

## Cyber Security Services Overview

Attacks happen because cybercrime is lucrative. A hacker's primary aim is to steal, capture, hold hostage or destroy information – usually for financial gain.

With this in mind, cybercriminals have become incredibly proactive and they continue to evolve.

Therefore, organisations must be as determined as they are about staying secure, by developing strategic approach to prevent and detect cyberthreats.

Without the expert knowledge and the right security measures in place, your organisation can be at risk from a variety of cyber threats.

Having a trusted cyber security provider ensures that an effective cyber security solution is put in place as well as the added benefits of:



Remaining GDPR compliant to industry standards



Access to high-level security services & solutions



Access to best-of-breed products



24/7 support & network monitoring



A high-level security consultancy on your side

## Preventative Cyber Security Measures

At Silverbug, our team specialise in secure IT solutions to prevent a cyber threat from taking advantage of your business.

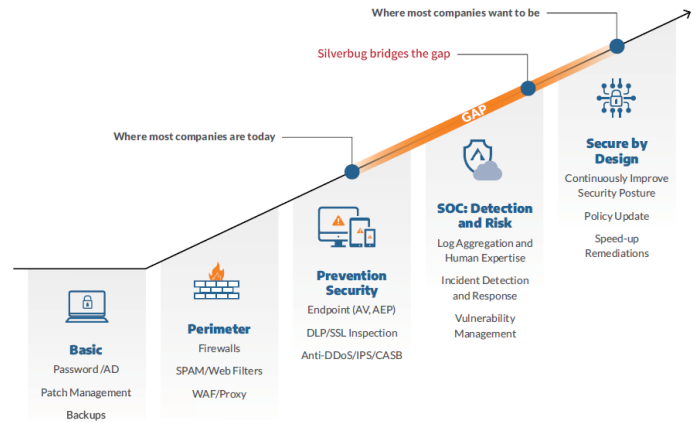
Using our layered approach, Silverbug can offer a variety of Managed Cyber Security services and solutions, such as:

- Endpoint detection and response (EDR)
- Mobile device management (MDM)
- Change and permission auditing
- Device encryption
- Email and web security
- Multi-factor authentication

## Evolution of Cyber Security

Using only preventative measures to secure your data is simply not enough anymore.

For businesses aiming to be secure, it's important to be utilising a layered approach that includes proactive measures to cyber security.



## Proactive Cyber Security Measures

Adopting a Security Operations Centre will provide organisations with complete visibility into their entire network, detecting hacker activity and ceasing potential or active cyber-threats.

Silverbug can offer a Managed Security Operations Centre named Silverbug Guardian, enabling us to proactively detect, analyse, investigate and remediate cyberthreats found in your network.

We will be working in the background, preventing cyber-threat from entering the network using the following methods:

- 24/7 Managed Detection and Response
- 24/7 Proactive Monitoring
- Compliance Management
- Log Management
- Intrusion Detection System (IDS)
- Security Incident & Event Monitoring (SIEM) technology



## Security Assessments

While your organisation may have the right cyber solutions in place, it's always beneficial to conduct an annual security assessment of your IT infrastructure. This will be to ensure that all systems and processes are working as intended and highlight any weaknesses that need remediating.

### Penetration Test

Designed as a focused security analysis on a product, application, or process, to expose potential or active flaws, unpatched software or any other weaknesses.

### Red Team Engagement

Designed as a full-scale security assessment across the entire organisation, utilising various skills including, full exploitation, vulnerability chaining and social engineering etc.

## Improve your Cyber Security Posture

**73%** of UK organisations feel their in-house teams lack the capability or expertise to fend off a ransomware attack or sophisticated threats.

**39%** of IT teams find the number of security alerts & updates, they receive are overwhelming and unmanageable.

**55%** of IT members have ignored a known security incident to prioritise another business activity.

**1 in 5** IT members have admitted to ignoring security alerts altogether, which can result in lingering vulnerabilities

---

Web: [www.silverbug.it](http://www.silverbug.it) | Tel: +44 345 565 1953 | Email: [consult@silverbug.it](mailto:consult@silverbug.it)  
#WeGetIT #ProjectSilverbug

