BLACKFOG™

Privacy. Security. Prevention.

Go-to-Market Messaging Document

June 2020

About BlackFog

Founded in 2015, BlackFog was born to combat the growing number of online threats targeting your personal and corporate data. Hackers will get into your network; BlackFog stops them getting out. Through a layered approach to security, BlackFog spots, in real-time, when an attacker is trying to remove unauthorized data from your device / network and stops them in their tracks. Consisting of multiple layers of defense against ransomware, spyware, malware, phishing, unauthorized data collection and profiling, BlackFog blocks over 24 million threats across mobile and desktop endpoints around the world, protecting organizations' data and privacy, and strengthening their regulatory compliance.

What Does BlackFog Do?

BlackFog provides on device threat prevention for individuals and organizations. Our behavioral analysis and data exfiltration technology stops hackers before they even get started. Through a layered approach to security, we spot, in real-time, when an attacker is trying to remove unauthorized data from a device and network and shut them down before they get the chance to. We provide threat prevention for data breaches, insider threats, ransomware, spyware, malware, phishing, unauthorized data collection and profiling.

What's Unique About BlackFog

BlackFog is the only on device data privacy solution. Rather than focusing on perimeter defense, our unique preventative approach focuses on blocking the exfiltration of data from your devices. Perimeter defense techniques and anti-virus software are powerless against the types of attacks we see today. BlackFog approaches the problem differently by targeting threat vectors where it hurts most, when they try to replicate, activate, communicate or exfiltrate data. By neutralizing the attack at multiple points of its lifecycle it cannot move laterally within the organization or do any damage. Multiple layers of defense prevent threats and dramatically reduce the risk of a data breach.

Key Benefits

On Device Data Privacy

BlackFog's on device data privacy technology prevents data loss and data breaches by blocking the unauthorized collection and transmission of user data from every device on and off the network.

On Device Data Security

BlackFog prevents cyberattacks across all endpoints and monitors the exfiltration of data from any network to ensure compliance with global privacy and data protection regulations.

Insider Threat Prevention

BlackFog protects intellectual property and the risks associated with industrial espionage by preventing malicious activity from inside organizations.

Why is Privacy so Important?

Complex regulatory environments around the globe have led to considerable new legislation, government watchdogs, compliance departments and hefty fines. Protecting privacy and mitigating the risks of data loss and data breaches has never been more critical to ensuring business survival. To avoid loss of intellectual property, reputational damage, trust and revenue, businesses must ensure they prevent valuable information from falling into the wrong hands.

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 cyberattacks 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 Does BlackFog do to Protect Privacy?

BlackFog blocks the exfiltration of data. BlackFog ensures that what is on the device stays on the device. BlackFog monitors outbound traffic flow to prevent 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's Special About BlackFog?

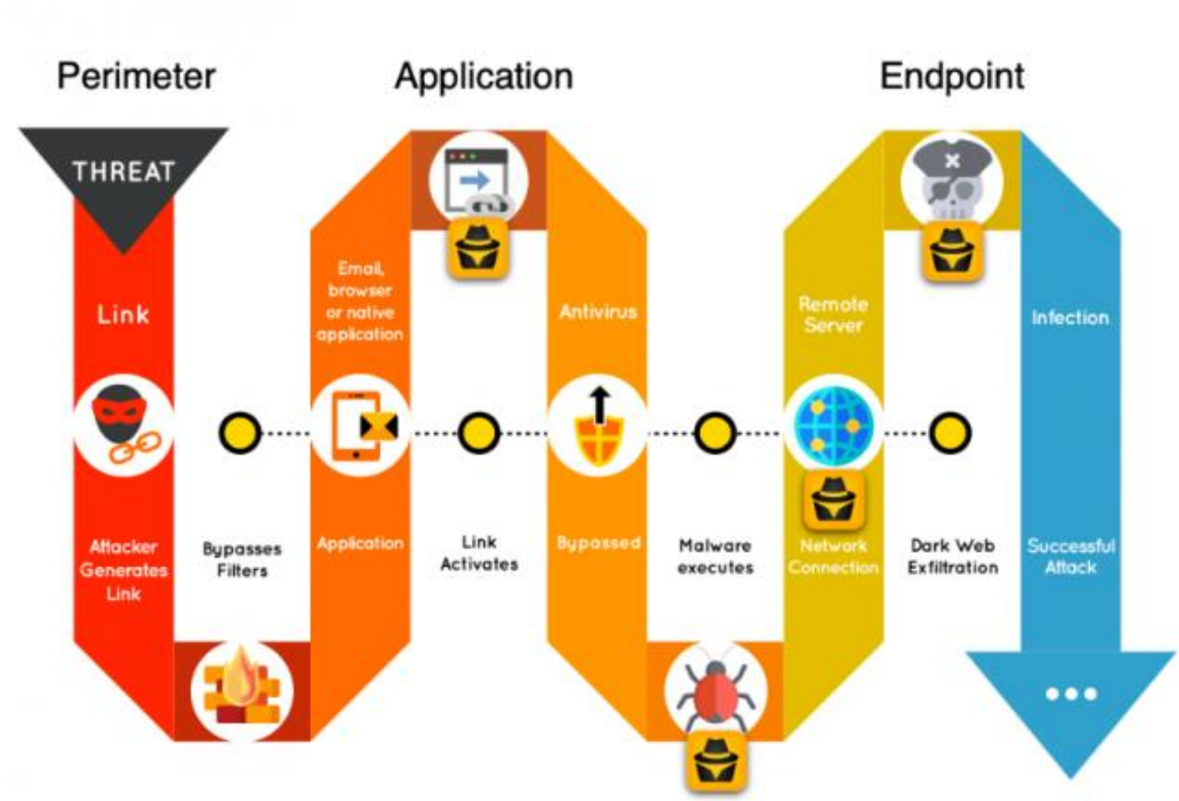
Lots of cybersecurity firms can tell you when a breach or attack has taken place and your data has been compromised. BlackFog stops it from happening in the first place. It's inevitable that cybercriminals will find their way in; BlackFog prevents them from taking anything out by focussing on data loss,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

How Does BlackFog's Technology Work?

As we think about how viruses infect a device and spread laterally within an organization, we can see a number of traits. Firstly, the point of a cyberattack is to steal information, be it financial, personal or intellectual property. If the attacker cannot communicate with command and control (C2) servers or transmit any data, then there is little value in the attack.

BlackFog's technology focuses specifically on data exfiltration to neutralize the attack. By preventing malware from communicating and isolating the code, it is possible to stop the loss of information and the lateral spread to other devices within the network.

There are many points within the lifecycle of a typical cyberattack where you can target data exfiltration. The illustration provides an example of how BlackFog targets malware using layer 3 packet monitoring.



BlackFog’s Multiple Layers of Defense

Dark Web

As the primary channel for activating ransomware and stealing your data, BlackFog blocks all traffic through the Dark Web.

Ransomware and Spyware

There are more than 4,000 file encryption attacks every day. BlackFog actively protects your device from these attacks.

PowerShell Defense

PowerShell attacks are a major entry point for attack vectors. BlackFog detects these attacks in real time and immediately terminates execution.

Malware & Phishing

With more than 26 million blocks, BlackFog virtually eliminates phishing attacks through email and the Web so you can use your device with confidence.

Execution Prevention

BlackFog automatically validates executables and system processes to prevent the execution of rogue applications.

Botnets

BlackFog prevents Botnets from stealing your data, sending spam or controlling your device.

Fake News

BlackFog includes the ability to block Fake News sites which is often used as clickbait to attract users and to extract personal information.

Cryptojacking

BlackFog protects your device from the exponential rise in cryptocurrency mining and CPU hijacking.

Ad Blocking

Online advertising is a major distribution channel for malware. BlackFog actively blocks 99% of all advertising and tracking.

Geofencing

A large majority of attacks originate from just a few countries. Our geofencing technology blocks data transmission (exfiltration) to specific countries to control the data flowing off your device and prevent attacks.

Forensics

BlackFog eliminates forensic data collection on your device to ensure your privacy is kept intact.

Suspicious Activity

BlackFog identifies and terminates malicious applications that attempt to hide network communication through anonymous addresses.

Profiling and Tracking

BlackFog prevents the unauthorized collection, aggregation, and sale of your data to the highest bidder.

Facebook

BlackFog can prevent data collection and profiling by Facebook, whether or not you are a Facebook user.

Key Messages

- ✓ BlackFog is the leader in data privacy and the **ONLY** on device privacy solution
- ✓ BlackFog does not send any data to the cloud
- ✓ BlackFog prevents cyberattacks across all endpoints
- ✓ BlackFog monitors the exfiltration of data in real time to ensure compliance with global privacy and data protection requirements
- ✓ BlackFog prevents data breaches by blocking the unauthorized collection and transmission of user data from every device in a network
- ✓ BlackFog blocks more than 99% of web advertising, a major distribution channel for malware
- ✓ BlackFog consists of multiple layers of defense against ransomware, spyware, malware, phishing, unauthorized data collection and profiling