REMOTE WORK SECURITY

CONSIDERING REMOTE WORK IN THE WAKE OF CORONAVIRUS?
PRIVACY AND CYBERSECURITY ESSENTIALS

On-Device Protection

BlackFog does NOT send data to the cloud for analysis

Blocks Outbound Data Flow

BlackFog STOPS the activation of threats and data theft

Fileless Network Protection

BlackFog stops threats using behavioral analysis

50% of CIOs expect a rise in employees working remotely

$4.5 TRILLION could be saved by 2030 in the US alone from remote working

The average company would save
$11K per year for each employee allowed to work at home for half the time

Desks are vacant
50-60% of the time in across Fortune 1000 companies globally

54 MILLION tons of greenhouse gas could be reduced each year employees worked at home half the time

159% In countries like the U.S., there has been an increase in people who are working remotely from 2005 to 2017

CONTENTS

Remote Work Economics

With the onset of Coronavirus, the issue of remote working has been pushed to the forefront for organizations globally.

No longer a question of if employees should be able to work from home in flexible conditions, but rather quickly becoming a mandatory practice. Fortune 1000 companies around the globe are entirely revamping their office spaces to accommodate the fact that employees are already mobile, with studies repeatedly showing that desks are vacant 50-60% of the time. Twitter has also just announced that it is now mandatory for all of its 4900 global employees to stay home, while the story at Google is similar as they advise all employees in North America, Europe, the Middle East and Africa to work from home due to the virus.

The economics of remote work make it clear that it is not just a great choice for health reasons but also for the bottom line. Studies show that businesses would save an average of $11,000 per half-time telecommuter per year if employees were permitted to work from home.

When Boris Johnson unveiled his government's plan to tackle the virus in the UK, homeworking for millions of people was a key part of his battle plan to help mitigate the risk of spreading. The overall impact of the virus is still unknown, but what's clear, is that there is no easy fix and it is something serious that will affect us globally for months to come.

For many organizations, particularly those in the tech space, working from home is the norm and those companies have little to fear from the disruption of remote operations. However, for organizations who do not have programs and systems in place for their staff, they will find they have other significant issues to deal with. Namely, cybersecurity and protecting their devices and networks outside of their corporate environment.

A dispersed workforce has always posed significant risks and challenges for those responsible for IT security within their organization. Cyberattacks are now at an all-time high and have been growing exponentially over the last several years, and this year experts are predicting a 50% increase in the rise of attacks on mobile devices.

Risks of Remote Work

WiFi Security

81% of users connect to free unsecured WiFi (oneworldidentity)

Hacking

57% of mobile workers have been hacked within the last year (helpnetsecurity)

Public Spaces

70% of incidents occur using unsecured WiFi in public spaces (CyberOregon)

BYOD

94% of Enterprises say BYOD has increased security risks (helpnetsecurity)

VPN Use

Only 46% are confident that mobile workers use a VPN (iPass)

Privacy & Security Challenges

With a dramatic increase in remote workers, organizations need to be prepared for an entirely new set of problems and challenges.

The sheer breadth of infrastructure, locations and skillsets puts new burdens on an already resource strapped IT department.

Organizations need to look at the problem in new ways to protect the endpoints of remote workers. Since these employees can be anywhere we cannot assume anything about the infrastructure and we therefore must focus on ZERO trust. Users can now be working in coffee shops, airports, homes and other public spaces. In fact, recent statistics suggest that 62% of Wi-Fi related security events happen in café's and coffee shops.

Organizations need to adequately monitor data exfiltration, threats, and data flow wherever the user may be based, no matter what device they are using.

The VPN Fallacy

Existing techniques are no longer adequate to protect devices from a new breed of malware and ransomware. Traditionally, companies have employed VPN's to connect to corporate networks, or third-party VPN's to provide some level of anonymity. Unfortunately, there are several problems associated with this technique. Firstly, it assumes that users actually turn on the VPN on their device, which is often not the case. Recent reports suggest that only 46% of users actually turn it on when using the device.

Additionally, VPN's don't actually prevent an attack on a device, and they are still prone to the same vulnerabilities as a normal device. They can still download malware, become infected by ransomware and are therefore still subject to data breaches. From a security perspective, VPN's have become a new attack vector for cybercriminals. Reports have suggested that hackers have been targeting VPN's from major vendors to infiltrate and plant backdoors into corporations all over the world.

From a privacy perspective, VPN data breaches are not uncommon, as evidenced by hacks at NordVPN and TorGuard. These attacks allow hackers to access user activity and extract data. It is therefore not surprising that they have become new targets, providing a central repository of network traffic by individuals.

VPN's are specifically designed to provide secure access to a corporate network, allowing access to internal documents and other corporate services. However, in recent years, VPN's have been used to bypass regional controls on content for services such as Netflix, music services and government censorship. More recent concerns about privacy have increased their popularity with promises of online anonymity. However, users should be mindful that there is no such guarantee and that they are subject to government regulation and recording. Several reports have demonstrated that many VPN's and ad blockers are secretly collecting user data. In addition, within some regions of the world such as China, United Arab Emirates, and Turkey, VPN's are illegal.

Data Exfiltration

Perhaps the biggest concern facing remote workers is the level of data exfiltration (data loss or data leakage) happening on their devices.

The always on nature of mobile devices means that data is constantly leaking. Personal and corporate data is being mined even while we sleep. This includes exact location information, name and address and even usage patterns and available applications. This has massive implications for corporations entrusted with customer data as well as corporate trade secrets and other valuable information.

Exfiltration is very difficult to detect because it happens silently in the background with the victim not even realizing it has occurred, leaving organizations and individuals highly vulnerable. With cyberattacks growing in both volume and sophistication, it is inevitable that malware will find its way onto a device. Such malware often remains latent to avoid detection and only activates when the machine has been idle for a certain period of time. People are often surprised how much data their mobile device consumes overnight when they haven't even been using it. This is commonly data being exfiltrated from the device.

Data exfiltration can be divided into two categories, outsiders trying to infiltrate the network to steal valuable corporate data, and people on the inside willing to share it. Whilst often malicious in nature data exfiltration can also be the result of insider carelessness, sending confidential documents to personal email accounts and / or cloud servers.

In an outsider threat scenario, a cybercriminal will insert malware onto a network-based device, such as a computer or mobile phone. The malware will crawl other network devices in search of valuable information and attempt to exfiltrate it. Once compromised the malware orchestrating the attack may lay dormant until the point of data exfiltration, or, to avoid detection, subversively collect information over time and gradually exfiltrate the data.

Exfiltration Techniques

Data exfiltration can be achieved using various techniques, but it's most commonly performed by cybercriminals over the internet or a network. These attacks are typically targeted, with the primary intent being to gain access to a network or machine to locate and copy specific data.

Common techniques involve anonymizing connections to third party servers to protect the identity of the attacker. This can include using the Dark Web, direct IP addresses, tunneling over HTTP or HTTPS and Fileless attacks, where attackers can use remote code execution. According to BlackFog's 2019 internal research, around 15.85% of all traffic is being exfiltrated to Russia and 2.62% is going to China. Data exfiltration to the Dark Web represents around 3.12% of all traffic.

How BlackFog can Help?

Intrusion detection systems such as Firewalls and Anti-Virus solutions that remove known infections are not enough to prevent attackers from infiltrating the network.

The inherent mobility of today's workforce and the number of new remote workers emerging in the wake of Coronavirus is making it increasingly difficult for companies to keep track of what's happening on every device in the network. With a significant proportion of network transactions taking place in the background without consent, it is important that organizations are closely monitoring this activity. Preventing the transmission of sensitive data to unidentified servers in regions where high levels of cyberattacks originate is paramount to protecting all network infrastructure. Modern attacks are predicated on the ability to communicate with third party servers to steal data. It is crucial that any cybersecurity solution is able to monitor, detect and prevent the unauthorized transmission of such data in real time.

To protect your remote workforce its critical to stay ahead of cybercriminals and this can only be done by protecting your organization from data exfiltration with a multi-layered defense system preventing data loss, unauthorized data profiling and data collection. Only by monitoring the flow of outbound traffic and stopping attacks in real-time can you ensure no unauthorized data will fall into the wrong hands, whether your employees are on or off the network.

97% of CIO's say their workforce will be widely dispersed across geographies and time zones soon

62% of U.S. CIOs believed most Wi-Fi-related security incidents occurred at cafes and coffee shops

In 2019 50% of employees globally work away from their office at least 2.5 days per week

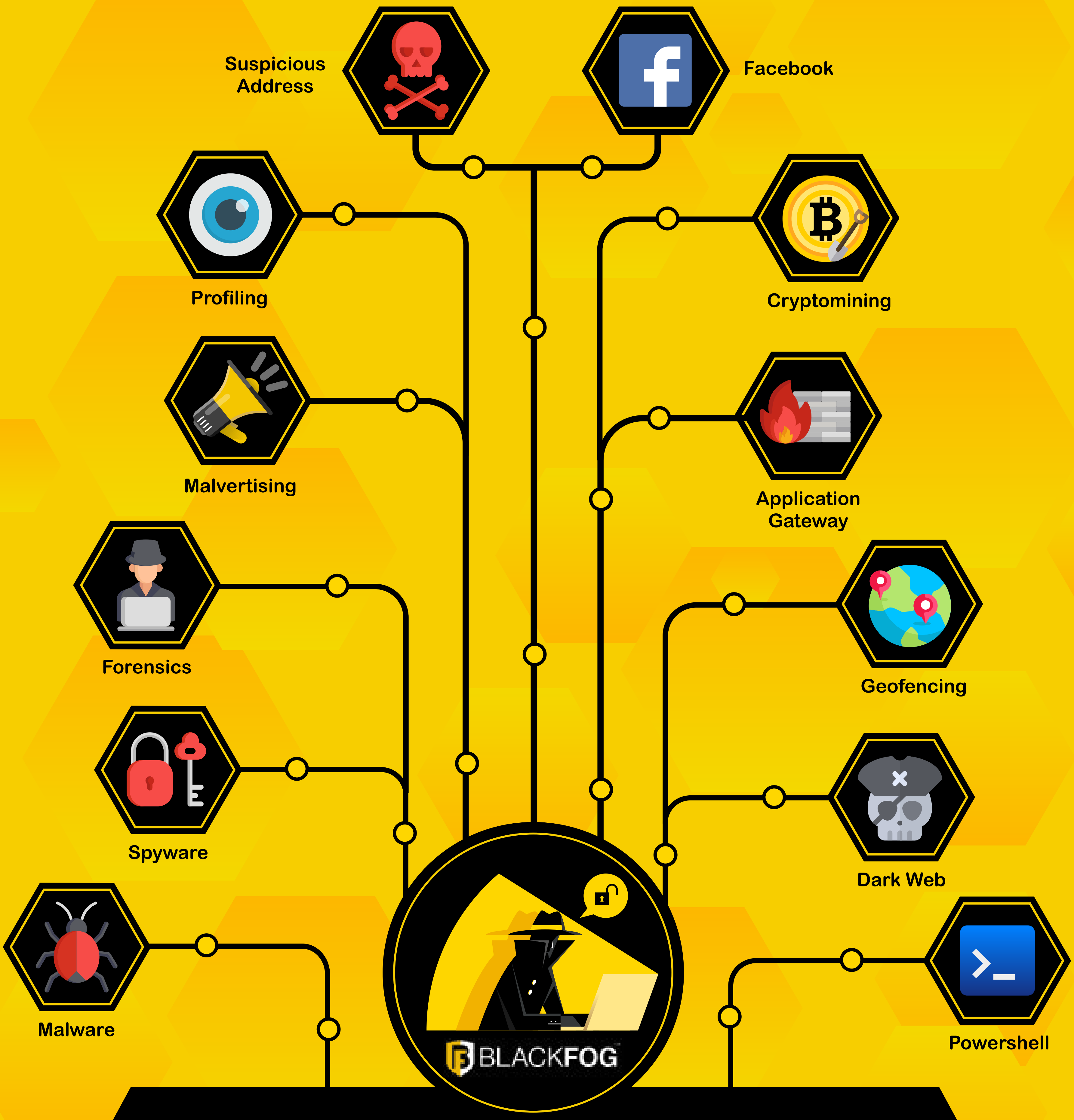
61% of global companies currently allow their staff to have some sort of remote working policy

57% of U.S. CIOs suspected their mobile workers had been hacked in the last 12 months

95% of UK businesses struggle with remote working with one third saying they experienced a data loss or breach as a result

A 2018 study of 1,000 UK and German remote workers found that 25% admitted breaking security policies to work remotely and more than 40% said they didn't have the right tools to work remotely

BlackFog's 12 Layers of Defense



Hackers will get into your network. BlackFog stops them getting out. With 12 layers of defense we shut hackers down before they can remove your data.