Zero Trust: Security in the age of the porous perimeter

Many financial services organizations are taking a Zero Trust approach to cybersecurity. This framework is designed to help secure the ubiquitous nature of modern enterprises. It lays the foundation to help organizations meet the challenges caused by evolving business models, shifting workforce dynamics, and complex IT environments.

Zero Trust adoption may seem daunting, but it doesn’t need to be. Explore five insights and actions to help you take an incremental approach that alleviates the potential for operational disruption and drives down risk.

### 5 things you should know

1. Cyber resilience is top of mind for many financial institutions due to the proliferation of destructive cyberattacks (e.g., ransomware) and increasing regulatory oversight. The need for financial organizations to effectively respond to and recover from a breach is imperative for individual organizations and the industry as a whole.

2. Financial service institutions are operating increasingly complex IT ecosystems with globally distributed operations, including remote workforces and third-party connectivity, which are contributing to a challenging risk landscape.

3. Many financial institutions are accelerating cloud adoption to compete with fintech entrants and support consumer-led demand for transformed and digital banking experiences. The need to secure and manage hybrid and multicloud environments alongside legacy infrastructure can lead to increased complexity, operational overhead, and talent and skills challenges.

4. Cyber due diligence, including adversarial simulation, and threat profiling should be conducted during merger and acquisition (M&A) transactions in order to enhance situational awareness of relevant threats and weaknesses that inform the adoption of leading IT integration practices.

5. There is an increase in regulatory oversight for financial service institutions, especially on the topics of geospecific data sovereignty and privacy requirements.

### 5 actions you can take

1. Implement network segmentation and microsegmentation to limit the blast radius of potential attacks. Start with baselining the environment by leveraging telemetry and analytics to enhance visibility. Then take a phased approach and implement coarse-grained environmental segmentation (e.g., production versus nonproduction) before moving to fine-grained segmentation (e.g., microsegmentation, application ringfencing).

2. Enforce least privilege and dynamic access control for identities, including employees, service accounts, customers, and third parties. Consider centralizing access control decisions and challenge each user and device through continuous monitoring and anomaly detection. Additionally, reduce static access and drive toward dynamic “just-in-time” access to enhance control during breaches.

3. Implement the appropriate security controls and guardrails as foundational elements in cloud environments before migrating workloads. Account for operational implications by harmonizing the technology stack across cloud and legacy environments, enhancing automation and orchestration, protecting privileged accounts, addressing cloud configuration issues, and protecting data at rest and in motion.

4. M&A can introduce complexity during the integration or divestiture of entities. Modern capabilities such as software-defined perimeter (SDP) or secure access service edge (SASE) can be leveraged to enable secure Zero Trust Network Access (ZTNA) for enterprise resources while maintaining consistent and broad cybersecurity controls aligned to Zero Trust guiding principles.

5. Enforce data inventory, classification, and governance capabilities to understand where data resides, its criticality, how to protect it, and who and what should have access to it. This can support compliance with data sovereignty and privacy laws while enhancing overall data risk posture.

Learn more from these additional resources
Zero Trust: Never trust, always verify Zero Trust strategy insights

Connect with us
ANDREW RAFLA
Principal, Zero Trust offering leader
Deloitte & Touche LLP
arafla@deloitte.com

KIERAN NORTON
Principal, Infrastructure Solution offering leader
Deloitte & Touche LLP
kinorton@deloitte.com

MARK NICHOLSON
Principal, Financial Services Industry Cyber leader
Deloitte & Touche LLP
manicholson@deloitte.com

STEPHEN MARTIN
Senior Manager
Deloitte & Touche LLP
smartinrajan@deloitte.com

This publication contains general information only and Deloitte Risk & Financial Advisory is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decisions or taking any action that may affect your business, you should consult a qualified professional only.

Deloitte Risk & Financial Advisory shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, “Deloitte Risk & Financial Advisory” means Deloitte & Touche LLP which provides audit, assurance, and risk and financial advisory services; Deloitte Financial Advisory Services LLP, which provides forensic, disputes, and other consulting services; and its affiliate, Deloitte Transactions and Business Analytics LLC, which provides a wide range of advisory and analytic services. These entities are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2022 Deloitte Development LLC. All rights reserved.