Clearedin

CASE STUDY

Case Study: Tekion

Top 3 Case Study Highlights:

- Modernize the existing IT stack by strengthening Mimecast SEG, offering file sharing DLP sensors, and securing against supply chain attacks within collaboration, as well as improving reporting for compliance-sensitive global automotive brand partners and customers
- Create and expand a Zero-Trust security environment to eliminate all possible coverage gaps for all cloud-based applications, including Tekion's own Dealer Management System (DMS), and achieve SOC 2 compliance
- Ensure user and DevOps security for 1,000+ global staff, remove internal and external threat vectors for cloud collaboration applications, and add Clearedin innovations to prevent user Account Takeover (ATO) and Business Email Compromise (BEC)

Who is Tekion?

Disrupting a 50-year reliance on aging Dealer Management System platforms, Tekion has challenged the paradigm with the first and fastest cloud-native automotive retail platform, Automotive Retail Cloud (ARC). This transformative dealership software platform uses cutting-edge technology, big data, machine learning, and AI to seamlessly bring together OEMs, retailers/dealers and consumers. With its highly configurable integration and greater customer engagement capabilities, ARC is simplifying the dealer/consumer relationship and journey. Founded in the Silicon Valley, Tekion employs over 1,000 innovators globally.

What are the primary goals of security modernization at Tekion?

Tekion's diverse multi-cloud application offering automates the end-to-end transportation dealer's operations. Securing Tekion DMS to harden customers' service, parts, ordering, showroom, payroll, and all other applications is a lynchpin in driving company growth. Keeping every aspect of the dealership securely running on time and without exposing any dangerous threat vectors was the first primary goal. To achieve this stance, Tekion's IT team established an ambitious onboarding automation

TEKION

Headquarters:
Pleasanton, CA

Founded:
2016

Industry:
Automotive, Cloud

www.tekion.com

TEKION

"Our global team is now cloud-first everywhere. We needed a cloud-first collaboration application security solution like Clearedin to scale with our growth. Several prior security investments missed the multi-cloud integration transition and still focused on in-house prem infrastructure. Our goal, made easier through Clearedin's approach, is to securely automate access login for core identity needs leveraging Okta."

– Guru Sankararaman
Co-Founder, CFO, and VP of Operations
Tekion

"We needed to quickly span a multi-cloud gap in our DLP and SEG cloud infrastructure to achieve our goal of 99% self-installation. The ramp up includes meeting the diverse needs of global customers and even physical training for Tekion's 1,000 users: first training of dealer staff, integration with existing dealer processes, and tracking employee operations."

– Steven Bang
Director of IT
Tekion

that covers all cloud applications through back-end integrations. This initiative began with securing user email and expanded into DKIM, antivirus, and Mimecast's Secure Email Gateway (SEG).

The second primary goal was to unify cloud security across multiple file-sharing platforms, including DropBox, OneDrive, and O365. There are literally thousands of file collaboration requests both internally and through external clients, requiring the unified security of Clearedin's platform to prevent dangerous phishing exploits, supply chain attacks including ATO and BEC. Many global customers' entire back office operations rely upon the secure deployment of Tekion's cloud application and API suite. Clearedin supports this entire ecosystem through complete multi-cloud collaboration protection.

Why is Tekion automating security operations for staff and customers?

A critical element in Tekion's IT buildout is automating the onboarding of staff and customers with a compliance-first mindset. Since the Tekion cloud platform powers the back-end of automotive dealers, it presents an extremely attractive attack surface for malicious exploits. At stake: vehicle sale transactions, service records, parts invoices, and customer data and transactions, not to mention staff payroll details. By creating a unified view of user cloud application activity, Clearedin helps Tekion through powerful Machine Learning, AI, and the visibility of a scalable Trust Graph to proactively manage multi-cloud risks.

How did Tekion deploy Clearedin to solve specific needs and requirements? Why select Clearedin over existing solution providers?

The IT team began to see scattered security incident reports, with social engineering root causes among the largest concerns. Examples included spoofed sent invoice and payment received emails. Prior to Clearedin, Tekion addressed these emerging needs with several existing Microsoft solutions. While Microsoft security applications helped identify up to 1,000 attacks weekly, the team believed that this was only the tip of the iceberg, and that many more attacks were hitting users and potentially customers. The ability to identify, audit, and ultimately remediate these social engineering threats led the Tekion team to install and widely deploy the Clearedin platform.

Clearedin

"Tekion's secure multi-cloud collaboration, API connection, and automation initiatives align perfectly with Clearedin's approach to unifying collaboration security across every cloud application, including Slack, Teams, OneDrive, and O365."

– Ajay Mishra
CEO
Clearedin

What are Tekion's primary goals to deploying multi-cloud collaboration security to prevent supply chain attacks over collaboration and file sharing?

Ramping up security and onboarding automation are among Tekion's top IT initiatives. The company previously leveraged hybrid security but steers clear of the speed bumps inherent in Active Directory, VPN solutions, and on-prem server deployments. A primary use case for Clearedin quickly developed to proactively monitor file sharing without prescriptive user activity. By leveraging Clearedin's Trust Graph, this approach helps IT identify malicious activity, including BEC and ATO exploits. The Trust Graph also delivers full audit transparency for both users and customers across the Tekion DMS cloud.