cowbell®

Activate Connectors for Deeper Risk Insights

A Leading Cyber Insurance Provider for SMEs | cowbell.insure

V.JAN23

cowbell®

Cowbell Connectors

Connectors enable our platform to access your cyber infrastructure in a secure and restricted way. They can read limited information related to your security configuration and use of security best practices.

Connectors refine our risk assessment with inside-out data and deliver visibility into security weaknesses you may not be aware of - at no additional charge.

Get Better Visibility into Your Cyber Risks

Every organization uses internet-connected systems, phones, and email. However administered, they always represent a cyber risk.

To assess this risk, we rely on data sources, external scanners, and dark web activity. Connectors add inside-out data to the compilation of our risk assessment factors, also called Cowbell Factors™, delivering a refined risk profile and helping you optimize your premium.

Improve Your Risk Profile

Cowbell Factors incorporate additional data when connectors are activated. A deeper assessment brings better visibility into security weaknesses as well as recommendations on how to minimize them. **The benefit:** Your organization can improve its security posture before any incident happens.

Optimize Your Insurance Premium

Activate one connector and become eligible to a 5% premium credit regardless of findings.*

*for Prime 250 policyholders only.

cowbell®

Available Connectors

(Ask us for an up-to-date list as we add new connectors monthly.)

- **Connector to Microsoft** - delivers risk insights related to Microsoft 365 (aka Office 365) and other Microsoft collaboration tools.
- **Connector to Google Workspace**- delivers security insights into common productivity apps (Gmail, Calendar, Meet, Chat, Drive,...)
- **Connector to Google Cloud**- discovers misconfigurations, and vulnerabilities, and detects threats within your Google Cloud deployment.
- **Connector to AWS**- delivers risk insights related to cloud based network services for security best practices.
- **Connector to Secureworks**- provides metrics on the customer deployment of the Taegis platform, a common cloud security platform.
- **Connectors to Qualys** - reports on current system vulnerabilities, patching of known vulnerabilities, container security, and regulatory compliance.
- **Connector to Security Studio** - reports on risks related to processes deployed in the organization (typically risks not related to systems).
- **Connector to Safeguard** - reports on policies in place and risks related to the use of social media.
- **Connector to Wizer** - supports businesses in developing a cybersecurity awareness program for their employees.
- **Connector to Cloudflare** - provides web performance and security services.

How Secure is the Use of Connectors?

We rely on APIs developed and maintained by the vendors themselves to share configuration and security data – these APIs are not unique to Cowbell. Access is read-only, limited to metadata and configuration information, and explicitly restricted to what the vendor API provides access to. We never access business information and data stored in the system itself.

Example: Connector to Microsoft

For heavily-used collaboration tools like Microsoft, it's critical to enforce security best practices to avoid Business Email Compromise (BEC) or other data breaches.

Microsoft 365 (aka Office 365) is commonly used as an email service deployed in the cloud. The service can be administered directly by the organization or outsourced to a third party.

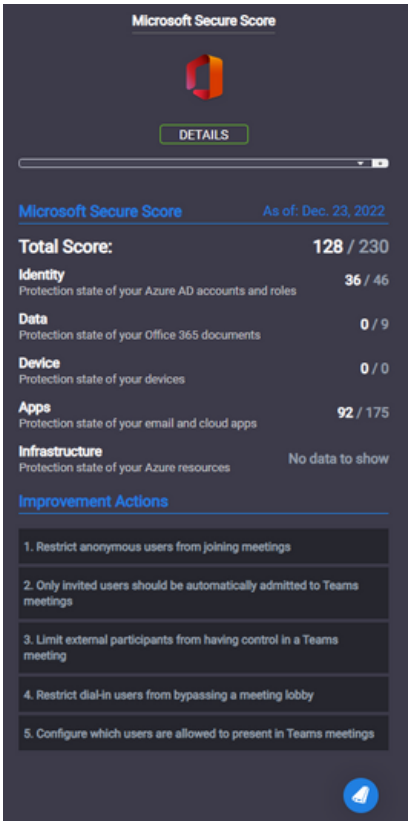
Cyber incidents due to misconfigurations of Microsoft 365 have been common enough that the U.S. government has issued several security warnings for Microsoft Office 365 since May 2019, recommending that every business review its Microsoft 365 configuration for security.

Better Risk Visibility

Every network-connected system, equipment, or device represents a cyber risk that needs to be assessed to fully understand your organization's risk profile.

Cowbell Connector to Secure Score offers an immediate, free audit of your Office 365 security configuration

- Get immediate visibility into data tracked by Microsoft: your score, strengths, weaknesses in the configuration of Microsoft Office 365, and improvement actions.
- The assessment is based on a standard set of controls jointly defined by Microsoft and the CIS and represents the best security practices for Microsoft 365.
- Common controls include the use of Multi-factor Authentication (MFA) or the need to limit the number of users with administrative privileges and access to sensitive data.



The Leader in Cyber Insurance for SMEs

Cowbell aims to make cyber insurance accessible to all and help insureds strengthen their cyber resilience. Our policies come bundled with extensive risk management resources so that businesses can reduce their exposure and avoid incidents.

5 Reasons to Activate Connectors

Avoid Cyber Incidents

Activating Cowbell Connectors could give you an early warning about a security weakness that you are not aware of. Acting on recommended actions to remediate vulnerabilities could prevent incidents.

Get a Cyber Policy that Best Matches Your Risk Profile

Cowbell Factors define your organization's risk profile and anchor our underwriting processes. Activating Cowbell Connectors delivers deeper and more accurate advice to improve your risk profile, resulting in the best possible insurance policy.

Optimize Your Premium

Activated connectors enable better visibility into cyber risks, which empowers you to proactively improve your risk profile. A better risk profile positively impacts your insurance premium. In addition, you become eligible for a 5% premium credit.*

*Premium credit available for Prime 250 policyholders only.

Share Our Free Assessment with Your IT/Security Team

Our risk assessment is free and shareable with your internal or external security resources. We can even give them access to our platform.

Get an Accurate Benchmark of Your Business's Risk Profile

Cyber attacks on small and medium-sized enterprises are often opportunistic, taking advantage of security weaknesses, or are used as a way to get to bigger clients or vendors. Knowing whether your risk profile is below or above your peers indicates the susceptibility of your organization to a cyber attack.

Need help activating a Connector?

Contact riskengineering@cowbellcyber.ai for assistance.