The Path to Secure and Productive Work in Financial Institutions

The push for digital transformation creates critical gaps in visibility and control.

The financial services industry continues to see rapid growth and innovation, but along with that comes a variety of challenges. New financial products, services, and partnerships create a complex web of interconnected systems, creating significant visibility and compliance challenges. Employee productivity and retention have become pressing concerns for many organizations, as they struggle to keep pace with a changing landscape and increasing competition. At the same time, cybersecurity threats continue to evolve and pose a significant risk to sensitive financial data. These challenges have left many financial services organizations grappling with how to effectively manage the needs and wants of their customers and workforce, while also safeguarding against privacy violations and potential breaches.

Top Challenges for Financial Services

Interconnectedness of financial systems

As financial services organizations increase their reliance on external parties, more and more outsiders require access to a variety of sensitive information, significantly increasing third party risk.

Evolving regulatory landscape

New and changing regulations mandate better control over how organizations protect their data, systems, networks, and people. GDPR, PCI, SOX, FFIEC, BCBS, CISA, and other regulations continue to evolve and introduce new regulatory challenges.

Drive for improved employee experience

Financial services organizations are seeing turnover rates at near-record highs, especially for younger workers, despite substantial pay increases. Attracting, onboarding, and retaining millennial workers in the new hybrid workforce demands an optimized employee experience that enables productive work from anywhere.

Increasing sophistication of cyber attacks

Modern attackers are well aware of the defenses that are most commonly deployed, and continuously update their tactics to adapt. Today's sophisticated phishing techniques, ransomware campaigns, and business email compromise attacks keep defenders on their toes.

Poor visibility and complex controls in SaaS solutions

Financial services organizations continue to migrate from self-hosted to SaaS services for banking and other critical applications. This migration helps drive costs down and improves user experience, but also reduces crucial visibility and complicates the controls that security teams need in order to prove compliance and protect key assets.

The Stakes for Financial Services

U.S. SEC fines 16 Wall Street firms $1.8 bln for talking deals, trades on personal apps
Poor controls over the applications that traders used led to large fines for many of the world's largest financial services organizations, including Barclays, Bank of America, Citigroup, Credit Suisse, Goldman Sachs, Morgan Stanley and UBS.

2022 Crowe Bank Compensation and Benefits Survey
An intrusion forced the firm's IT staff to shut down access to critical services including Citrix VDI, eliminating access to email, network, and internal document management systems. Some attorneys reportedly fell back to using personal computers to access client documents.

Former Block employee downloads personal information on 8.2 million customers
The "ABA 2022 Legal Technology Survey Report" shows that 27% of surveyed law firms acknowledge that their firm has experienced a security breach, but only 42% had prepared an incident response plan.

The Way Forward for Financial Services Organizations

Today's reality: the market for financial services is hyper-competitive, the threats are numerous, and regulations continue to expand and become more complex. This creates enormous opportunities for organizations who are able to navigate these challenges effectively. Key capabilities to keep in mind include:

Flexibility
Flexible financial services organizations are able to capitalize on new and emerging technologies to get a leg up on their competitors by reducing costs, opening new revenue streams, and improving experiences for employees and customers.

Visibility
As new capabilities are introduced within the organization, security teams must ensure they have the deep visibility they need in order to protect sensitive data against misuse or data loss.

Governance
When driving digital transformation, financial services organizations must maintain effective controls and governance over key processes, in order to protect sensitive data and demonstrate regulatory compliance.

Leading the Way with Island, The Enterprise Browser

Island pioneered the Enterprise Browser – the ideal enterprise workplace, where work flows freely while remaining fundamentally secure. With the core needs of financial services organizations naturally embedded in the browser itself, Island delivers complete control, visibility, and governance over the last mile, while delivering the same smooth Chromium-based browser experience users expect.

With Island, financial services companies can address a number of critical use cases:

- Protect sensitive information across all SaaS and web applications with integrated DLP, secure storage, and dynamic last-mile controls like screenshot protection, copy/paste control, and data masking.
- Enable safe access by contractors or third-parties to financial applications and documents, with full audit records of every action and last-mile controls to prevent data leakage.
- BYOD or BYOPC access with application boundaries to ensure sensitive data stays within the company systems and under their control.
- Safe browsing to block malicious content, phishing attempts, or other web-based threats and complete forensic logging to investigate incidents.
- User experience enhancements to improve employee onboarding, speed up common tasks, and deliver a world-class employee experience to help recruit and retain top talent.

"It's so rare that you can add a security tool that greatly enhances the security posture of the organization and that the end-users genuinely enjoy."
Tim Ringley, VP and CISO, The Bank of Marion
Read the Case Study

Island Technology, Inc
3501 Olympus Blvd. Suite 350
Dallas, TX 75019
886-832-7114
Island.io

When you're ready, let's talk.