PRIVACY

HOW BLACKFOG CAN PROTECT YOUR BUSINESS

On-Device Protection

BlackFog does NOT send data to the cloud for analysis

Blocks Outbound Data flow

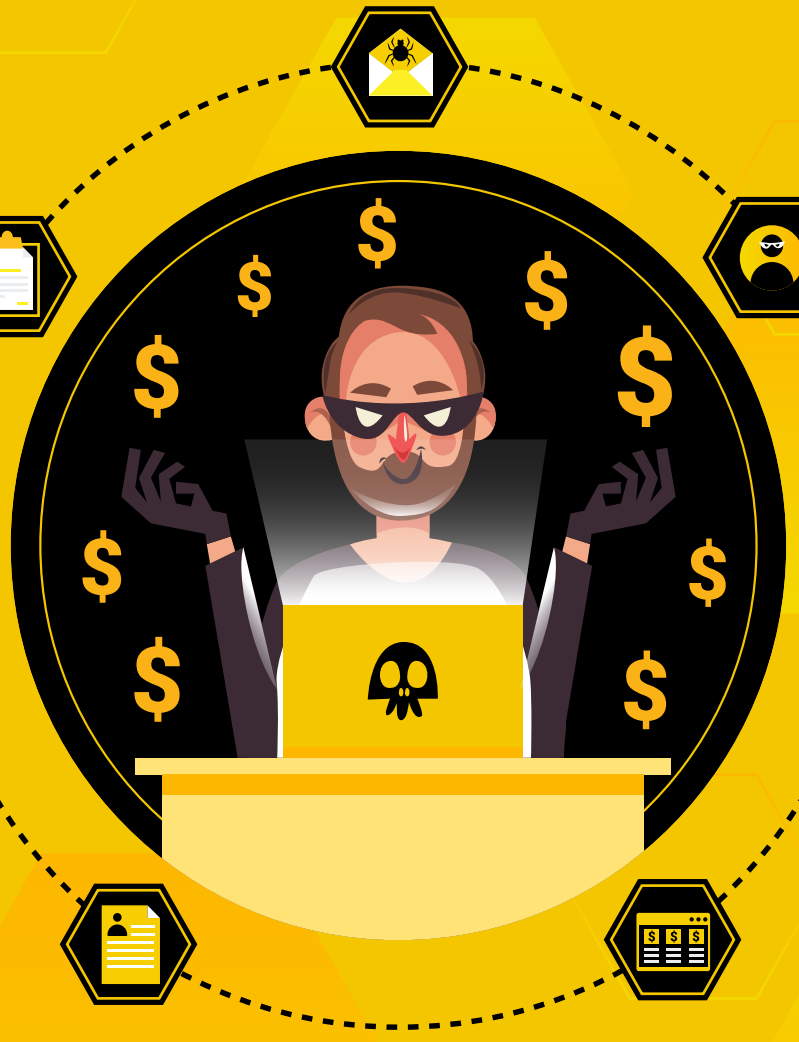
BlackFog STOPS the activation of threats and data theft

Fileless Network Protection

BlackFog stops threats using behavioral analysis

7,860,402,548

email addresses logged in 'have I been pwned?'



Patient medical records sell for **$1K** on the Dark Web

60M Americans affected by identity theft in 2018

Average cost of a data breach **$3.86M**

773M records exposed in Collection #1 data breach

Average cost per lost or stolen record **$148**

841M records from 16 websites listed for sale on the Dark Web

CONTENTS

3

What is Privacy?

Why is Privacy important?

How is Privacy being compromised?

4

What is BlackFog?

Why was BlackFog created?

What does BlackFog do to protect Privacy?

What makes BlackFog unique?

5

Why BlackFog?

BlackFog Key Messages

Why a preventative approach is required?

Key Questions to Address

6

12 Layers of Defense

What is Privacy?

Once described as “the right to be let alone,” privacy is now best described as the ability to control data we cannot stop generating, giving rise to inferences we can’t predict.

With an estimated 2.5 Quintillion bytes of data generated each day, the ongoing challenge is how to control the data we can’t stop generating and protect it from ever increasing malicious threats.

2018 was the year of privacy with major data scandals such as Facebook’s exposure of tens of millions of user accounts to Cambridge Analytica and the introduction of GDPR – the world’s most stringent privacy law. With other global privacy laws such as POPI in the process of implementation, privacy is firmly on the agenda for individuals and organizations alike.

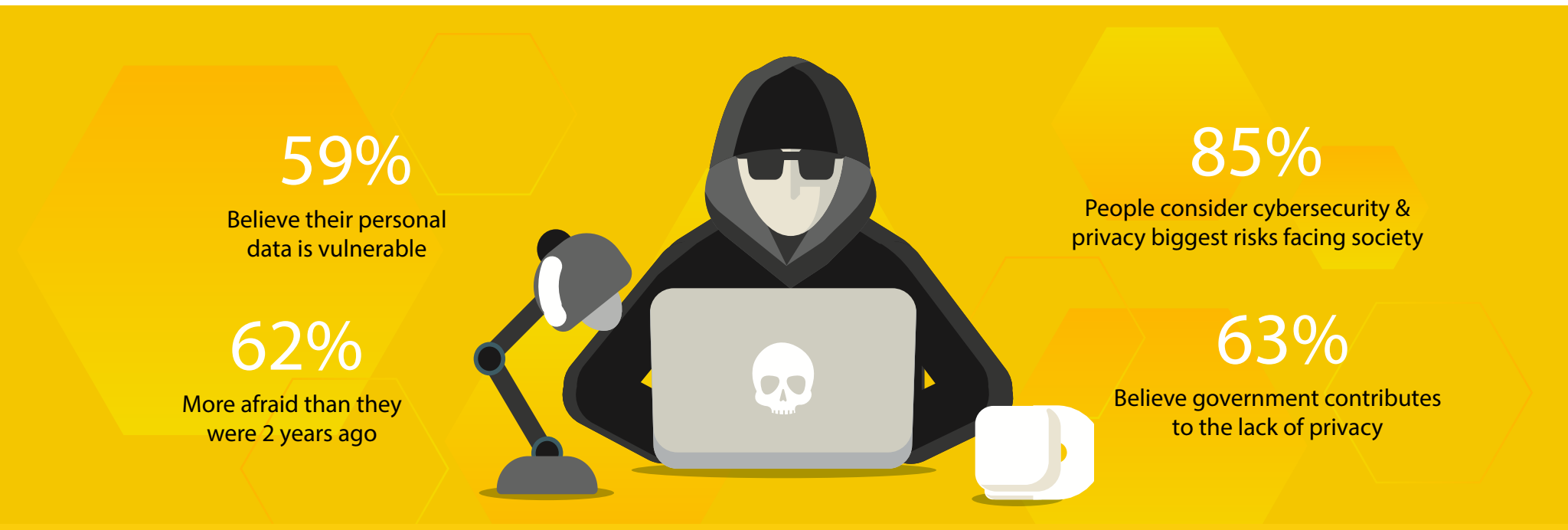
Why is Privacy Important?

In the wake of increasing privacy concerns and the arrival of new regulations, protecting privacy has never been more critical to ensuring business survival. While losing customer data can damage a brand’s reputation, trust, and revenue, preventing valuable corporate information from leaving the confines of the business and falling into the wrong hands is critical.

How is Privacy Being Compromised?

Company data is being stolen – often unknowingly. Every day the devices your organization uses runs tens of thousands of transactions as employees browse the internet or use applications. A high proportion of device transactions take place in the background, without the user’s knowledge – often resulting in sensitive company data unknowingly being sent to unidentified servers in regions where high levels of cyber-attacks originate.

Organizations don’t know what they can’t see so most are unaware that unauthorized data is leaving their environment and that their privacy is being compromised.



What is BlackFog?

BlackFog is an on-device data privacy and cyber security solution that detects and blocks the transfer of outbound data in real-time, preventing cyberattacks before they happen.

Why was BlackFog created?

BlackFog was founded in 2015 by Dr Darren Williams, a veteran of 3 successful start-ups. While working at an acquiring company, focused on recovering stolen laptops, it became apparent that hardware was becoming commoditized to a point where the value was no longer in the device itself, but the data on the device. Organizations had shifted from device centric to data centric in a short period of time. You can replace device very quickly and easily, but you cannot from data theft and ultimately a data breach. As governments started designing new laws around privacy and data loss, such as GDPR it was a clear there were no adequate solutions in the market focusing on this problem.

Existing security solutions focus on preventing attacks via known vulnerabilities, such as Firewalls and Anti-Virus software. Realizing that attacks can easily thwart these standard security regimes gave BlackFog the impetus to develop BlackFog Privacy to protect devices from data theft and cyberattack using behavioural profiling to prevent the attacks happening in the first place.

What Does BlackFog do to Protect Privacy?

In simple terms BlackFog blocks the exfiltration of data. BlackFog ensures that what is on your device stays on your device. BlackFog acts as a guardian of your data, constantly watching the outbound traffic flow and preventing any unauthorized data from ever getting out. BlackFog protects an organizations data and privacy enabling them to be compliant with data regulations such as GDPR and POPI.

What makes BlackFog Unique?

Lots of cybersecurity firms can tell you when a breach or attack has taken place and your data has been compromised. BlackFog stops it from happening in the first place. It's inevitable that cybercriminals will find their way in; BlackFog prevents them from taking anything out by focussing on data loss, data profiling and data collection. BlackFog is the ONLY firm that tackles this problem at all three levels, ensuring maximum privacy protection.

Why BlackFog?

The risk is real – it's no longer a question of if, but when a cyberattack will occur and your data will be compromised. It's inevitable that hackers will find a way into the network, BlackFog will stop them from getting out.

Through a layered approach to security BlackFog spots, in real-time, when an attacker is attempting to remove unauthorized data from your device or network and stops them in their tracks. BlackFog is the only company able to block outbound data-flow while keeping all data on the device. BlackFog defends against ransomware, spyware, malware, phishing, unauthorized data collection and profiling.

BlackFog Key Messages

- Privacy is all about owning and controlling YOUR data and BlackFog ensures what is on your device stays on your device
- BlackFog provides On-Device Protection – no data is sent to the cloud
- BlackFog Prevents the flow of data to the Dark Web
- BlackFog STOPS the activation of threats and data theft
- BlackFog blocks more than 99% of web advertising, a major distribution channel for malware
- BlackFog is the ONLY firm that offer on-device protection from data exfiltration
- BlackFog provides 12 layers of defense against ransomware, spyware, malware, phishing, unauthorized data collection and profiling

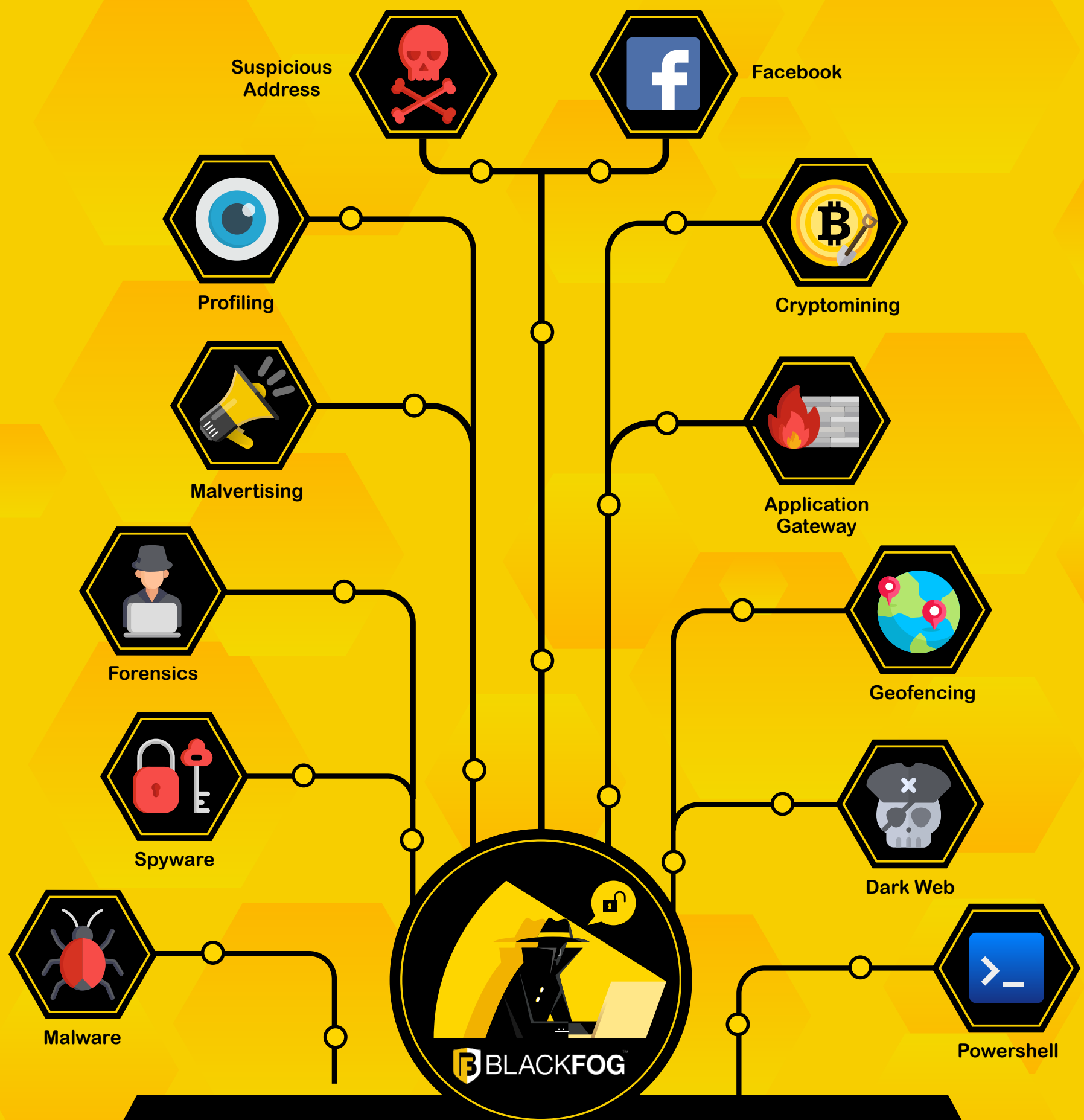
Why a Preventative Approach is Required?

Having a plan to deal with the inevitability of a data breach is critical but it's no longer enough. Organizations must take a proactive approach to protecting data security and privacy. Hackers will get into a network so organizations must implement cybersecurity tools that can identify threats in real time, shut them down and stop them in their tracks before they can remove any data or cause any harm. To remain compliant with data legislation a layered approach providing protection from ransomware, spyware, malware, phishing, unauthorized data collection and profiling is required.

Key Questions to Address

- Do you know where all of your all data is flowing from a security and compliance perspective?
- Do you know where your weakest links are?
- Is your organization compliant with data regulations?
- Do you know what the data breach fines are in your region?
- Are you confidant that your employees could identify a phishing email?

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.