SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

AUTOMOX

PARTNER SUCCESS STORY

Cybersecurity Services Firm Chooses Automox as a Low-Touch Patching Solution to Quickly, Easily Update Remote Customer Endpoints

BIOGRAPHY

- Jeremy Loudon, Director of Business Operations

ABOUT IHLOOM

Ihloom is a cybersecurity firm providing risk assessment, defense development, monitoring, training, and security coaching services to small and midsize businesses across the United States. Its client base is diverse, with a focus on real estate attorneys, marketing companies, biotech firms, and U.S. Department of Defense contractors. Ihloom is a full-service firm that provides primarily managed EDR, patch management, SIEM, and backup services, as well as assisting in security architecture development and compliance management. Its clients are often smaller companies whose dedicated IT staff do not have the time, knowledge, or expertise to develop or manage the details of an effective security program.

CHALLENGE

Patching and endpoint hardening has become more urgent as new vulnerabilities in commonly used software are announced almost daily. With the shift to a more distributed workforce in the past year, the urgency to keep these remote systems protected is more apparent. Attackers are quick to take advantage of remote devices that now sit outside of the protected corporate perimeter. According to leading industry data, adversaries are weaponizing new critical vulnerabilities in seven days on average. And zero-day vulnerabilities are already weaponized at the moment of disclosure. The easiest way to remediate these vulnerabilities is through patching, so having a solution that can easily identify which machines need the latest patches and then be able to quickly remediate them is essential to protect Ihloom clients.

Ihloom customers typically struggle with the ability to keep up with cybersecurity alongside the day-to-day challenges of keeping their systems running. Most customers are overwhelmed and don't have sufficient information or the skilled staff to process security alerts as needed. These customers are also struggling with misconceptions about the security of their corporate endpoints, where many of their employees may think, "My computer updates (patches) automatically," or, "Macs don't have security issues."

SOLUTION

Ihloom chose to offer Automox as its patching and endpoint hardening solution because of its small footprint, its ability to easily patch remote workers, and its skill in providing the visibility and swift remediation capabilities that most organizations need to effectively respond to newly reported vulnerabilities. Because Automox is cloud native, Ihloom feels confident that it can effectively patch and update client systems no matter where they are located. Additionally, being a cloud-native solution gives Ihloom customers the agility they need to stand up an endpoint hardening solution without the considerable investment in time or cost of implementing an on-premises solution.

"Automox is a great fit for many of our customers because it allows them to manage their Mac, Windows, and Linux endpoints in one platform. Because our clients may not have an on-premises file server or a traditional identity and access management solution, having a cloud-native solution like Automox gives them the security solutions they need without the considerable investment in hardware and software that on-premises solutions may require."

Jeremy Loudon, Director of Business Operations

RESULTS

With Automox, Ihloom customers are now able to shift manual patching operations that had been left in the hands of their employees to an automated approach that gives their IT teams more confidence that the necessary updates have occurred, coupled with the visibility and insight that systems are indeed up to date. With Automox, Ihloom customers are managing local user account policies through worklets, enforcing a baseline level of account and workstation security, and managing workstation patching.

"Automox layers nicely with other security products and is a more low-touch solution when compared to a traditional RMM. Our customers can have more confidence in their corporate security posture because they are able to protect their corporate and BYOD endpoints wherever they are located. Plus, they are able to report to regulatory authorities during compliance audits that they regularly and effectively patch all their machines as required."

Jeremy Loudon, Director of Business Operations