SOLACE CYBER

REMOTE WORKING:

How to reduce the risk of cyber attacks

REMOTE WORKING:
How to reduce the risk of cyber attacks

EXECUTIVE SUMMARY

The working world has changed. With government-mandated restrictions now removed and offices reopening, traditional working has not returned to how it was pre-pandemic. Employees have enjoyed the benefits of home working and successfully adapted to a hybrid version of remote working, with most businesses now allowing for more permanent flexible working options. Typically, businesses only require two days in the office per week, ensuring there is adequate face time between colleagues to complete any tasks that are office-based and maintain a level of culture. Furthermore, having flexible and remote working has become a non-negotiable for attracting and retaining the best talent.

At the start of the pandemic, remote working had been viewed by many stakeholders as both a challenge and an opportunity. Some of the benefits of remote and hybrid working allowed for a reduction in office space and the associated overheads, plus a greater sense of employee wellbeing. However, the benefits were counteracted by a concern that if employees were not at their office desks working, there was uncertainty that the same level of effort would be made against their workload. The increased use of presence-based applications like Microsoft Teams allowed companies to see if their employees were working, KPIs became more focused on output and general feedback was that net productivity had actually increased with the majority of the workforce operating from. Despite some initial scepticism from business leaders surrounding hybrid working, the consensus soon began to shift to support a largely remote workforce.

TECHNICAL CONSIDERATIONS FOR REMOTE WORKING

When working from home was first initiated during COVID-19, the primary business concerns focused on making sure that employees could continue to work without access to their normal offices. Whilst IT teams would have considered cyber security risks when deploying laptops to users, traditional security tools such as Security Information and Event Management (SIEM), web filtering and data exfiltration detection were usually placed behind the firewall and would not capture inbound/outbound traffic once the data was outside the network perimeter. Hybrid or remote working has now become the norm for most organisations and there are new threats that need to be considered. Employees laptops will be connected to home networks, IoT devices and even home routers, which now pose a potential risk to the organisation. Phishing risks to employees are growing exponentially and many new attack vectors are taking hold by focussing on the remote worker.

Following the expedited deployment of technology to optimise home working, it is important that business leaders strongly consider the increased security risks and the approach to mitigating them. Continuous cyber education also plays a big role ensuring all staff are always up to date on current risks and techniques aimed at getting their information or their corporate access credentials.

.

SOLUTIONS TO SECURE EVERY ENDPOINT FOR REMOTE WORKERS

Many business leaders believe that their current anti-virus will provide adequate protection against cyber attacks. However, traditional anti-virus products are slow to react to threats as they are signature based. This means that when a new virus is discovered, the security vendor will need to analyse it and create a signature to detect it before it is distributed to the clients.

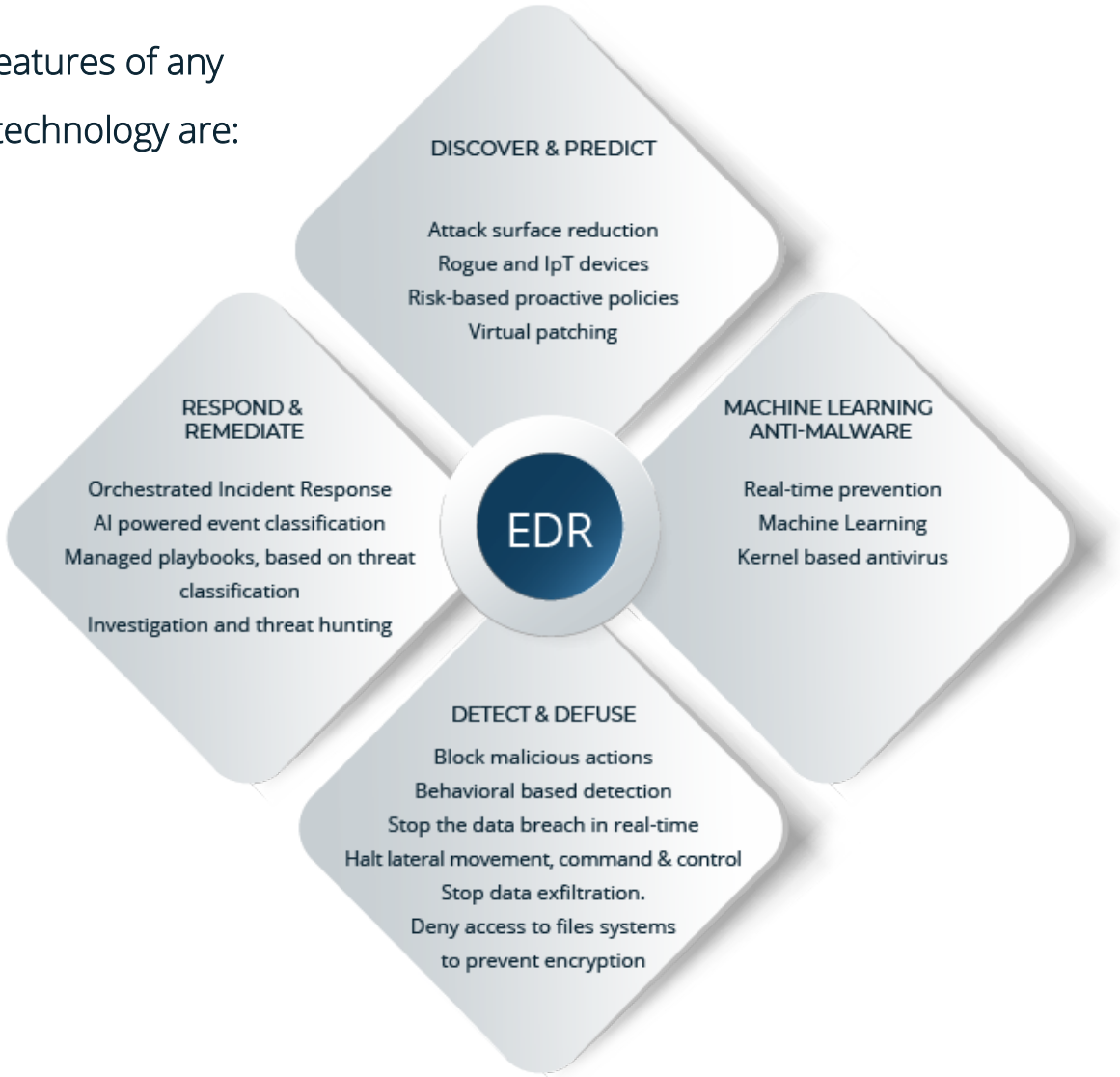
The more significant risks faced by organisations today are much more advanced and typically exploit zero-day vulnerabilities (weaknesses in code which are discovered that day). Technology vendors would not be aware of the problem and are unable to develop and distribute a security patch ahead of cyber attackers exploiting the vulnerability. Ransomware is now the typical endgame of exploits, it has now become so advanced that ransomware will adapt and mutate at such a pace, traditional signature-based anti-virus protection is unable to detect it.

ENDPOINT DETECTION AND RESPONSE (EDR)

To address these challenges, organisations are looking for a comprehensive endpoint security solution, one that provides much needed visibility into remote endpoints and enables them to not only protect themselves outside the bounds of the corporate network and its security controls, but also will self-heal in the event of an incident, without the need for human intervention.

Solace Cyber Managed Detection and Response (MDR) solution uses either FortiNet's FortiEDR platform or Microsoft's Defender for Endpoint (depending on client preference) providing cloud-based monitoring of your endpoint traffic and activity, that is analysed 24x7x365 by our Security Operations Centre (SOC).

Key features of any EDR technology are:



EDR differs from traditional anti-virus technology by intelligently tracking certain behaviours, as opposed to specific signatures. This provides advanced protection against all threat types, including zero-day vulnerabilities.

That said, any EDR technology is only as good as the people who configure, deploy and manage it on an ongoing basis. Solace Cyber differs from 'out the box' EDR solutions by spending a 60-day integration period within your business to learn the nuances of each organisation. What may cause a false positive alert for one company, could be a severe threat for another. This creates a finely tuned security platform.

Next generation security technologies such as EDR are best administered by the subject matter experts who can provide the people, process and peripheral technologies to create a functional security ecosystem. Further information can be found at Managed Detection & Response (MDR) - Solace Cyber.

ZERO TRUST NETWORK ACCESS (ZTNA)

Zero Trust Network Access (ZTNA) solves a number of problems relating to remote workers. Historically, remote workers would have operated a client VPN that had predefined access based on central firewall rules. This was often generic, the parameters were too wide and did not provide tailored restricted access to the individual. Additionally, to maintain corporate policies for internet access on corporate devices, all traffic would have to be tunnelled back to a central location, thereby increasing bandwidth requirements and latency. This issue has increased due to the uptake in SaaS services such as Office 365 or Teams that require a lot of bandwidth or are more sensitive to latency.

FORTICLIENT ZTNA EDITION

The Solace Cyber approach to ZTNA allows for the security fabric to be extended to the users directly using cloud-managed FortiClient solution. Remote users can maintain their security policy compliance by taking the traditional internal policies and running them directly on the endpoint devices. This cloud-managed solution can maintain access to corporate services by either individually tailored ZTNA VPN access, or by using automated tunnels to allow access to applications without the need for the VPN.

Web filtering is also provided directly on the endpoint to save SaaS applications or Internet traffic having to traverse back to a central location. This can all be tailored or it can be synchronised with the central Firewall to ensure minimal administration and full compliance with any policies that are already in place.

KEY FEATURES OF ANY ZTNA TECHNOLOGY ARE

- Zero trust agent with MFA
- Central management via EMS
- Central logging & reporting
- Dynamic security fabric connector
- Vulnerability agent & remediation
- SSL VPN with MFA
- IPSEC VPN with MFA
- FortiGuard web filtering
- USB device control

Solace Cyber offer a fully managed service for FortiClient deployments, including on-going proactive maintenance and incident support. This service is provided 24/7/365 by our Security Operations Centre (SOC) and supported by our FortiNet accreditations.

For further information around Solace Cyber Secure Edge & Remote Access solutions please see Secure Edge & Remote Worker Security - Solace Cyber.

END USER CYBER EDUCATION

It is becoming commonplace for organisations to provide their workforce with regular cyber training programmes, this ensures employees are educated to become self-vigilant when spotting potential security threats. These training programmes are often coupled with simulated phishing tests that will identify and report on the users most likely to fall victim to socially-engineered cyber attacks. Indeed, many insurers now mandate a cyber training and simulated phishing programme to be active, in order for organisations to reduce their cyber insurance premiums.

To ensure all staff are always up to date on current risks and exploitation techniques, Solace Cyber offer continuous cyber security education, which is key to maintain, as threats evolve rapidly and user awareness is a great defence.

Cyber education is provided in three different ways;

1. **Phishing**

Phishing emails are sent at regular periods with the aim of replicating seeming legitimate messages with some noticeable errors. Those users that proceed to click the links embedded within these emails are logged and this helps to identify which employees may need additional training.

2. **Group Sessions**

Solace Cyber run group sessions to re-enforce current risks and exploitation techniques over Microsoft Teams. We provide a dedicated senior security consultant to run these meetings, to make them more interactive, answer any questions and show additional examples here required.

3. **Online Education**

Web-based training is also available and Solace Cyber ave access to education libraries that allows customer-specific packages to be built and consumed at an agreed iteration (e.g. monthly). The benefit of web-based training is that it can be completed at each person's own pace. This training covers all aspects of security awareness.

Protect your remote workers from cyber threats

Discover free resources and risk assessments, to help identify your organisation's cyber security position.

- Learn more about Solace Cyber educational programmes
- Book a free of charge Cyber Risk Assessment

Contact our cyber risk management specialists today

cyber@solaceglobal.com

+44 (0)1202 308810