ESSENTIAL PLUS SECURITY

ACTISOFT TECHNOLOGY LIMITED

Overview

Modern cyber threats use multiple vectors to attack, from malicious email attachments and links to infected web ads to phishing sites. The bad actors combine a range of tactics and the threats are constantly evolving which increases the likelihood of success.

Multiple layers of security are in response to today's ever-changing threat landscape. With each layer, an additional level of protection is added making it more challenging to find ways to infiltrate your systems. While each layer in and of itself is not an adequate defence mechanism, layering them together improves each one's efficiency and success in blocking attacks.

A multi-layered security approach protects your systems against threats before they happen, proactive defences to protect your company and brand reputation.

Our Foundation Security Bundle is fully managed and ideal for businesses of more than 15 users, it is cloud-based and managed centrally so you are protected everywhere you are working and at all times.

Email Security - Spam and Malware Protection

The extensive features and thorough filtering mechanisms of our Spam & Malware Protection module keep mailboxes free of annoying and harmful spam with a guaranteed 99.9% spam detection rate and 99.99% virus detection rate.

- Email Live Tracking shows all processed emails in a single view
- Compliance Filter adds additional filters to prevent data loss
- Content Control blocks various file types on incoming and outbound emails
- Threat Defence uses machine learning to prevent spam and viruses

Endpoint Protection

The foundation of an advanced cyber resilience strategy is highly effective multi-vector protection and prevention. Cyber resilience starts by stopping the attacks aimed at endpoints and their users. Advanced, next-generation, and automated, Webroot Business Endpoint Protection:

- Stops malware, ransomware, known and unknown infections
- Protects against file-based and fileless scripts, APTs, exploits, and evasive attacks
- Stops phishing and users identity and credential theft
- Automatically remediates and returns local endpoint drives to pre-infected state without reimaging

Email Security - Advanced Threat Protection

Ransomware, spyware and viruses manipulate or damage operational and production processes which can cause considerable operation, reputational and financial damage. The Advanced Threat Protection module detects even the most sophisticated cyber attacks.

- ATP Sandboxing with detailed reports (screenshots, signatures detected)
- Targeted Fraud Forensic Analysis
- URL Malware Control (with Realtime navigation protection)

0203 931 0199
hello@actisofttechnology.com
www.actisofttechnology.com

ACTISOFT TECHNOLOGY LIMITED

ESSENTIAL PLUS SECURITY

ACTISOFT TECHNOLOGY LIMITED

DNS Protection

Every business uses the internet, and every internet connection uses DNS. Unless you privately and securely filter all DNS requests, your business is at risk. The next layer of a comprehensive cyber resilience strategy must be domain layer security that can provide both privacy and security by supporting DNS over HTTPS (DoH). Webroot DNS Protection:

- Automatically filters DNS and DoH requests to malicious and dangerous domains, blocking 88% of known malware before it can hit your network or endpoints*
- Provides private DNS resolvers in Google Cloud™ to stop internet usage request surveillance by bad actors, or those mining data for profit
- Provides network, IP address, and user policy management over bandwidth and unproductive or noncompliant internet access, using 80 URL categories
- Uses the most timely, accurate and reliable DNS filtering intelligence backed by the Webroot BrightCloud® Web Classification Service

*Based on Webroots internal testing and threats identified after scanning real-world network traffic

Cloud to Cloud Backup & Recovery for Microsoft 365 and G Suite

There are many studies that report on how data loss can be pretty devastating for an organisation but the time lost in attempting data recovery can soon mount up and be as equally damaging.
How long could you afford to be without your data?
Cloud-based data is vulnerable to:

- Malware damage and Ransomware Attacks
- Accidental or malicious deletion
- Retention policy gaps and confusion
- Cancelled user licences causing data loss
- Intentional or accidental data overwrites
- Lost time when restoring data

Our Backups provide:

- Cloud to Cloud Agentless Deployment
- Unlimited Data Backup Space
- Unlimited and Flexible Retention/Versioning
- Scheduling Function
- Multiple Restore Options
- Point-in-time Recovery

All data has 256 bit encryption.

Email Continuity

Protect from interruption of your business operations due to email server/service failure.

- All emails are available via an alternative mailbox
- Email traffic is stored for 90 days. If emails are accidentally deleted or lost they can be instantly retrieved
- When your email server is available it automatically adds missing emails
- Guaranteed availability of 99.9%

Firewall Management

Purchase a FortiGate Next-Generation firewall and FortiCloud and we manage it. Fortinet's Security-Driven Networking approach provides tight integration of the network to the new generation of security.

- Delivers industry's best threat protection performance.
- Delivers advanced networking capabilities.
- Protect against network exploitable vulnerabilities

work securely, everywhere, every time

0203 931 0199
hello@actisofttechnology.com
www.actisofttechnology.com

ACTISOFT TECHNOLOGY LIMITED

ESSENTIAL PLUS SECURITY

ACTISOFT TECHNOLOGY LIMITED

Domain Dark Web Monitoring

The dark web is a part of the internet where most criminal activity occurs. It is the preferred space used by cyber criminals to buy and sell stolen data online. Business and personal credentials can be acquired by the highest bidder.

If any of your credentials or personal information are out there on the Dark Web, then you have suffered a data breach. That data breach could have occurred at any time, on any insecure website or through a suspicious link in an email, or even through an app on your mobile phone. The danger is that your valuable data and credentials are in the hands of capable cyber criminals, and you don't even know about it. What do you think will happen next?

How could you ever know if you have suffered a data breach and your credentials are in criminal hands and available on the Dark Web?

Only by using a Dark Web Scanner. Dark Web monitoring or scanning is a security process that constantly monitors dark web activity across the globe looking for any breach data linked to your email domain, business email accounts and even personal email accounts.

We run 24-hour scans on your accounts to discover any new breaches related to your personal or business domain email accounts. You will be alerted immediately when a breach has occurred. Giving you such important details as which email account, which password and whether it has been decrypted and even when and how the breach occurred, where available.

That's why Dark Web monitoring is vital for your business. It's the intelligent way to prevent future attacks, and mitigate past breaches.

As Dark Web monitoring is an identity theft prevention process, it allows you to monitor any presence of your confidential business data on the dark web and be notified immediately if your stolen credentials are found online. You don't have to worry, as we do the scanning for you.

Password Manager

81% of breaches are from a failure to secure passwords and credentials. Protect access to applications, systems, secrets and IT resources with zero-trust irrespective of the platform or device.

When an employee leaves the organisation what happens to sensitive information such as passwords? Will they always be accommodating and prepared to provide them? Our Password Manager allows you to take immediate control of a departing employee's business password vault and transfer it to another user or block access to it.

- Safeguard against Ransomware Attacks
- Protection against Account Takeover
- Prevent breaches
- Ensure Compliance

work securely, everywhere, every time

0203 931 0199
hello@actisofttechnology.com
www.actisofttechnology.com

ACTISOFT TECHNOLOGY LIMITED

ESSENTIAL PLUS SECURITY

Online Quarterly Reviews

We will review your security with you each quarter to check your security posture and ensure that your productivity isn't being hampered. Review any organisational changes and identify any security-related issues and determine the level of risk associated with them and make informed decisions about risk mitigation or acceptance.

Check that all compliance requirements are being met.

Help Desk

Log support issues via email, web portal or phone. Check the status of any support issues via the portal.

Monthly Reporting

Receive monthly reports on the level of threats blocked by your managed services, including emails blocked, blocked web traffic, endpoints protected and any passwords compromised in the period (you will be notified of any compromises as they happen).

Overview

By partnering with a Managed Security Service Provider to look after your IT Security you'll benefit from specialist expertise that organisations would struggle to justify in terms of cost. We proactively monitor your security to allow you to focus on growing your business.

Additions

Add the following products/services to enhance your security posture;

- Security Awareness Training
- Cyber Essentials Certification
- Security Keys
- Monthly Vulnerability Scans

work securely, everywhere, every time

0203 931 0199
hello@actisofttechnology.com
www.actisofttechnology.com