UNISYS | Securing Your Tomorrow®

# EMBRACE OPEN BANKING WITH RISK-RELEVANT SECURITY SOLUTIONS

## ABOUT THE AUTHOR

*Stephen Migliore, global head of cybersecurity for financial services at Unisys, has more than 25 years of global management, business development and consulting experience, delivering innovative, industry-aligned security solutions and services to support clients around the world.*

*Contact him at Stephen.Migliore@unisys.com or connect with him at Linkedin.*

Open banking presents tremendous opportunities for the financial services industry. It opens the door to products, services, features, and benefits that banks and financial services firms might otherwise have no way of offering to their customers. With those opportunities, however, comes increased risk. Addressing that risk is essential if institutions are to embrace open banking with confidence.

## Interconnectivity and Risk

Open banking increases risk by multiplying the interconnectivity between banks, providers, partners, vendors, and customers. This interconnectivity introduces systemic risk. For instance, a security incident at one financial institution has a much greater likelihood of propagating to other businesses if they are connected via open APIs. Interconnectivity also enables bad actors to gain access to a bank's core systems and databases via a connection with a third-party.

Banks need to approach security differently to ensure protection of systems, data, and customers. Perimeter defenses are completely insufficient to respond to this new type of systemic risk. The perimeter is porous – if it exists at all. This does not come as a surprise: the IT perimeter has been getting more and more porous for years as business has surged across virtual connections and into the cloud. Open banking is simply punching yet more holes into a perimeter that already looks like Swiss cheese.

To combat the systemic risk that comes with open banking, security professionals need a new approach and a new solution. That comes in the form of a Zero-Trust security model.

## Understanding Zero-Trust

Zero-Trust is a hot topic today. Like many new terms, it can mean different things to different companies. At Unisys, we understand Zero-Trust in this way: it is a security approach which treats everyone as an insider.

The reason a Zero-Trust approach is necessary with open banking is because interconnectivity with partners, vendors, and customers means that every person could theoretically gain access to sensitive data. Not that such access is purposefully granted, but the connections exist that make access possible. There is no perimeter to keep people out.

Zero-Trust also recognizes that, in addition to internal or external malicious actors, perfectly well-meaning employees can accidentally do bad things from time to time, whether that is clicking on a link in a phishing email or inadvertently exposing information. With no ill intention at all, such accidents can result in data breaches, regulatory audits and fines, fraud, and reputational brand damage.

*A user must have his or her identity authenticated via security protocols such as biometrics in order to gain access to the data that is appropriate for their role.*

## Three Components of Zero-Trust Security

A Zero-Trust security model has several components. The first is **identity-driven access**. Verified identity – not a device or role – is the key that unlocks access to information. A user must have his or her identity authenticated via security protocols such as biometrics in order to gain access to the data that is appropriate for their role. For example, once verified, a bank customer would be granted access to his account, whereas a bank employee would be granted access to the various systems that pertain to her job.

Zero-Trust security requires the use of **machine intelligence, behavioral analytics, network analytics**, and other advanced technologies to detect and respond to anomalous activity more quickly than is possible for people. People can easily miss seeing a problem, particularly in its early stages. That same problem can be instantly identified in its nascent form through tools such as artificial intelligence, dramatically reducing the mean time to detect. In like manner, the mean time to respond – which may be hours, days, or even weeks when reliant upon people – can be near real-time when the system can automatically respond to address a breach, attack, or other questionable activity.

Finally, a Zero-Trust approach requires **dynamic isolation**. That is, once a problem is identified, it needs to be stopped in its tracks before it spreads. For example, if a piece of malware is pinpointed, the system needs to be able to quarantine the affected area before the malware explodes to take down the entire company. Or again, if a user suddenly starts engaging in unusual activities – such as accessing large amounts of personally identifiable information – the system needs to be able to shut the user out instantly. It is critical that dynamic isolation take place in real-time, as opposed to waiting for a security professional to see and respond to the issue. Given the speed at which attacks occur or problems expand, the slightest delay can have devastating ramifications.

By leveraging identity-driven access, advanced technologies, and dynamic isolation, banks and financial institutions can leverage a Zero-Trust security model to counter the systemic risks that open banking introduces. Connections with strategic vendors and partners can then be made with confidence, and the full benefits of open banking can be realized.

**To learn more visit www.unisys.com/Elevate**

For more information visit www.unisys.com



Printed in the United States of America 04/19 19-0183