# Designed to Fail

By Lou Senko, SVP and CIO, Q2

There's an aging notion that security requirements add friction to the code-to-customer delivery cycle, and that it can't be helped. Some accept the friction and suggest that slowing things down and adding processes will result in a better, safer, customer experience.

I disagree with both sentiments—that security *must* add friction and that deceleration is necessary for security. I think if we can trust our security and testing, avoid issues early, and implement fixes sooner, we can move even faster. It's just a matter of proactively reducing risk, employing strong, smart security solutions, and intelligent testing—all working together. With a multilayered approach, no single layer's failure results in a security breach. In a sense, each layer is designed to fail—or to allow for the inevitable—while still providing exceptional security.

In this article, we'll explore security postures digital services providers can take from a technical standpoint, illustrating the benefits to IT teams that can be applied as industry best practices (and provide financial institutions (FIs) some insight into the conversations they should be having with their digital services providers).

## Security Through Layers

For some digital services providers, increasing market presence and rapid technology adoption can result in attack surface expansion that increases at logarithmic rates. As these factors scale, the importance of a layered approach to threats can't be overstated. Many environments now include presence in datacenters and the public cloud, access from users coming to services over the internet, and employees managing those services from connected corporate networks (including the remote workforce).

To add complexity, digital services providers are defending against threats that are both internal and external:

- Over 8,000 breaches occur yearly; 35% can be traced to insiders; nearly half are accidental.
- Software vulnerabilities have increased by 22% over the last year.
- Phishing attacks have increased by 300%, DDoS attacks have increased by 200%, cyberattacks against the financial sector have increased by 238% since the COVID-19 pandemic pushed the workforce to remote work.
- Ransomware represents a prevalent technical threat targeting employees; 46% of attacks are from a new variant, and 59% of victims are using up-to-date security. New ransomware strains don't just lock environments. They exfiltrate the data first, forcing victims to pay ransom to unlock their environment and prevent stolen data from being exposed.

## Security Through Solutions

The goal of security isn't to eliminate risk, but to appropriately tolerate certain kinds of risk while mitigating the rest. With this in mind, there are a number of adjustments digital services providers can make to mitigate risk. Some companies that provide digital banking services have merged security and operations, since everyone who touches production also shares the responsibility of ensuring and maintaining security. Adopting this strategy can help the provider execute against a purposeful roadmap for maturing its capabilities:

- Digital banking services providers must evolve alongside FIs' security, compliance, risk, and fraud teams. Security engineering and tools team should consider building out Application Security functions within their DevOps team, adding Security Incident Response functions, even establishing further approaches such as establishing a Security Operations Center and a fraud assist team. It may be critical for digital services providers to build out security architecture featuring an insider-threat and threat-intelligence platform to provide the airtight security FIs demand.
- Implementing respected industry frameworks may also serve to elevate a service provider's posture, which can help apply a new tool while better defining the problem/control statement. Service providers should also keep their eye on mastering the five levels of the new Cybersecurity Maturity Model Certification (CMMC), in order to evolve from practicing 'good cyber hygiene' to executing enhanced practices to detect and respond to advanced persistent threats (APTs).
- Technology stacks should be refined continuously; this can be accomplished by adopting a suite of innovative, leading solutions, including encoding and blockchain technologies, third-party service augmentation, threat-mitigation tools, and more.

Security Through Architecture

While the above strategies represent significant steps in building out a mature security organization, the adoption of zero-trust implementation where every access request and session is authenticated separately represents a significant step for providers to take. In this approach, what's inside the network is treated no differently than what's outside, and each level is designed to fail without compromising overall protection.

Zero-trust implementation can start with access tied to employee roles, authentication, and the application of minimal security. Identifying the user and applying their role-based security shouldn't grant them access to anything other than the *opportunity* to authenticate against something they want to access. Rigorous evaluation and standards for employee access should be agreed upon by internal stakeholders and regularly reviewed.

An employee's standard access may cover corporate domain network login access, Single-Sign-On (SSO) access to email, personal and shared group drives, email distribution lists, collaboration suites, and the default application access for the role (which shouldn't be confused with the actual application role access). Here's an example; if you work on the digital service provider's accounting team, you get access to the SSO that allows you to log in to NetSuite, but you also need a NetSuite account. That NetSuite account then requires appropriate security to be added to your role within the application itself. So, access to one thing (the corporate network) does not imply access to another (the applications).

Another strategy sees employees only able to use a device managed by the provider to access the provider's network. In this strategy, the network looks for deployed certificates, so only endpoints that meet the provider's security posture can access the network. This strategy can be strengthened by tying all work campuses to a single network domain and requiring all remote employees to first connect to the corporate domain using multi-factor authentication (MFA) and an SSO to VPN.

Once logged into a hosting environment, the provider can consider employing Privileged Access Management (PAM), which requires employees to request access to assets. If someone's role is allowed to access the asset, they can self-service a request for access, which is documented and granted. Once

they log off, their access is removed. Even though the provider identifies and authenticates each, they must authenticate and request access again when taking a new step.

Yet another strategy may see all of the digital services provider's laptops relying on encrypted drives, disabled USB ports, and Endpoint Detection and Remediation (EDR) software installed (which uses an AI agent) to detect 'not normal' behavior. Since the endpoint is a critical part of this posture, the provider should validate the OS patch monthly and ensure the various tools are active and up-to-date. For global, third-party contractors, the provider should consider deploying a virtual desktop enabling them to log in using their device. (In this case, that virtual desktop would serve as the starting point of access to the provider.)

Beyond this, there are many additional external protection layers, including next-generation firewalls, advanced web application firewalls, DDoS protections, credential stuffing services, real-time threats feeds, and security features that digital services providers can ensure the right user is operating the application as intended.

Here's where it gets even more technical. Because many providers' online services may be positioned between the end user and the banking core, they should consider deploying secure connections from their hosting environments to the cores, usually back through the financial institutions. This may help maintain a VPN spoke-and-hub network where standard VPN hardware devices connect all the spokes and huge security doors at the edge of the provider's hosting environments only let in desired traffic. Depending on its constitution, the network can be refreshed to an SD-Wan that provides ease of operation and rapid deployment and takes another leap forward into a Secure Access Service Edge (SASE) solution. Using the cloud as the center of the network, the provider should identify an SASE that can distribute security services across the network, preventing unwanted traffic into the VPN mesh and including the entire network footprint into a Zero Trust Network Architecture (ZTNA) security posture. Surpassing Network-as-a-Service layering onto Network-Security-as-a-Service architecture, using the edge of the network can deliver more services faster, and more securely, to the endpoints. SASE is transforming the industry as the convergence of services (Network-as-a-Service and Network Security-as-a-Service) move into this new delivery model. This can serve to improve security, performance, scaling, and future-proofing and allow data to flow dynamically. With these trends in mind, the future may look more like a pay-as-you-use service where bytes are protected and flows are inspected.

Another essential piece of a zero-trust architecture involves leveraging data in a way that protects all surrounding layers. In this model, the data itself can become a part of the security posture through the sophisticated use of tokenization, encoding, and blockchain technology. All sensitive data can be removed, replaced by tokens within the application surface, then randomly encoded and fragmented into pieces scattered and stored across multiple blockchains. The actual data itself is never stored in a usable form and it needs to be "re-hydrated" for use. Should a compromise occur, no real data can be harmed. Without being "re-hydrated," it's meaningless.

That's a lot of technical talk, but it illustrates how zero-trust is a significant project to tackle. That said, the benefits are far-reaching, create a solid foundation to build on, and should allay fears that your layers are only covering issues (or that you're one failure of a layer away from disaster). This zero-trust approach not only improves your security posture but positions you to keep pace with a truly exciting development project, using truly disruptive and cutting-edge technologies.