SENSEON

lineup

Securing a Remote Workforce:

Tips for Staying Safe in an Uncertain World

Introduction

Like so many others, in mid-March Lineup's staff began working remotely. Work carried on at its usual rapid pace across all of our teams, now spread out in thirteen different countries. By all accounts, we have been very privileged to remain busy, productive, and yes, secure. This is not by accident – we've taken concrete steps to ensure we can protect ourselves and our customers during this time and beyond.

Outside the secure, controlled environment of a traditional office lurk many security threats, and no IT team can protect against them all without help. That is why we have not only implemented security systems and procedures, but we've also made a concerted effort to educate the wider Lineup team on these measures, so that each and every employee is as secure as possible.

In the last several months, we have:

- Become an ISO/IEC 27001 accredited organization
- Delivered base level of security awareness training (completed by 98% of staff within the first two weeks)
- Run regular phishing tests and delivered targeted training, effectively reducing our phishing risk to 1.6% (industry standard is 12.2% or lower)
- Tightened our password strength policies, expiring system passwords and implementing multi-factor authentication
- Completed a device audit on every company-owned device and encrypted all hard drives
- Implemented a technical solution (Senseon) to detect and respond to dangerous network activity
- Meticulously secured and backed up Adpoint to reduce our customers' risk

Of course, this list is not comprehensive, and there will always be new threats to address. But these decisive actions have no doubt secured our team and reassured our customers worldwide.

To that end, this whitepaper will share actionable advice from our chosen cyber-defense platform, Senseon. We've followed this advice and educated our staff on potential threats. Whether you're planning to continue remote working long-term, adopt a hybrid model, or eventually return to the office, this is an excellent place to start.

Share this information with your team, even your customers. I'm confident you'll find it useful.

Best,

Rob Hesmondhalgh
Chief Information Officer

TABLE OF CONTENTS

Understanding the Scope of Data and Cyber Attacks During COVID19

An increasing number of malicious actors are exploiting the Coronavirus pandemic for their own objectives. The UK's National Cyber Security Centre has detected more UK government branded scams relating to COVID-19 than any other subject. Within this section, we will provide an overview of Coronavirus related malicious activity. Malicious actors have been indiscriminate in their exploitation of the pandemic, targeting individuals small and medium businesses, as well as large scale enterprise organisations.

VARIETY OF ATTACKS

APT groups and cyber criminals are exploiting the COVID-19 pandemic as part of their malicious cyber operations. Coronavirus related attacks are varied, including phishing campaigns (using the subject of Coronavirus/COVID-19 as a lure); distributing malware using COVID-19 themed lures; registering new malicious domains containing COVID-19 or Coronavirus related wording; and attacking newly and rapidly deployed remote working infrastructure.

SOCIAL ENGINEERING ATTACKS

The Coronavirus pandemic has created conditions that significantly increase the likelihood that an attack employing social engineering techniques will be successful. Taking advantage of human traits such as curiosity and concern that are likely to be heightened at this time, malicious actors are using Coronavirus-related email subject lines to entice victims to open emails and click links. To create the impression of authenticity, malicious cyber actors may spoof the sender information in an email to make it appear to come from a trusted source, such as the World Health Organisation (WHO) or an individual with 'Dr' in their title; in other instances they may purport to be from a department within the victim's own organisation - HR, for example.

PHISHING

The NCSC has observed a large volume of phishing emails, specifically related to COVID-19. Attackers may use email subject lines suggesting the email and its attachments contain updates about the pandemic, outbreaks in the victim's vicinity or purporting to have found a cure.

PHISHING (cont.)

Phishing emails may have macro-enabled Microsoft documents which trigger the download of Trickbot or Emotet malware once opened, or which exploit known vulnerabilities to run malicious code. In other examples, phishing emails may direct users to fake websites which solicit the victim's financial information and/or credentials, such as instances of malicious actors posing as HMRC offering tax rebates/income support in light of the current climate.

Typically, phishing attempts arrive by email, but the NCSC has also observed some attempts to carry out phishing by other means, including text (SMS) messages. Historically, text phishing utilises financial incentives to lure the victim and COVID-19-related SMS phishing campaigns have followed the same theme. For example, a series of SMS messages, purporting to be from the UK Government, have been used to attempt to harvest victims' personal information and banking information. The text message includes a link directly to the phishing site.

For many APT actors, social engineering and phishing or spear phishing campaigns are the primary attack vectors by which they will seek initially to compromise a user or device before employing other tactics and techniques that can be found on the Mitre ATT&CK framework. For example, in January 2020, the APT group TA505 (AKA Dudear) launched a phishing campaign that used HTML redirectors to deliver malicious macro-enabled Excel files. In Mitre terms, TA505 used spear phishing to gain initial access as well as other techniques such as Scripting, Process Discovery and Standard Application Layer Protocol to carry out further tactics such as defence evasion and execution. The malicious excel sheet contains an embedded executable that drops the payload. Once loaded to memory, it beaconed to their command and control server. Previously, and like many phishing attack attempts, TA505 would deliver malware to their targets' devices via a malicious link in the email body, or via an attached document. However the use of HTML redirectors as attachments meant that, once opened, the excel file was downloaded automatically.

CEO FRAUD EXPLOITING SOCIAL DISTANCING

CEO fraud involves emails and phone calls made by malicious actors, impersonating senior members of staff/managers (such as the CEO, hence the name). The attacker will attempt to persuade the receiver to transfer corporate accounts to other funds, often within a very short space of time due to some sort of time critical business operation. These attacks are usually unsuccessful because when everyone is in the office environment, it is much easier for employees to attempt to verify the legitimacy of the request, by checking with the individual directly or asking a colleague/manager for their advice. Attacks of this nature are therefore far more likely to be successful as checks may be less extensive and given the external influences of the current climate, it is a perfectly reasonable expectation on the part of the attacker, that somebody trying to be helpful in the circumstances will facilitate a successful attack.

Staff with access to corporate accounts should be reminded of the policies and procedures in place when it comes to money transfers, including how requests will be made and the incident escalation policy they should follow in the event of irregular or suspicious communication.

Understanding the Scope of Data and Cyber Attacks During COVID19 *(cont.)*

INCREASED INSIDER THREAT

The current economic uncertainty relating to COVID-19, combined with the ongoing furlough scheme operated by the Government may create financial and job worries for employees. Such individuals may become a prime target for actors - in this instance, possibly foreign nation state actors, or even competitors - who might approach the potential victim with the promise of payment for divulging sensitive corporate information. Within this context, it is extremely important that the business recognises and understands exactly what its 'crown jewels' are, and how to protect them. For example, for businesses that provide financial services to mega wealthy individuals and celebrities, the crown jewels may be highly sensitive information pertaining to the financial status of their clients; for a business operating in a highly competitive and crowded market space, this could be the contents of their CRM which represents a goldmine of leads and potential opportunities for their competitors. As well as having an understanding of the most valuable assets, the business also needs to understand who has access to these - in the CRM instance for example, this is likely to be the sales team.

Employers should be as transparent as possible with employees to reduce the risk of this occurring. Perhaps now more than ever, it is imperative to play close attention to the mental and physical well-being of members of staff working remotely and in isolation; regular team check-ins and standups offer managers a good opportunity to pick up on cries for help and potentially concerning behaviour.

Where staff have been furloughed and therefore unable to work, teams could consider recalling corporate devices or limiting access to corporate applications (such as your CRM) so that, even if employees are tempted, it is harder or even impossible for them to comply with the attacker's requests.

Even with comprehensive endpoint security tools in place, these can be easily bypassed if the employee turns off their VPN and uses their home WiFi, or if the organisation has had to employ Split Tunnelling in order to reduce the impact on their VPN. Utilising a Split Tunnel VPN can render an organisation's Data Loss Prevention (DLP) tools ineffective because traffic is sent outside of the DLP tool, thereby reducing the effectiveness of controls designed to prevent data being sent externally to the organisation.

In the last section of this paper, we offer additional safety measures--like the data security tool Senseon--that can strengthen companies against these kinds of attacks in real-time. In the next section, we will consider ways executives can strengthen their company culture for cyber safety in remote working conditions.

Invest in Prevention as the Strongest Data Protection

Over recent years, information and cyber security professionals have done an exceptional job at raising the status and profile of potential breaches and security incidents to be of board-level concern. It's no longer a question of 'if' but 'when.' At times of such global upheaval and uncertainty as COVID-19 has bought, as well as the opportunities these unique circumstances present for would-be attackers, cyber security is more important than ever and the stakes have never been higher. Data breaches and security incidents are becoming costlier; take, for example, the 2018 data breach incidents which saw the ICO impose fines of £183 million and £99 million against British Airways and Marriott International respectively.

Whilst these are some of the most high-profile examples at the extreme end of the scale, it remains a universal truth that the financial implications of security incidents remain high for organisations of all shapes and sizes and across all industry verticals, particularly those subject to more rigorous regulatory requirements such as healthcare and financial services. The Ponemon Institute's (commissioned by IBM) Cost of a Data Breach Report 2020 puts the average total cost of a data breach at $3.86 million. Whilst this is a 1.5% decrease on 2019's $3.92 million, the findings from the 2020 report still contribute to an overall trend of a 10% increase in the total average costs over the past 5 years.

UNDERSTANDING CHALLENGES OF REMOTE WORK AND DATA SECURITY ATTACKS

Whilst remote working is not a new concept or practice for many organisations and employees, the requirement to do so on a much greater scale and for a longer period of time presents new risks and security challenges to teams. The UK's NCSC recently published guidance to help people through this transition which acknowledges the increased risk this transition poses. Within this section, we will explore some of the real-world attacks that malicious actors may utilise to specifically target remote workers.

> As much as a 25% of a security analyst's time is spent chasing false positives—sifting through erroneous security alerts or false indicators of confidence—before being able to tackle real findings.
>
> Ponemon Institute Report, 2019

With travel restrictions and social distancing measures enforced, many organisations are turning to software solutions in place of face-to-face meetings for everything from sales demos to board meetings. One such example is the use of video conferencing platforms, such as Zoom. Easy to set up, and allowing up to one hundred people enter a virtual meeting room for free, throughout 2020, the business has added 2.2 million new monthly users, outstripping the entire new user base of 2019, which came in at 1.19 million. There is, however, a downside: in recent weeks a number of security vulnerabilities in Zoom's software have been detected and there has been a surge in so called 'Zoombombings' whereby trolls scan the web for unencrypted meeting links (possibly posted on social media or forums), break into and disrupt meetings. This has been especially problematic for remote learning sessions during which lewd and offensive content has been broadcast into the meeting room.

UNDERSTANDING CHALLENGES OF REMOTE WORK AND DATA SECURITY ATTACKS (CONT.)

There is, however, a downside: in recent weeks a number of security vulnerabilities in Zoom's software have been detected and there has been a surge in so called 'Zoombombings' whereby trolls scan the web for unencrypted meeting links (possibly posted on social media or forums), break into and disrupt meetings. This has been especially problematic for remote learning sessions during which lewd and offensive content has been broadcast into the meeting room. These malicious communication offences are being taken seriously: in April, the US Department of Justice deemed Zoombombing a crime, and in the UK, the police have urged the public to be vigilant. The NCSC advises that any new software needed to support remote working should have guides and best practices produced and provided to employees.

A further risk with having corporate devices outside the normal office environment is the possibility of these devices being either lost or stolen, especially if employees are using public transport to commute between meetings or different offices. As per our top tips to keep remote workers safe, it is advisable that all devices should have their data encrypted at rest by utilising tools built into their operating system, such as bitlocker on Windows and FileVault on MacOS. It is also recommended that IT and security teams use some form of mobile device management software which allows administrators to remotely wipe lost or stolen devices. Employees can play their part in helping to combat the possibility of theft by keeping devices out of sight of windows and doors and staying vigilant when in public or travelling.

Employees should also be reminded of the importance of discretion when working remotely. When working from home, or public spaces such as cafes and libraries, not everyone in the surrounding area is vetted to hear or see confidential information. Children, spouses, roommates and the person peering over your shoulder may not be aware of the confidentiality level of the information they hear or see (or perhaps they are, hence the peering over your shoulder). Where possible, staff should be encouraged to work in separate rooms and should conduct calls and meetings through headphones, rather than on speakerphone.

Remote working presents a risk of employees being susceptible to man-in-the-middle attacks, whereby a malicious actor secretly relays or even alters the communication between two devices, which believe they are communicating directly. Whether you live in shared accommodation with shared WiFi, or you are using free WiFi in public, once your connection has been intercepted an attacker can inject various things into your device using the connection. Some legacy corporate applications and portals still do not use HTTPS encryption, meaning any data accessed or sent to these services (including usernames and passwords) is accessible in plaintext to other people on the network. Man-in-the-middle attacks are difficult to detect, so the best method of protection is prevention: where possible you should try to only use HTTPS sites and certainly avoid entering credentials into unencrypted sites (look for the padlock in the address bar) and make use of a VPN which will encrypt all traffic to and from the device.

UNDERSTANDING CHALLENGES OF REMOTE WORK AND DATA SECURITY ATTACKS (CONT.)

Working remotely from other colleagues and managers also increases the risk of employees falling for phishing scams. Through targeted phishing campaigns, attackers will often attempt to impersonate colleagues, sending emails with malicious documents attached or containing links to malicious websites where staff will be prompted to enter their corporate credentials.

(Moved paragraph to different section/reorganized) COVID-19, and the changes to organisations' operating models it has brought with it, has naturally had a significant impact. 70% of organisations report that having a remote workforce will increase the cost of a data breach and 76% said it would increase the time it takes to identify and contain a potential incident. Time, in this instance, really is money: according to the Ponemon Institute's report, having a remote workforce increases the average total cost of a breach by nearly $137,000.

TOP TIPS FOR PREVENTING A MAN-IN-THE-MIDDLE ATTACK

Change the configuration settings on your devices so they don't automatically connect to WiFi by default

Check if a website is encrypted by looking out for the padlock symbol at the beginning of the URL.

Don't do any sensitive browser activity such as Internet banking while connected to public WiFi networks.

If you can't avoid connecting to a public WiFi network, set your device to 'forget' the network so it doesn't automatically re-connect.

Stay alert to potentially malicious WiFi networks using a similar name to the legitimate one, for example 'Starbucksfreewifi' and 'Starbucks_WiFi_join' - one may be fake.

Look out for suspicious SSIDs (WiFi names) that don't look right.

If you absolutely must do something like online banking in a public place, hotspot from a 4 or 5G cellular connection instead.

Where available, use a VPN.

Invest in Prevention as the Strongest Data Protection *(cont.)*

COST-SAVING BENEFITS OF PREVENTATIVE MEASURES

There is a significant and growing divergence in total costs between those organisations who are prepared for such security incidents, and those who are not. Despite the overall nominal decline from $3.92 million in 2019 to $3.86 million in 2020, businesses that are lagging behind in investment in security automation (defined as the use of artificial intelligence platforms and automated breach orchestration) saw an average total cost of $6.03 million, more than double the average cost of a data breach of $2.45 million for those organisations who have fully deployed security automation technologies.

The potential for cost savings that these technologies are able to deliver is clearly recognised by the industry; the number of organisations investing in these capabilities is investing - up from 15% of respondents in 2018 to 21% in 2020. The $2.45 million average saving that investing in these capabilities delivered in 2020 has increased from $1.55 million in 2018.

This divergence has increased year-on-year and it is likely that it will continue to do so. Investing and engaging in effective cyber security practices significantly reduces costs in the event that a breach or security incident does occur.

Broad Preventative Measures: MITRE Techniques for Company-Wide Remote Work

The Mitre ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Framework is a globally accessible knowledgebase of adversary tactics and techniques based on real-world observations. When Mitre first released the framework in May 2015, tactics and techniques were a new way of representing the taxonomy of cyber attacks. Rather than analysing the results of a cyber attack after it is successful, analysts can use the tactics and techniques to see how an attack is propagated as it is in progress. Senseon uses the Mitre ATT&CK Framework heavily within our product - every event or security observation is mapped to a real-world technique to enable teams to quickly and easily understand the threats they face and adversary techniques being used against them.

Research by the IT Security organisation Anomali conducted during March 2020 when the pandemic was at its global peak, found 16 distinct campaigns attributed to 11 malicious actors or groups, distributing 42 different malware families and employing 80 various Mitre tactics and techniques.

Employees working remotely and the potential ensuing disorder created under such conditions can create opportunities for attackers, not least because an organisation's attack surface is significantly increased and the number of vectors for exploitation is also increased. The Mitre ATT&CK Framework can be an extremely useful tool here, used to better understand attackers' techniques and their likely behaviour. Organisations can then ensure they have the correct resources in place and security teams can track the techniques attackers are likely to exploit.

Within this section we will explore some of the tactics and techniques that everyone should be aware of to minimise the risk to the business, and maximise the chance of spotting potentially malicious activity.

ELIMINATE EMPLOYEE HARDWARE ADDITIONS

One of the oldest and most common ways malware is spread is by hiding itself on removable media such as USB sticks and then infecting any computer which it is plugged into. Employees should be reminded not to use personal USB devices on corporate machines, or, where possible, security teams should lock down USB ports on computers.

ENFORCE REGULAR BROWSER EXTENSION REVIEWS

In recent years, malware authors have turned their attention to browser extensions. A large majority of corporate applications now run in web browsers and as such a malicious browser extension provides an easy way for attackers to steal sensitive information.

Browser extensions require a wealth of access permissions to operate, including things like browsing history, website content and even users' credentials. Because extensions are not applications in their own right, antivirus software generally cannot detect malicious extensions. These innate vulnerabilities make them attractive to targets for malicious actors.

Broad Preventative Measures: MITRE Techniques for Company-Wide Remote Work *(cont.)*

Malicious actors may attack on two fronts: developing extensions deliberately designed to be malicious and hijacking perfectly legitimate extensions for their own nefarious purposes. Most of the time, deliberately malicious extensions are designed to steal credentials and other sensitive information, redirect user searches to affiliate pages that the developers earn money from; or redirect users to phishing sites or those containing drive-by downloads.

The danger of USB devices

According to four intelligence services, Stuxnet, the infamous malware worm that was deployed to sabotage Iran's Natanz nuclear power station in 2010, was introduced into the network via a USB flash drive.

Operation Olympic Games, a joint mission between the US and Israeli intelligence services, delivered the digital weapon via a USB flash drive that was inserted into the control systems by a Dutch mole, posing as a mechanic.

The mole did not return to Natanz.

Some legitimate browser extensions may have been hijacked by attackers. This could be accomplished through several means:

Some legitimate browser extensions may have been hijacked by attackers. This could be accomplished through several means:

1. The malicious actors may use a phishing scheme to harvest credentials for extension store accounts belonging to developers of legitimate extensions. They can then add malicious code to the extensions and push an update through.

2. They may take control of a popular extension legitimately, by purchasing it from the developer, add malicious code and push an update through.

3. They could utilise malicious code embedded on a website to compromise the API of a vulnerable browser extension.

Some extensions may also contain undiscovered security vulnerabilities, or have privacy policies that go against the organisation's policies, for example a recent Netflix extension that has clauses in its privacy policy which allow for the collection of users' behaviour.

The risk of a compromise through a malicious browser extension is significantly increased if employees don't have access to a corporate laptop and have to use their personal device to work remotely. If this is the case, IT and security teams should ensure their BYOD policy reflects this risk.

Broad Preventative Measures: MITRE Techniques for Company-Wide Remote Work *(cont.)*

MANDATE COMPANY-WIDE POLICIES TO PROTECT AGAINST DRIVE-BY COMPROMISE

A drive-by compromise is when an adversary gains access to a system via a user visiting a website over the course of normal web browsing. With this technique, the user's web browser activity is usually targeted for exploitation via a multitude of means:

- Compromising a legitimate website and injecting some form of malicious code such as JavaScript, iFrames and cross-site scripting (XSS). This is especially common on sites linked by bots across social networks like Twitter and Facebook.
- Malicious ads are paid for and served through legitimate ad providers.
- Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content).

When working from home, employees may be tempted to check the latest headlines or updates from sites that they wouldn't normally access whilst in the office. Often the website used by an adversary is one visited by a specific community where the goal is to compromise a specific user or set of users based on shared interest. Visiting non-work related sites from corporate devices should be avoided, no matter how tempted a user is to check their newsfeed or update their status.

TOP TIPS TO PROTECT YOURSELF FROM MALICIOUS BROWSER EXTENSIONS:

Only install browser extensions that you actually need and will use.

Regularly review your installed extensions, and uninstall any that you no longer need or do not recognise/recall installing

Conduct your due diligence before installing extensions: visit the developer's website, read the description and the reviews.

Watch out for spelling and grammar mistakes in the description; beware if the extension is relatively new but still has a lot of reviews - all of them five-star and similar in content; and pay attention to the ratio of downloads to reviews - if there are millions of downloads and only a few reviews, it is likely users don't know they have it installed.

Broad Preventative Measures: MITRE Techniques for Company-Wide Remote Work *(cont.)*

MANDATE COMPANY-WIDE CREDENTIALS IN FILES POLICY

f employees have been given a new device such as a laptop to enable them to work from home, they may be tempted to store their password and credentials in a text file and email this to themselves or, worse, store them on an easily lost USB device. Storing credentials in plaintext represents a security risk as adversaries may search local file systems and remote file shares for files containing passwords. Attackers may use advanced exploitation tools such as Mimikatz to perform credential dumping. If users have recycled passwords across multiple accounts, the same credentials could be used to enable the attacker to expand their access and move laterally within the organisation's environment.

Irrespective of whether the employee has been given a new laptop, all users should be encouraged to make use of password managers such as KeepPass, which encrypt passwords and enable the secure access of passwords from multiple devices.

UTILIZE EXTERNAL REMOTE SERVICES

As we have discussed previously, many organisations will have implemented services such as VPNs, Citrix and other mechanisms to enable users to connect to internal network resources from external locations, such as their own home. Remote access VPNs can serve as a devastating point of initial compromise. According to Patrick Sullivan, CTO of Akamai, this trend emerged following a presentation at Blackhat USA 2019, 'Attacking the intranet like the NSA', which provided detailed techniques that would later allow for the compromise of many of the world's leading remote access solutions.

Remote access VPNs are often highly trusted devices. Once compromised, adversaries may find themselves with privileged access to highly confidential and sensitive areas of the network.

UNDERSTANDING DLL SEARCH ORDER HIJACKING

Windows systems use a common method to look for required Dynamic Link Libraries (DLLs) to load into a program. Malicious actors may take advantage of the Windows DLL search order and programmes that ambiguous specify DLLs to gain privilege escalation and persistence. For example, in March 2020, APT17, a known Chineses state sponsored threat actor used a malicious RTF file as part of a phishing campaign to perform DLL Search Order Hijacking and load the DLL to memory.

UNDERSTANDING DLL SEARCH ORDER HIJACKING *(cont.)*

Using a COVID-19 related file name as bait, once executed it exploits a known vulnerability in Microsoft Office software (CVE-2017-11882) and drops two files in the %temp%directory: LBTServ.dll and confax.exe.

LBTServ.dll is a legitimate signed DLL which is part of the Logitech Bluetooth services.

APT17 used the Search Order Hijacking technique to load a malicious DLL of the same name to memory by executing confax.exe which then loads the LBTServ.dll residing in the current directory.

Once loaded into memory, the malware then calls to its C2 servers.

COMMUNICATION AND TRAINING

In many cases, the transition to home and remote working has been disruptive for both employees and IT and security teams alike; coupled with external stresses such as job security, finances and child care, this has been a trying and distracting time for many. These distractions could lead to staff not following general guidelines or the company's security policy. Communicating with the team to remind them of security policies may go some way in making them think twice about clicking a potentially malicious link or installing a browser plugin.

ENSURE THAT STAFF KNOW HOW TO REPORT SUSPICIOUS ACTIVITY

Attackers and malicious actors will often exploit the heightened sense of panic and emotions that situations such as the Coronavirus pandemic create for their own nefarious ambitions. Even with staff outside of their regular routine and normal company communications impacted, it is important employees stay vigilant. Remind staff of the tell-tale signs they can look out for to spot potential attacks, such as emails pertaining to be from senior members of staff requesting large and unusual bank transfers. Refresh staff on how to report suspicious activity and create a positive information security culture by praising individuals who do, in order to encourage others to do the same.

This is not an extensive list of the tactics and techniques attackers will use to exploit employees and organisations working remotely, but a few important solutions a company can enforce to protect themselves. As a knowledge base of the tactics and techniques used by over 100 APT groups, the MITRE ATT&CK framework is worthy of its own separate paper. Rather it has been designed to give you an insight into the types of techniques you can expect attackers are most likely to utilise in order to exploit the opportunities created by employees and users working remotely.

Creating a Culture of Security by Trained Collaboration between Employees and IT Teams

Beyond broad policy measurs, companies can also train employees and IT teams to work together for more targeted prevention. At an already busy time, IT and security teams may find themselves overwhelmed by the number of alerts produced by tools that rely on unusual behaviour or anomaly detection. Such tools have a tendency to over-alert because they cannot differentiate between behaviour that is simply new and unusual, and that which is genuinely interesting and malicious. Anomalies happen all the time within environments, a problem which could be exacerbated by hundreds or even thousands of devices suddenly being used from new locations and at different times of the day, so the challenge for security teams comes when they need to discern between what is simply new and unusual behaviour and that which is genuinely interesting and malicious. If you would like to learn more about this challenge, we explore the issue in more detail in our Whitepaper.

As much as a 25% of a security analyst's time is spent chasing false positives—sifting through erroneous security alerts or false indicators of confidence—before being able to tackle real findings.

Ponemon Institute Report, 2019

Where possible, teams may wish to configure their tools to suppress alerts directly related to a large number of employees working remotely. However, this should be exercised with caution to avoid the risk of important or genuine alerts getting filtered out. Suppressing or completely switching off specific alerts is a manual and time consuming task and may significantly decrease the value for money that teams receive from the tools they are using. Security professionals find themselves at an impasse: overwhelmed with a huge number of alerts for which they do not have the resources and capacity to work through. Whilst it is likely that the majority of these will be false positives and innocent anomalies, the inherent risk of suppressing these alerts is that genuinely malicious activity gets missed.

Another possible solution to this challenge is to invest in a platform that is able to automate the initial qualification and disqualification of anomalies in order to determine which is worthy of further analysis and investigation. This avoids bombarding teams with vast swathes of threat intelligence and means they have the capacity to respond to genuine attacks as and when they occur If you would like to learn more about how Senseon's platform is able to automate the process of threat detection and investigation to mitigate this risk, you may be interested to watch our demo here: http://senseon.io/demo or even take a test-drive to see for yourself.

Simple Security Tips for Remote Workers

With the vast majority of employees working remotely, the risk to many businesses has increased significantly. We have outlined the scope of the problem and some policy and team-wide measures companies can utilize to better protect themselves. However, there are also relatively simple and sensible steps that employees can take individually to ensure that teams and the business as a whole have the best defences in place during these uncertain times. Education and communication can be some of the most useful and effective tools here: as we explored in our Insider Threat eBook, the vast majority of employee-related incidents are caused through negligence rather than malice. Transparent communication may make individuals more likely to comply with seemingly inconvenient or irrelevant security controls if they understand why they are put in place.

STRONG PASSWORDS

Whilst it should go without saying, it never hurts to remind users that they should be using strong, non-recycled, passwords and, where possible, Two-Factor-Authentication (2FA). These are some of the most basic steps to protecting devices and data and is especially true when devices are leaving your normal place of work.

FOLLOW BYOD POLICIES

In many cases, employees may not have a corporate laptop. To accommodate, and to avoid having to invest a significant amount in new devices, IT and security teams may need to consider relaxing or updating their Bring Your Own Device (BYOD) policy to include the use of personal devices to enable staff to work remotely. Personal devices generally have poorer security measures in place than corporate ones, so where possible, employees should be encouraged to implement the steps in this white paper to keep the organisation secure.

USE SECURE COLLABORATION TOOLS

Secure collaboration tools, such as Slack and Google Hangouts are convenient and secure ways for teams to communicate. Where possible, ensure collaboration tools offer end-to-end encryption and store data privately. Whilst solutions such as these do lend themselves very well to enabling teams to work remotely, there are potential security risks to take into consideration as well, for example, as a direct result of the increase in consumption of video conferencing tools, there has also been a surge in instances of trolls joining and disrupting virtual meetings (see page X).

Simple Security Tips for Remote Workers *(cont.)*

USE A TRUSTED VPN

Many organisations may already have a Virtual Private Network (VPN) for its travelling workforce or devices that leave the corporate network. Teams with VPN capabilities already in place may need to review whether they can support the increase in data consumption that working from home brings with it. Before the Coronavirus pandemic, analysis of global traffic showed that 10% of traffic coming into the enterprise was from remote working during the week, rising to 20% at the weekends. In China, during the peak of the crisis, it peaked at 70% during the working week and is now back down to 40%. If the VPN you are currently using will not support this increase, it could lead to frustratingly slow connections, or a loss of connection entirely, impacting on the productivity of your workforce.

For those without a VPN already in place, there are plenty of trusted, open-source options available, however you will need to consider the hardware and setup implications.

It is important to encourage staff not to install their own VPN software. There are lots of examples of untrusted VPNs that collect user's data and share this with third parties, or even malware masquerading as free VPN software.

HOW TO KEEP YOURSELF SAFE WHEN USING ZOOM:

Don't use your personal meeting ID; instead, use a per-meeting ID, exclusive to a single meeting.

Only share your meeting ID privately: do not post it on social media or open forums where anyone can easily find it.

Disable other options, including the ability for others to join the meeting before the Host, screen-sharing for non-hosts, the remote control function; as well as all file transferring, annotations and the autosave feature for chats.

(For paid Zoom accounts), create an invite-only meeting, meaning only people you invite can join the call, and they must sign in using the same email address you used to invite them.

Enable the 'Waiting Room' feature. This means you can see who is attempting to join the meeting before you allow them access which means if you see names you don't recognise, you don't have to let them in.

Inevitably, an unruly participant will sometimes manage to slip through the net. Remember, as the meeting host, you have the power to remove a participant mid-call. By default, an ousted guest cannot rejoin.

Once all the participants are in and the meeting begins, lock the meeting to outsiders. Consider assigning meeting co-hosts who will be able to help control the situation in case anyone bypasses your efforts and causes trouble whilst you are presenting.

Simple Security Tips for Remote Workers *(cont.)*

ENSURE ANTI-VIRUS SOFTWARE IS UP-TO-DATE

Anti-virus is one of the most basic measures an organisation can take to detect threats based on previously seen attacks. IT and security teams should ensure that all devices leaving the office have AV installed and, where already in place, that they are up to date.

KEEP OPERATING SYSTEMS UP-TO-DATE

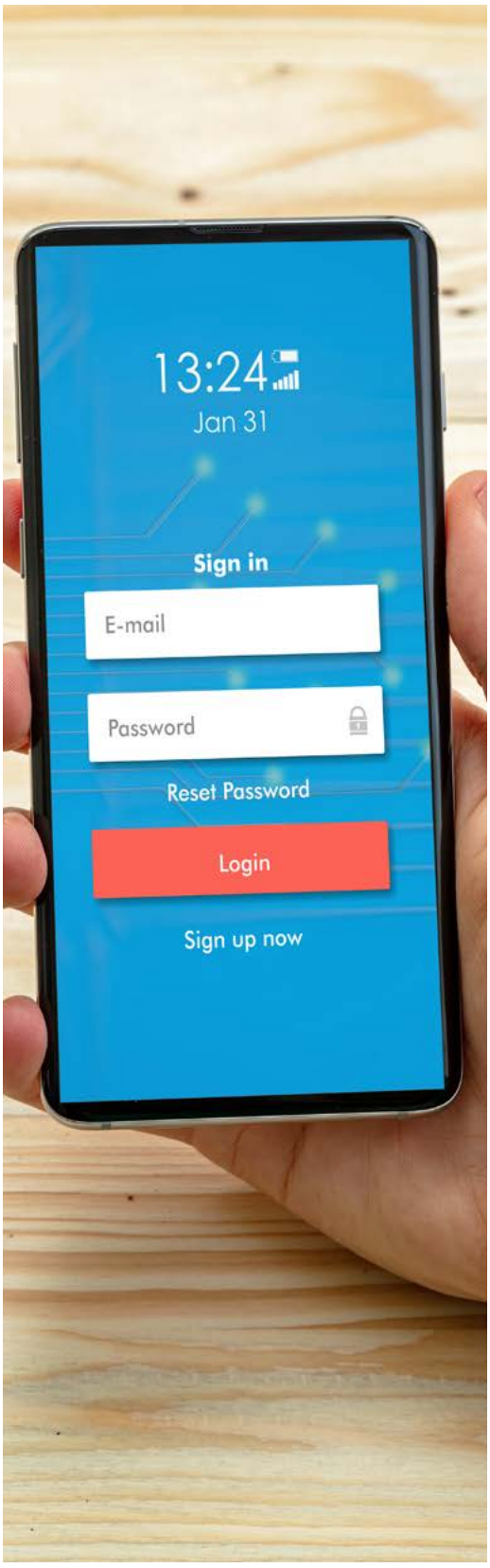
It is important to ensure that devices and operating systems are also updated; often updates to operating systems carry with them fixes for vulnerabilities that can be exploited. For example, the WannaCry ransomware crypto-worm exploited the Eternal Blue vulnerability in Microsoft's Operating System. Microsoft had released a patch to fix the vulnerability one month prior to Eternal Blue being leaked by hackers, but many of the infected devices were running outdated OS versions.

ENCRYPT HARD DRIVES

Although this consideration is often overlooked, devices carrying sensitive information outside of the corporate network should have encrypted disks. Workstations remaining unattended in the office should also have their disks encrypted, in addition to the security measures outlined above.

AVOID PUBLIC WIFI

As the lockdown measures continue to be lifted, including the opening back up of public spaces such as cafes, bars and restaurants, employees may wish to work from shared or public work spaces rather than their kitchen tables. Using a public WiFi network on a corporate device without a VPN in place and active should be discouraged. As an alternative, employees may wish to tether a mobile device with a 4 or 5G connection. Whilst this is far more secure than using public WiFi, the cost of data roaming charges to the business will need to be considered.



Make Use of Time/Cost-Saving Tools: Senseon's Approach and Solution/ Response to COVID19

Irrespective of whether organisations are accustomed to remote working, or have had to rapidly adapt to these new working conditions, it is clear that the current COVID-19 pandemic is presenting unique challenges. With early indicators pointing to this way of working becoming the 'new' normal, even after the lockdown restrictions are lifted, it is likely that organisations will need to continue to invest in technology that will enable this new way of working. Alongside this investment in technology, it will be the role of IT and security teams to secure it. In addition, the knock-on effects to the economy have financial analysts predicting the worst economic downturn since the Great Depression. Moving forward, it will be more important than ever that security teams are able to justify the value they are receiving from their existing security stack, as budgets will inevitably come under increasing scrutiny as organisations look to tighten the belt somewhere. Where there is duplication and cross-over created by multiple solutions offering similar capabilities, teams may look to consolidate their existing security stack.

Within this section, we will explore Senseon's cyber defence platform, including how our reimagined approach to cyber security infrastructures is helping security teams exponentially increase their operational efficiency and securing remote users and devices no matter where they are.

Senseon was designed from the ground up with a mission to take on the biggest industry challenges and to make you the best at what you do. We created Senseon for those who demand more from their security tools. Effortless to use and relentless on your behalf, Senseon learns and adapts to every event within your environment in order to automatically expose and investigate threats at a speed and scale no human team could ever match.

Make Use of Time/Cost-Saving Tools: Senseon's Approach and Solution/ Response to COVID19 *(cont.)*

SENSEON HAS THREE CORE DIFFERENTIATORS:

Breaking down the silos of cyber defence

Historically, cyber security vendors have taken a domain first approach to cyber security, for example some vendors may develop solutions with network detection and response capabilities for monitoring network traffic; and on the other side of the fence, other solution providers may develop tools with endpoint detection and response capabilities. Taking a retrospective perspective of the evolution of the security industry, a clear pattern emerges whereby new tools are developed in response to the discovery of new vulnerabilities, attack vectors and techniques. In the majority of cases, tools have been developed to combat a very specific type of threat and may therefore be considered 'point' solutions.

1

The overarching result is that security stacks have evolved to become bloated with point-heavy and operationally inefficient, with the necessary information existing in multiple silos. The burden is then passed on to the analyst to manually correlate across multiple solution sets in order to make this information actionable. With the Ponemon Institute estimating it takes an analyst anywhere between 9 and 50 minutes to follow this process, this very quickly becomes a problem that is not humanly scalable.

In contrast, Senseon takes a unified data approach to cyber security, gathering data from the richest sources of intelligence across your entire estate, including network data, endpoint processes and public/private cloud traffic. This not only offers IT and security teams unparalleled visibility across their entire digital estate, it also means that a single analytic or manual threat hunting query can be used to query data cross a high-speed columnar database containing data collected from across all your on-premise architecture, public and private cloud and user devices, irrespective of whether they are on or off the network/VPN.

Executing blended methods of detection

2

Different tools deploy different detection methodologies in order to identify suspicious and malicious activity. For example, anomaly detection at the network layer within Network Detection and Response platforms, or the use of rules and signatures within Anti-Virus tools. Each detection has its distinct strengths and weaknesses, and none is suitable for every detection task. Taking a purely rules and signatures approach to threat detection, for example, is a highly effective method of detecting attack vectors which require the attacker to exhibit very specific behaviours around which analytics can be written to detect these behaviours; however this approach falls short when it comes to detecting previously unseen or unknown attacks.

Senseon does not subscribe to the idea that there is a single detection methodology that works for every type of attack, compromise and insider threat. Within our platform we deploy multiple different detection methodologies against specific detection use cases, including rules, signatures, user and entity behaviour analytics (UEBA), supervised and unsupervised Machine Learning and more novel methods such as deception for detection through the use of honey tokens and honey files. This creates significant new value for IT and security teams by ensuring the right detection approach is applied against the correct detection use case.

AI Triangulation

When founding Senseon, our overarching ambition was to make security teams more operationally efficient, give them their time back and allow them to take a more proactive approach to securing the business. Fundamental to this ambition is what we have called AI Triangulation.

3

AI Triangulation is the ability for the platform to be able to automatically investigate the output of events captured through multiple detection methods. It is a virtual workforce for our customers, conducting advanced and nuanced investigations tens of thousands of times a day on their behalf. With the ability to pivot between different sources, including from the Internet, AI Triangulation automatically enriches investigations to produce the most deterministic reasoning of what is occurring within an environment.

By automatically investigating observations, Senseon is able to intelligently triage alerts before raising them to human analysts for further investigation and action, leading to a significant reduction in both the overall number of alerts teams receive, as well as the number of false positives. By reducing teams' workloads by up to 99.4%, security functions achieve much greater levels of operational efficiency and significantly reduce their mean time to detect and respond to cyber threats.

At a time when organisations' attack landscapes are increasing exponentially, visibility is key. Senseon's unique ability to gather data from the richest sources across your estate, and irrespective of how rapidly that estate is changing and evolving, provides IT and security teams with the real-time visibility they need, through a single pane of glass. Combining both the detection methodologies and capabilities of multiple solution sets into a single platform, Senseon offers teams the ability to significantly increase the value they receive from their security stack; a crucial factor when considering that expenditure is likely to be scrutinised more than ever due to the knock-on effects to the economy created by the pandemic.

Make Use of Time/Cost-Saving Tools: Senseon's Approach and Solution/ Response to COVID19 *(cont.)*

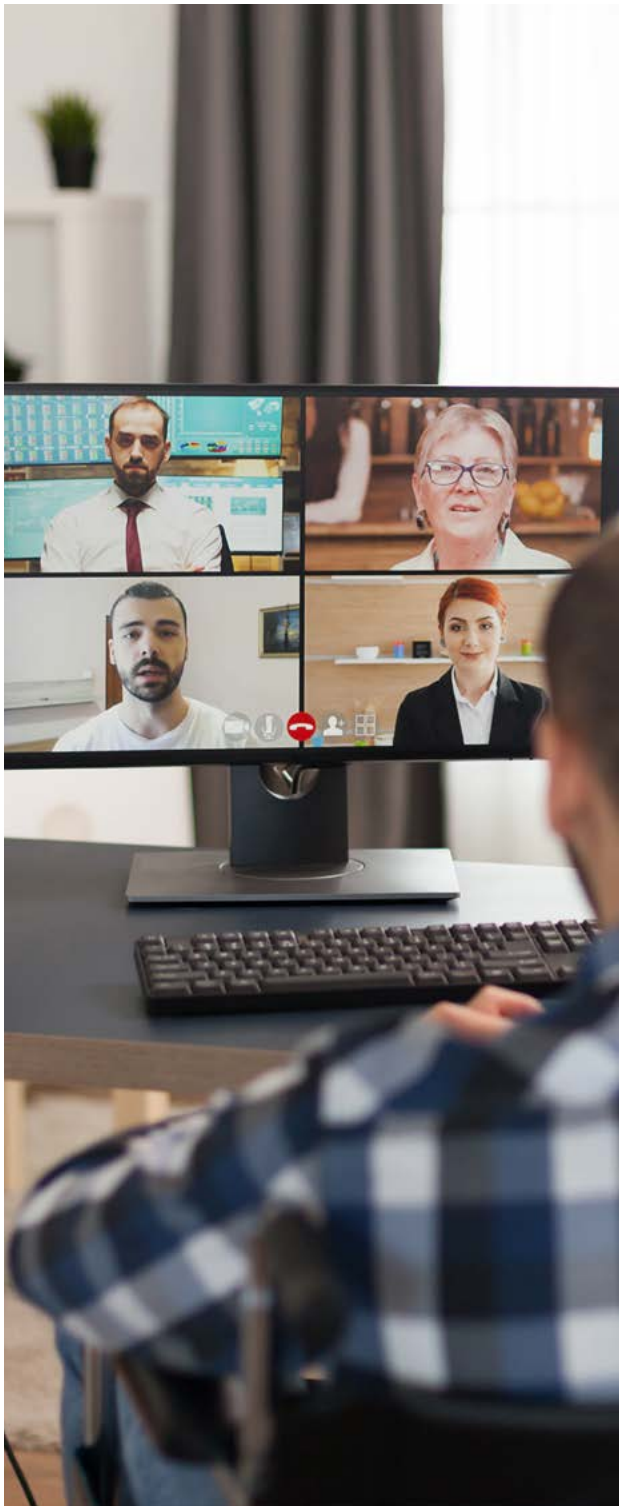
HOW SENSEON PROTECTS REMOTE WORKERS

As we have discussed previously, early indicators are suggesting that social distancing and some form of remote working are here to stay for the foreseeable future. It is highly unlikely that staff will be travelling into offices any time soon and, looking to the future, the general consensus is that the days of offices filled with thousands of employees will be consigned to the history books.

Whether or not there is an ongoing global pandemic, it is paramount that IT and Security teams have visibility of remote devices, and the capability to protect them.

Endpoint 360 is a feature of the Senseon platform which enables the endpoint agent to intelligently change how it calls home, depending on whether it is on the corporate network or the VPN. This means that, regardless of whether employees make use of the VPN when working remotely, IT and security teams still have real-time visibility and protection over remote users and devices wherever they are working from.

This is of course incredibly important during the current pandemic but Endpoint 360 use cases extend well beyond global pandemics. The Endpoint 360 agent can be deployed to meet a wide variety of use cases, from having a field sales team who spend the majority of their time working from and travelling between customer sites to VIPs like the CEO and FD who require additional protection for the rare occasion they leave the office. Senseon's Endpoint 360 enhances teams' ability to protect the organisation 24/7 no matter how much the attack surface increases. Regardless of whether the team has eyes on the box, Senseon is effortless to use and relentless on your behalf - always watching and always protecting.



Summing Up Your Safety Solutions

For some organizations, remote working was already second nature; for others, the Coronavirus pandemic forced them to rapidly deploy technology to enable teams to work from home, in many cases, having to sacrifice thorough implementation testing and security vulnerability assessments in favour of speed and convenience.

With early indications suggesting that some form of social distancing will be in place until at least the end of the year, for employees who cannot walk, cycle or drive to work, it may be the case that they need to continue to work remotely in order to avoid public transport. Organisations will therefore need to maintain and secure the infrastructure that enables remote working. Based on a recent Gartner report, it is likely that many employers will give employees the option to continue to work from home permanently, even when this is 'over.' Even amidst a global pandemic, employees have reported greater productivity and higher job satisfaction, translating to increased profitability for employers even in an economic downturn.

As well as increased profits, the business also benefits from a reduction in overhead expenditures, such as saving on the rent for office spaces large enough to accommodate teams which are now no longer required. Employees benefit from reduced commute times, increased family time and a better work-life balance.

It is likely that remote working is here to stay in some form; while the general consensus is that we will see an end to massive office spaces with thousands of employees, it may be that organisations develop some form of hybrid model as restrictions are eased and we continue to adapt to the new normal. It is inevitable that Covid-related attacks will subside and, as they always have, attackers will continue to innovate and find new attack vectors and vulnerabilities to exploit. Irrespective of whether teams find themselves operating under the highly challenging circumstances of a global pandemic, within this white paper, we have identified consistent and constant attack techniques and methodologies that organisations are more susceptible to when their employees are working remotely.

Most prominently, the attack surface that attackers have to take advantage of is significantly increased with employees working remotely. As restrictions are lifted and people begin to travel and move around more freely not only will the attack surface increase but as employees work from shared spaces on public WiFi networks the number of opportunities for attackers will increase exponentially as well.

It is imperative that IT and security teams are aware of the risks that remote working, pandemic or not, presents. As we have discussed within this paper, the Mitre ATT&CK framework can be an extremely useful tool to understand attackers' likely techniques and map your capabilities to these to analyse where your biggest vulnerabilities may lie. As we continue to adapt to this new 'normal', organisations must invest in technologies and capabilities that will enable teams to secure this way of working, including ensuring that they have visibility of users and devices, regardless of where they are operating. After all, the home is the new enterprise.

Frictionless Software Signup

"Clearly setting themselves apart from this noisy landscape, Senseon is the only solution with a vision far beyond what I have seen from the rest of the market and with the team to enable them to pull it off...At such a genuinely devastating time for so many reasons, it means so much to be working with a company that genuinely wanted to do all they could to help their customers get through this."

Karl McArthy
CISO, Oodle Car Finance

Arrange a **1:1 personalised demo** here:
https://www.senseon.io/demo-options

Take Senseon for a **test drive** here:
https://www.senseon.io/test-drive

Take a **virtual tour** with Senseon's Founder and CEO here:
https://www.senseon.io/demo-options