have encountered a number of CXOs with impeccable strategic instincts who nevertheless struggle to translate them into pragmatic deliverables. When we're dealing with complex concepts, like the cloud, or zero trust, it's easy to get lost in the weeds

It's critical that tactical actions like a VPN replacement are framed in terms of the business and security problems they solve. For example, an insurer replaced their VPN with an integrated zero trust solution for remote claims adjusters, resulting in faster access to data, enhanced security and reduced operational costs. I return to the VPN example because it is a perfect illustration of enhancing security and the user experience, making it a model IT solution for a business issue. Users become more productive and benefit from a smoother experience, the opportunity for lateral movement is reduced, and cost savings are likely to accrue.

5. **Fix the basics**
   It may sound simple, but it's a critical point that I have often seen overlooked: You must tackle the low-hanging fruit, or threat actors will do it for you. So, what are the basics? Phishing remains the top threat for financial services, accounting for many breaches. Creating a culture of security within your organization is critical. I don't mean in terms of high-tech solutions, but by fostering basic cybersecurity literacy organization-wide. With the advent of AI-assisted phishing, this will only become more critical in the near future.

   Zero trust is a mature approach that will uplevel your organization's security, whether you're starting from scratch or looking for a more comprehensive implementation. By taking these steps, your financial services organization can align with regulatory demands, protect customer data, and ensure resilience in the face of evolving threats.

To evaluate your organization's transformation journey, take the CXO REvolutionaries digital transformation assessment.

Meet the Author

Greg Simpson
Chief Technology Officer (Retired), Synchrony

Greg is an experienced technologist having been CTO at numerous GE businesses, and GE Overall. As CTO of Synchrony, Greg first launched the foundational infrastructure to support their IPO and then drove a transformation built on a strategic technology stack that was built on the cloud, a new data lake, application API's and AI, enabling faster solution delivery for Synchrony customers. He also was instrumental in their transformation to a work from home culture during the pandemic, leveraging solutions like Zscaler to deliver the security and performance necessary to successfully move the business forward to a new way of working.