Island

The Path to Secure and Productive Work in Hospitality

Delivering a world-class hospitality experience for staff and guests while protecting critical systems and data

Technology plays a central role in today's hospitality industry both for guests who book online and use their mobile phones as room keys to the various applications that help orchestrate a wide range of staff. An optimized technology landscape can be the difference between a delightful guest experience and a frustrating day — or worse, a breach of trust. Protecting the sensitive payment and guest information that passes through their systems everyday requires a unified system that is flexible and adaptable.

Top Challenges for Hospitality

Flexibility is key

Hospitality staff need technology systems they can access from anywhere, often on mobile devices. It must be highly scalable to support a boutique hotel or a large resort and events center.

Guest information must be protected

Guests trust their payment information, itinerary, and personal data with the hospitality provider. This trust must be repaid with strong security that keeps private information private.

Supporting a range of staff

Hospitality staff cover a variety of roles with a variety of technology fluency. Any company-wide system must be convenient and easy to use for all staff.

Threat actors are external and internal

Security professionals in the hospitality industry must protect against a range of threat actors, including staff members who accidentally — or maliciously — seek to disclose private guest information.

Delivering a differentiated employee experience

The hospitality industry faces hiring and retention pressures, so delivering a differentiated employee experience is key to long term success. IT teams can help improve onboarding and employee engagement through the thoughtful use of technology that delivers a great employee experience.

The Stakes for Hospitality

Verizon Data Breach Investigations Report 2022
Verizon research shows that the accommodation and food services industry faces a wide range of threats, from system intrusion to social engineering and basic web application attacks. Further, they found 10% of threat actors were internal to the organization. posing as their brand (versus 38%).

IBM Security: Cost of a Data Breach Report 2022
According to IBM, the average cost of a data breach in the hospitality industry is nearly $3M.

The Way Forward for Hospitality

Cyber security is critical for hospitality — but it's table stakes. Succeeding in the industry means offering a great service to guests while offering a positive employee experience for staff. When done well, these two form a positive feedback loop with engaged, productive employees who go above and beyond to delight guests.

Digital Transformation

Hospitality companies can improve their employee experience and the service they offer to guests by transforming the digital experience for everyone. Putting the right tools and information in the hands of every staff member lays the foundation for a differentiated employee and guest experience.

Improve Visibility and Security

With private guest information passing through every digital system within a hospitality organization, security is critical. Visibility is essential to govern how this data is accessed, by whom, and empower IT & Security teams to respond and adapt.

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. Island delivers complete control, visibility, and governance over the last mile of any web application interaction, while delivering a smooth, frictionless browser experience on any type of device.

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

- Universal access from any device type: laptops, desktops, thin clients, smartphones, or tablets with a familiar browser interface that requires no additional training for users.
- Protect sensitive data 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.
- Manage privileged user accounts and protect critical back-end services, whether in the cloud, over SSH, or private web applications. Audit every privileged user interaction with complete visibility including screenshots, clicks, and keystrokes.
- Enable safe access by contractors or third-parties to web applications and data, with full audit records of every action and last-mile controls to prevent data leakage.
- BYOD or unmanaged device access with device posture assessment to allow application access only on safe devices that adhere to security policies.
- 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 automate business logic through robotic process automation.

When you're ready, let's talk.

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