CASE STUDY

Krumland Auto Group

About Company

Industry: Automotive retailer and dealer

Location: Roswell, New Mexico

Founded in 1952, Krumland Auto Group ("Krumland") has established itself as a reputable and customer-centric automotive dealership group, serving the community with a wide range of high-quality vehicles and exceptional service. With a rich history spanning over seven decades, Krumland has evolved into a trusted name in the automotive industry, known for its dedication to customer satisfaction and its extensive inventory of new and used vehicles. The company's commitment to exceptional customer service has earned it a loyal clientele and numerous accolades over the years, making it a trusted destination for automotive needs in the region.

In the fall of 2021, the Federal Trade Commission (FTC) proposed an amendment to the Safeguards Rule, requiring non-financial institutions engaged in financial transactions to develop, implement, and maintain a comprehensive security program to safeguard customer information. Krumland took proactive measures to enhance its data security protocols to comply with this new regulation. One crucial aspect was the implementation of multi-factor authentication

(MFA) for anyone accessing customer information. Among various vendor options available, the company selected BIO-key's PortalGuard IDaaS, a solution that fulfilled its core authentication security requirements while enhancing the user experience.

PortalGuard's flexible MFA methods include phoneless, tokenless, and passwordless Identity-Bound Biometrics (IBB) that seamlessly integrated with the company's IT workflows and systems, ensuring the highest level of security while maintaining operational efficiency. Unlike any other product or solution in the authentication category, BIO-key's IBB provides a FIDO2-compliant passwordless authentication option, which allows users to take advantage of a true biometric passwordless authentication solution that does not require the use of phones or tokens to assist in the authentication process. With phish-resistant MFA and passwordless authentication top of mind for organizations of all sizes and across all industries, Krumland addressed a critical business use case that traditional MFA overlooks – users who cannot use a phone or token to authenticate.

Key Issues & Existing Challenges Addressed by PortalGuard

As the deadline loomed for compliance with the FTC's Safeguards Rule, Krumland faced the challenge of identifying a suitable multi-factor authentication (MFA) solution that could meet their requirements and be implemented before the deadline.

Krumland had specific criteria for their MFA solution, emphasizing the need for a comprehensive and flexible system capable of securing desktops, web applications, remote access, and remote desktops. It was also critical to be able to fully integrate with their existing Microsoft Active Directory servers and Cisco Systems VPN Client was crucial to their decision-making process.

Perhaps of the utmost importance, however, was finding a solution to fit the needs of the company's technicians. Many of the IAM options on the market could only address some of Krumland's unique requirements – such as employees being unable to use mobile devices or fingerprint readers for authentication – and BIO-key emerged as the comprehensive solution to the company's security challenges.

The PortalGuard Resolution

Before engaging with BIO-key, Krumland had initially provided its end users with SMS one-time passcodes for multi-factor authentication; however, it became clear to the company's IT team that a more sophisticated security solution was needed to address their security requirements while improving the user experience. With a diverse group of users across the Accounting, Sales, and Manufacturing departments, the company required a solution that support vastly different use cases and environments while adhering to new government compliance regulations and cybersecurity insurance requirements.

In 2021, Krumland deployed PortalGuard for multi-factor authentication – supported by the additional layer of security provided by IBB – which was critical to securing roving user access on the shop floor and shared workstations on the sales floor. The company implemented IBB authentication supported by BIO-key's PIV-Pro and SideSwipe fingerprint readers at each workstation. Employees on the shop floor were no longer concerned with using their mobile devices to authenticate with the quick, simple fingerprint scan; every user could access applications and data seamlessly while avoiding using less secure authentication methods.

In addition, Krumland's shop technicians required additional authentication options to support their unique use case, as many work in hostile environments, wearing protective clothing and gloves. Leveraging the authentication flexibility of PortalGuard, BIO-key's implementation team provided the company with additional configuration options to ensure secure and seamless access to applications and data throughout the workday.

"*It prevented us from losing millions of dollars in lost revenue due to the new MFA requirements placed on dealerships like ours. Forcing technicians to remove their gear just to access their phones would create a tremendous loss of productivity for them, which in turn would cost us money.*" – **IT Director, Krumland Auto Group**

Based on the number of technicians at Krumland, the average number of times per day a desktop screen locks, and the amount of time it takes to remove and then re-apply protective gear, BIO-key helped the company save over $6M annually.

In less than 60 days, Krumland was fully deployed with PortalGuard and Identity-Bound Biometrics – enabling MFA authentication for its users before the required compliance deadline. With PortalGuard Desktop, the company could also implement MFA for workstation access, bolstering security to sensitive information for remote access and remote desktops.

Top reasons Krumland Auto Group selected BIO-key

- Provided the most compelling solution for a phoneless, tokenless, and passwordless MFA solution to meet its government compliance regulations and cybersecurity insurance requirements
- Unrivalled deployment options to address unique use cases
- Easy integration and management for the IT team
- Rapid implementation and return on investment