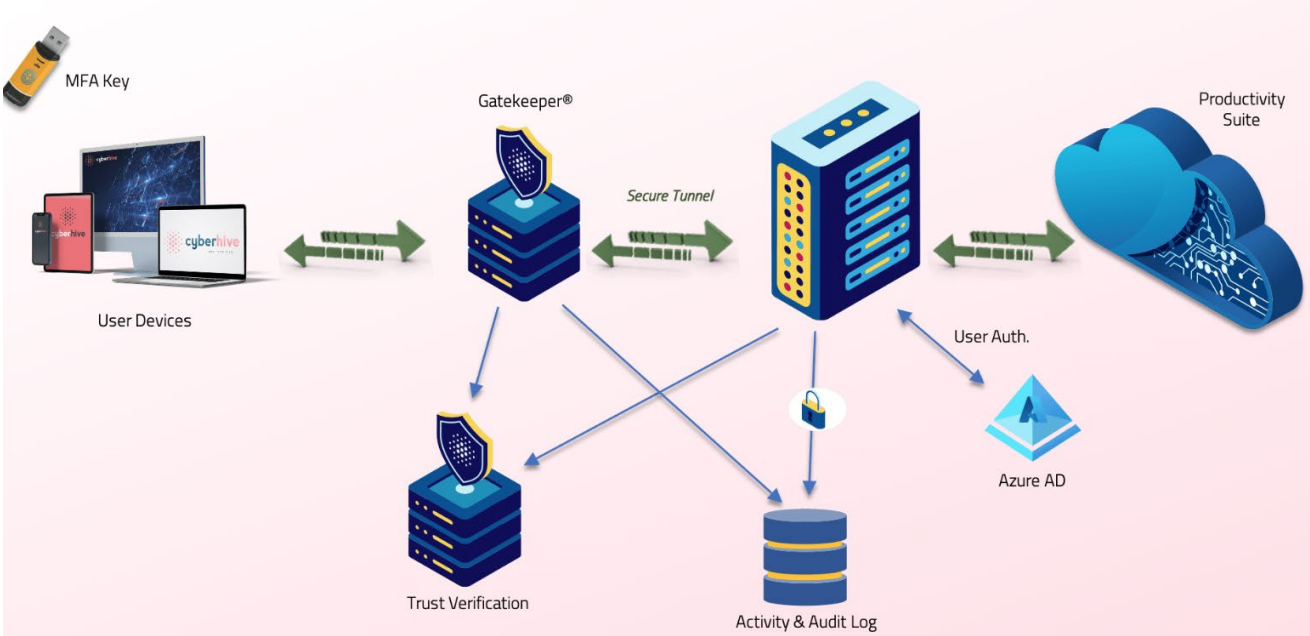
CyberHive Gatekeeper for Microsoft 365

Microsoft 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 Microsoft 365 commercial customers worldwide. Microsoft 365 also offers great flexibility, allowing users to benefit from cloud services, accessing emails and files from anywhere.

Unfortunately, this very flexibility can result in 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 fool proof.
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 can result in significant security weaknesses.

CyberHive Gatekeeper for Microsoft 365

Recognising these weaknesses, CyberHive has designed and implemented a truly secure implementation of Microsoft 365 which overcomes many of the issues associated with alternative technologies.



CyberHive Gatekeeper for Microsoft 365 is a private cloud service, built specifically for your business and managed for you by CyberHive.

CyberHive Ltd
Registered office: 2nd Floor ▪ Newmarket House ▪ Market Street ▪ Newbury ▪ Berkshire ▪ RG14 5DP
Registered number 03974231 ▪ Registered in England & Wales
www.cyberhive.com

It is a Software-as-a-Service (SaaS) solution provided on the industry-leading AWS cloud, with a private instance provided for each customer. The proven CyberHive design takes care of everything needed to give your business a fully functioning and secure Microsoft 365 environment. It is quickly configured and deployed for you by CyberHive's skilled team and all you need to do is connect your users' devices and get on with business.

The entry-point to the service is controlled by a VPN gateway, which is configured as a high-availability pair and is dedicated to your business. **CyberHive Gatekeeper** is able to lock out lost or stolen user devices (such as laptops), therefore your business is completely secure from the threat posed by lost, stolen or withdrawn devices being used to access your information.

This means your business will have a highly performant and secure, yet simple to use, Microsoft 365 environment.

Our solution offers a huge number of other benefits including:

- simple to use with your existing client devices and quick to deploy for you; with only a minimal footprint on your client devices such as laptops and mobile phones (minimum specs apply);
- based on proven design and industry-leading components, it is simple to comply with best practice – such as providing robust security logging out-of-the-box with no further decisions needed;
- your business information is secure - protected by elevated and unbypassable security, yet retaining simple user access.

The CyberHive Gatekeeper for Microsoft 365 service keeps things simple and secure, yet totally performant of your business needs.

Simple to use

CyberHive Gatekeeper for Microsoft 365 is designed to be extremely simple to use for the end-user because it avoids introducing complex log-on procedures.

The user's endpoint device (e.g. a laptop or mobile phone) uses a pre-installed security certificate which enables automatic connection to the service through the protective VPN. This is totally transparent to the user who does not need to enter a VPN password. Devices that do not have a valid certificate cannot connect to the VPN and gain access the service.

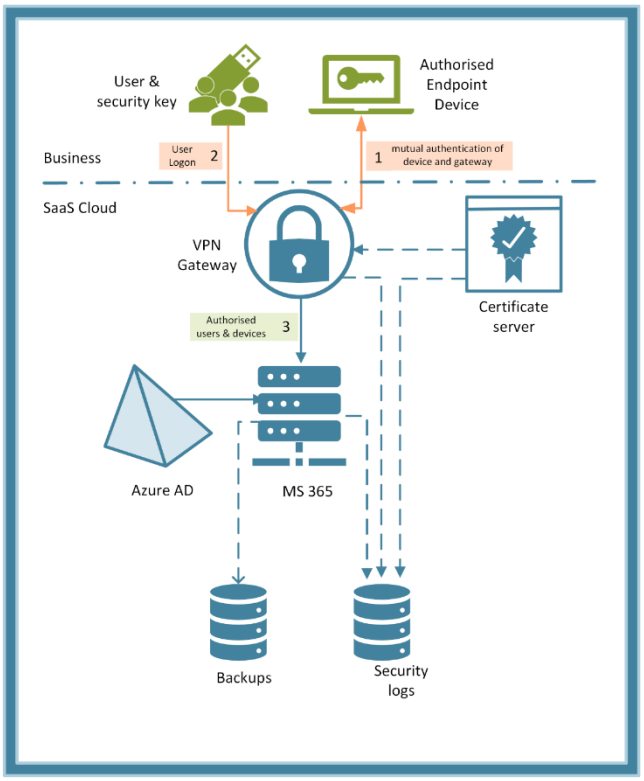
Once the device is connected, the user will personally log-on with their password and a dedicated USB security key (we specify Yubikey 5 as MFA).

This means that no single security lapse can result in unauthorised access to the Microsoft 365 account since all access requires the combination of a pre-approved endpoint device, a user account with password, a security key and a personally issued security certificate.

CyberHive Ltd
Registered office: 2nd Floor ▪ Newmarket House ▪ Market Street ▪ Newbury ▪ Berkshire ▪ RG14 5DP
Registered number 03974231 ▪ Registered in England & Wales
www.cyberhive.com

Secure design

CyberHive Gatekeeper is a Software as a Service (SaaS) solution provided on AWS cloud, a private instance is provided for each customer and this is deployed and administered by CyberHive. Deployment of the service is a highly standardised process carried out by our skilled CyberHive team.



The entry-point to the service is controlled by a VPN gateway, which is configured as a high-availability pair and is dedicated to the customer.

For customers that require the service to include lockdown to a range of source IP addresses such as a corporate gateway, an additional VPN gateway can be provided.

The VPN is configured to require bidirectional authentication based on dual digital certificates, meaning that the client must authenticate the gateway certificate and the gateway must authenticate the client certificate before mutual trust is established. This aims to prevent man in the middle attacks. Once mutual trust is established the user can proceed to be authenticated and access the service.
A private certificate authority server is used to generate certificates for the VPN and customer's endpoint devices.

In the event of endpoint device (e.g., laptop) loss or theft, the client certificate of the misplaced hardware can be added to a certificate revocation list on the VPN gateways hence locking out the device.

Access to Microsoft 365 is controlled by Microsoft Azure Active Directory (AD). This central repository is configured with details and access rights of the business users within the system and will verify the username, password and security key before permitting access within Microsoft 365. Conditional access policies can also used to enable fine-tuned restrictions where required by your business.

The service also uses Microsoft 365 Advance Threat Protection to check email attachments and links for malware, blocks malicious files in SharePoint online, and attempts to detect phishing attacks and spoofed emails.

CyberHive Ltd
Registered office: 2nd Floor ▪ Newmarket House ▪ Market Street ▪ Newbury ▪ Berkshire ▪ RG14 5DP
Registered number 03974231 ▪ Registered in England & Wales
www.cyberhive.com

Appropriate security logs are recorded from key components such as the VPN gateway, the certificate server, and Microsoft 365 and stored on immutable cloud storage.

A standard backup solution is included for the customer's business data.

Administration access by CyberHive is highly controlled with key-based authentication and connections restricted to an allow-list of approved management IP addresses.

Fast deployment – reliable administration

CyberHive Gatekeeper is provided as SaaS on the AWS cloud. CyberHive deploys it as a private instance specifically for each customer. The service includes the appropriate level of Microsoft 365 licences to ensure availability of all the facilities required. Deployment uses CyberHive's standard and approved architecture and our scripted approach allows it to be rapidly yet confidently deployed. Configuration of the customer's endpoint devices with the digital certificates and issue of the Yubikey USB tokens will be agreed with the customer.

The service is remotely administered by the CyberHive team located in the UK, using enhanced authentication.

Reliable and resilient

The critical firewalls, VPNs, servers and networking components deployed in CyberHive Gatekeeper use multiple redundant servers and systems to ensure that no single failure can result in losing access to your Microsoft 365 service. By using multiple independent security technologies, no single configuration error, such as an Active Directory configuration problem, can lead to a data breach.

Microsoft 365

The Microsoft 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 including:

- Azure AD to provide resilient active directory services
- Advanced Threat Protection which checks email attachments and links for malware, blocks malicious files in SharePoint online, and attempts to detect phishing attacks and spoofed emails

Enhanced authentication

Multi-factor authentication can be achieved using most standard 2 factor authentication systems. For maximum security this is achieved using hardware 'YubiKeys' to act as the second factor. These can be connected directly to a laptop using USB, or to a mobile phone using NFC wireless communications, allowing access to your Microsoft 365 account from both PCs and mobile devices.

CyberHive Ltd
Registered office: 2nd Floor ▪ Newmarket House ▪ Market Street ▪ Newbury ▪ Berkshire ▪ RG14 5DP
Registered number 03974231 ▪ Registered in England & Wales
www.cyberhive.com

Ready for your SOC and SIEM

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 Microsoft 365 and all other cloud platforms and services and automatically transfer them to the activity datastore.

CyberHive Gatekeeper generates an archive of logs from the various components of the solution which are stored in S3 cloud storage. Data will be available for exploitation by your existing or future Security Operations Centre (SOC) and Security Incident and Event Management (SIEM) system.

Flexible – your business – your choice

CyberHive is responsive to the detailed requirements of your business, therefore several things can be excluded or included as options or alternatives, including:

- The method of deployment of certificates to your endpoint device estate can be achieved in several ways and we will explore with you the most suitable for your business;
- If your business has extended requirements for connectivity, perhaps encompassing restricted corporate gateways as well as work from home, additional VPN gateways can be provided;
- specific requirements for the configuration of the Microsoft 365 environment;
- a balanced set of audit log recording is configured as standard and these are stored in immutable cloud storage for one year. If the business requires additional logging this can be designed in for you;
- the geolocation of the AWS cloud can be as required by the client (within the extent of AWS service), so for example a UK entity can specify UK hosting;
- CyberHive can, if the customer wishes, create or takeover and then manage, the customer's domain that will be used with the service.

About CyberHive

With over 20 years' experience, CyberHive brings you a new standard in cyber security. Helping to protect your data not only from external threats, but also from any security lapses by employees, which could damage your business reputation and even result in a loss in revenue. CyberHive offer innovative, scalable and secure solutions including Gatekeeper for Microsoft 365, the award winning Trusted Cloud, and CyberHive Connect.

Cyber Security is not just a technology decision, it's a business decision.

CyberHive Ltd
Registered office: 2nd Floor ▪ Newmarket House ▪ Market Street ▪ Newbury ▪ Berkshire ▪ RG14 5DP
Registered number 03974231 ▪ Registered in England & Wales
www.cyberhive.com

Act now and get in touch

Don't leave your organisation open to attack, safeguard your cloud workloads, critical connections, and sensitive data today.

For further information on how CyberHive can protect your business, contact the CyberHive team.

Contact info@cyberhive.com or visit www.cyberhive.com to find out how CyberHive can protect your business.

CyberHive Ltd
Registered office: 2nd Floor ▪ Newmarket House ▪ Market Street ▪ Newbury ▪ Berkshire ▪ RG14 5DP
Registered number 03974231 ▪ Registered in England & Wales
www.cyberhive.com