ManagedMethods

CASE STUDY

ManagedMethods & American Exteriors, LLC

Visibility and control of data shared in Google G Suite provides security of critical business and customer data

American Exteriors, LLC is a national home exterior and bathroom remodeling company, growing over the past thirty years to more than 300 employees in 11 locations throughout the Midwest and Rocky Mountain regions. The company manufactures and sells replacement windows, siding, exterior doors and other products, including Kohler bath and shower products, that improve the energy efficiency and appearance of an existing home.

To support American Exteriors' continued growth, the company's IT group transitioned from legacy in-house file sharing and email applications to Google G Suite for seamless data sharing and to empower its employees to provide the best experience for their customers.

The Challenge

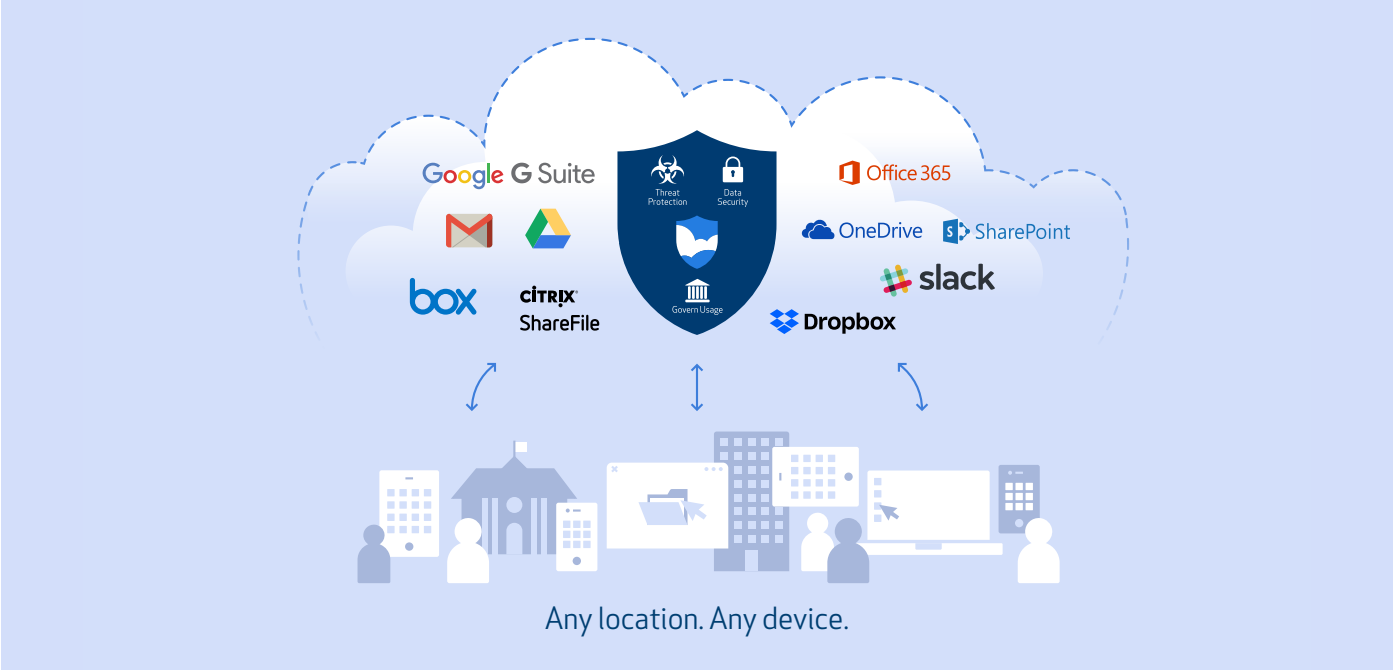
After deploying Google G Suite, American Exteriors' IT team lost visibility into email content and how documents were being shared and with whom. Since the company had continued to use its legacy network security suite of firewalls, end-point detection, and email MTA, there was no way for the IT team to know what data was being shared, stored, and accessed in G Suite. In addition, G Suite's standard security features offered no way to audit or control document access and sharing in the cloud. This created potential data loss situations where price lists, customer lists and sensitive PCI and PII information could be easily shared with either an employee's personal Google account or individuals outside of the corporate domain.

The Solution

American Exteriors deployed ManagedMethods' CASB solution, Cloud Access Monitor to gain the critical visibility and control of their G Suite accounts. Cloud Access Monitor's highly-customizable Data Loss Prevention (DLP) policy engine and machine learning capabilities now provide visibility into the more than 160,000 documents and images shared in the cloud containing potentially sensitive corporate and customer data.

> **With our multiple locations and employees working both in the office and in the field, it was critical for my team to be able to secure our corporate and customer cloud data from outside the protection of our corporate network. ManagedMethods' Cloud Access Monitor provides the visibility and control of our G Suite accounts so we can stop worrying about the risks and focus on our success.**
>
> ***Mike Hurst, Director of IT, American Exteriors***

Another reason that American Exteriors chose Cloud Access Monitor is the quick implementation and out-of-the-box policies that tag objectionable content and PII. Cloud Access Monitor deploys in minutes and without proxies or agents, so American Exteriors was quickly able to get the visibility into how their data is stored, accessed and shared in G Suite, with no impact on existing networks or user experience.



Benefits

- Cloud Email Security - protect against advanced malware, phishing attacks, protect against data loss and enforce content and compliance rules.
- Cloud DLP and Policy Monitors - Out-of-the-box highly-customizable cloud DLP policy engine to monitor for sensitive information and enforce policy.
- Cloud Threat Protection - Surface risk in the form of anomalous user behavior and potential account compromise.
- Quick Time-to-Value - Rapid deployment via API and out-of-the box policies to provide immediate visibility and control.
- Extensibility and Scalability - Secure multiple cloud environments and integrate with existing security technology investments.

About ManagedMethods

ManagedMethods makes Cloud Security Easy by quickly providing visibility into how data is stored, accessed and shared in popular cloud applications, including Google G Suite, Microsoft Office 365, OneDrive, and Sharepoint, as well as to secure cloud-based email, including Gmail and Office 365 Email. ManagedMethods' Cloud Access Monitor is the industry's only Cloud Access Security Broker (CASB) solution that can be deployed in minutes with no special training, and with no impact on users or networks.