# SECURITY OVERVIEW

## DATA

Metadata only, collected with **GRAPH API**, service accounts with **GLOBAL READER ROLE**

Data Encrypted in **TRANSIT** and at **REST**

## ACCESS CONTROL

Privileged Access by CoreView is strictly by **JOB NEED**, through a **CENTRALIZED VPN** and through **JUMPBOXES**

All activity is logged in **SIEM PLATFORM**, plus video recording of sessions; logs and videos held for **10 YEARS**

## OPERATOR ACCESS

Uses single sign on with Microsoft account so **NO CREDENTIALS** stored in CoreView

Multifactor **AUTHENTICATION** methods are respected

Optional advanced management mode, service account details held in **AZURE KEY VAULT**

## VULNERABILITY MANAGEMENT

Ongoing and continuous monitoring of **VIRTUAL MACHINES**, **NETWORKS** and **SERVICES** through Azure Security Center and Microsoft Defender

**STATIC CODE ANALYSIS** part of the Continuous Integration process

Code Quality ensured through constant Pull Request process performed by a dedicated set of **SENIOR SOFTWARE ENGINEERS**

## COREVIEW EMPLOYEES

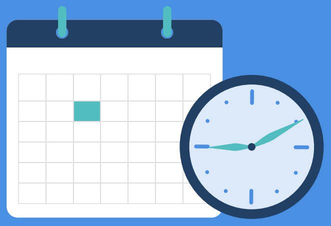
Mandated annual **SECURITY** and **COMPLIANCE** training for all staff

**BACKGROUND CHECKS** during hiring motion

End user computers **PROTECTED** with Microsoft Intune, DLP, Microsoft Defender and Firewalls

## BUSINESS CONTINUITY

Disaster Recovery and Backup/Restore procedures **CONSTANTLY UPDATED** and **TESTED** as part of Industry Standards Certification process



Business Continuity plan, documented and tested every **6 MONTHS**

Automated patching with **PROCESS** to ensure no impact on **LIVE SERVICE**

## CERTIFICATIONS

AICPA SOC

CERTIFIED ISO 9001:2015 COMPANY

Information Security Management System ISO 27001 Certified

CoreView