

How Lookout Protects Point of Sale Devices

The hospitality industry is embracing the use of mobile POS

Security and Business Challenges

Modernization of the hospitality industry takes place in many different ways, but the most evident sign is that of more advanced point-of-sale (POS) systems present in restaurants, hotels, gyms, and anywhere that takes credit cards. These systems are a great way to offer payment flexibility and ensure loyal customers get their rewards points, but they also offer an easy point of entry for an attacker if they're not properly locked down.

Security teams may overlook these devices in their evaluation of their overall security posture, but it's important that they remember these devices are run on mobile OSes and connected to the network in the same way that other employee devices are. Therefore, they are subject to the same level of risk and, as mobility expands, compliance standards are also becoming more complex and include mobile devices in their parameters.

Hospitality Mobile Risk in the Real World

As a way to bust lines and make the customer experience more positive, hospitality organizations are embracing mobile POS solutions so customers can pay right on the spot without losing sight of their card or waiting in line. However, this convenience is not without its risks, as proven by the Landry's hospitality chain breach in late 2019. Landry's disclosed that it had been victim of a cybersecurity attack targeting its POS systems in many of its 600 restaurants, hotels, and casinos that put customer credit card data at risk.

Security teams need a way to easily secure these devices from multiple attack vectors, such as an attacker infiltrating the network to drop malware onto all connected devices. There also needs to be additional visibility as a way to be sure that these devices align with expanding compliance standards, such as PCI, to avoid discipline and hefty fines.



Industry Challenges

1. Point-of-sale systems are easy to overlook as part of organizational security.
2. Compliance standards are expanding to include mobile devices, which includes POS systems.
3. Security teams need full visibility into these devices and a way to remediate threats without putting the greater organization at risk

Lookout Critical Capability

Lookout gives security and IT administrators full visibility into corporate-owned POS devices to make sure no single device compromises a location's entire network. Lookout admins can put policies in place that allow them to cut a device off from the company's network as soon as malware is detected. Additionally, Lookout can help ensure alignment with PCI and other compliance standards on mobile POS devices as these standards expand to include mobile devices

Why Lookout

Lookout Mobile Endpoint Security ensures security and compliance on every device, leveraging a large data set fed by over 185 million devices and the analysis of over 90 million mobile apps. With the Lookout Security Cloud, it's easy to deploy Lookout and apply security policies across the entire organization for both managed and unmanaged devices. Users receive alerts and remediation steps on malicious apps, network connections, and system anomalies in real time; accompanied by dynamic device health checks to provide conditional access to sensitive corporate applications and data.