CyberHive Gatekeeper for Microsoft Office 365

Microsoft Office 365 is widely used as a business-to-business communication tool. The email, document sharing and teamworking features are well known and liked by over 1.2 billion office users and 60 million Office 365 commercial customers worldwide. Office 365 (O365) also offers great flexibility, allowing users to benefit from cloud services, accessing emails and files from anywhere.

Unfortunately, this very flexibility can offer security challenges for some organisations, with the loss of a single password or security credential resulting in a major data breach.

Some organisations choose to implement 2-factor authentication (2FA) as an improvement to the security features, however even this is not foolproof. Furthermore, 2FA using techniques such as text-based code authentication is seen as an unwieldy restriction and is often disabled for users operating inside a corporate office. This in itself can result in significant security weaknesses.

CyberHive Gatekeeper for Office 365

Recognising these weaknesses, a central government department worked with CyberHive to design and implement a truly secure implementation of Office 365 which overcomes many of the issues associated with alternative technologies. Our solution offers a huge number of benefits over other systems, including:

- Secures all O365 features, including Sharepoint, Email & Teams
- Simple to use. Just log on to your PC, insert the dongle and go!
- Prevents access to Office 365 from the open internet - Secured via IP restrictions
- Can only connect from computers / mobiles with a unique VPN certificate
- Requires hardware dongle & password to access O365
- Multiple independent security features – no single configuration failure can cause a security breach
- Secure logging of all access events, moved files etc.
- Protected by CyberHive's Patented 'Trusted Cloud' technology
- Easy to add new machines and users, and to remove lost or old machines

Using CyberHive Gatekeeper

To access Office 365, the user must use an endpoint device (e.g. a Laptop or mobile phone) with a valid unique security certificate to connect to a central VPN service. This prevents access to O365 services from any unauthorised devices. The connection is established automatically with no need for the user to enter a dedicated VPN password.

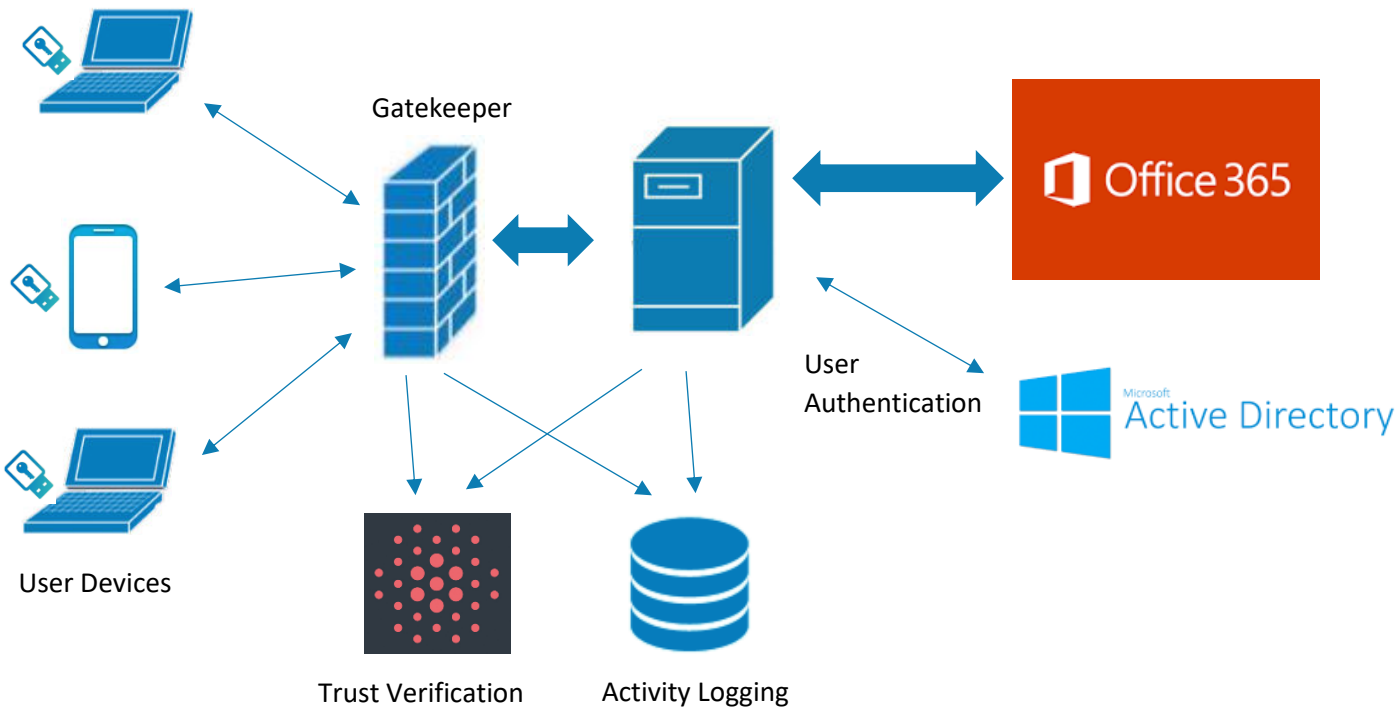
Once a connection to the VPN central service has been established, the user requires a dedicated USB security key to be connected to their laptop in addition to their central password to connect to O365.

No single security lapse can result in loss of security of the Office 365 account, since all users require a pre-approved laptop, a hardware security key and their user password before they can access the system.

Despite this high level of security, CyberHive Gatekeeper is designed to be extremely simple to use for the end user and avoids introducing unnecessary and complicated log-on procedures.

How it works

The simplified diagram below shows how CyberHive Gatekeeper works.



Access to your Microsoft Office365 account is controlled by CyberHive Gatekeeper. Your laptop or mobile phone is pre-configured with a unique VPN machine certificate which allows access through the high security firewall to the central services. Any unauthorised devices will be immediately rejected.

Access to Office 365 is then further secured by Microsoft Azure Active Directory (Azure AD) and requires username, password and a valid hardware security key to provide multi-factor authentication before access is granted to your account.

Office 365 is itself secured from access by restricting the IP addresses which are allowed to connect, preventing any unauthorised access by users attempting to bypass CyberHive Gatekeeper. The critical cloud servers used to restrict access to the service are protected using CyberHive's patented 'Trusted Cloud' technology to verify the trust status of the central servers deployed in CyberHive Gatekeeper.

A detailed audit trail is central to the design of the system to enable security analysis. CyberHive deploys custom code on a central log collection server. This will pull logs from Office 365 and all other cloud platforms and services and automatically transfer them to the activity datastore. Data will be available for automated analysis by machine learning systems / SIEM etc.

Wessex House, Oxford Road, Newbury, Berkshire, RG14 1PA
01635 881 880
www.cyberhive.com

Reliability and resiliance

The critical firewalls, VPNs, servers and networking components deployed in CyberHive Gatekeeper all use multiple redundant servers and systems to ensure that no single failure can result in losing access to your Office 365 service.

By using multiple independent security technologies, no single configuration error, such as an Active Directory config problem, can cause a data breach.

Trusted Cloud technology

The critical cloud servers, including VPN access points which are used to prevent unauthorised access to Office 365 are protected using CyberHive's patented 'Trusted Cloud' technology.

The technology employed is a cutting edge approach called distributed whitelisting. Every few seconds, each critical server generates an audit list of all programmes and configuration running on the server. This list is digitally signed using a cryptographically secure hardware module. This audit data is then sent to three or more verification servers where it will be cross-checked against a previously generated and signed whitelist. Even a single line of unauthorised code will be instantly detected and flagged, allowing our security team to stop an attack in its tracks.

Office 365

The Office 365 Business Premium package is standard for this solution as it meets the needs of providing desktop and cloud versions of Outlook, Word, Excel, PowerPoint and OneNote along with hosted Exchange and SharePoint.

Additional packages from Microsoft are used with the base Office 365 licence:

- Azure AD to provide resilient active directory services
- Office 365 Advanced Threat Protection.

Office 365 Advanced Threat Protection checks email attachments and links for malware, blocks malicious files in SharePoint online, and attempts to detect phishing attacks and spoofed emails.

Two Factor Authentication

Two factor authentication is achieved using hardware 'YubiKeys' to act as the second factor for two factor authentication. These can be connected directly to a laptop using USB, or to a mobile phone using NFC wireless communications, allowing access to your Office 365 account from both PCs and mobile devices.

Security Incident Event Management (SIEM) and Security Operations Centre (SOC) integration

CyberHive Gatekeeper generates an archive of logs from the various components of the solution which are stored in S3 cloud storage. If required, the customer can feed these logs into a SIEM platform configured to raise alerts to a Security Operations Centre.