DATA BREACH PREVENTION

A NEW PARADIGM

On Device Data Privacy

Prevent the unauthorized collection and transmission of user data on and off your network.

On Device Data Security

Ensure compliance with global privacy and data protection regulations.

Insider Threat Prevention

Protect your intellectual property and the risks associated with industrial espionage from inside your organization.

CONTENTS

Data Breaches

Despite increased global legislation around data protection and heightened consumer awareness around privacy and misuse of data, breaches were up a staggering 33% last year.

Hardly a week goes by without a major data breach hitting the headlines, with some of the largest global corporations being named and shamed. Repeat offender Marriott, whose 2018 breach was one of the largest in history, hit the headlines again in April 2020 with another breach affecting 5.2 million records. Other notable 2020 breaches include EasyJet who revealed that 9 million customers were affected by a cyberattack in May, while facial recognition software maker Clearview AI had their entire customer list stolen along with a database of around 3 billion photos.

There is no doubt that stories of data breaches and cyberattacks will continue to make headlines. Organizations are also increasingly negotiating with hackers to get their data back. In the first 5 months of this year alone, BlackFog tracked 76 publicized ransomware attacks and that number is rising fast.

Crime Does Pay

Cybercrime is a lucrative business and cybercriminals are always on the hunt for their next victim.

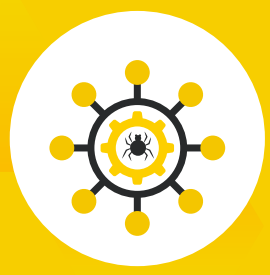
Cyberthreats are advancing so quickly it is perhaps not surprising that the average security team is struggling to manage an average of 57.1 different security tools in order to try and keep their organization out of the headlines.

Evidenced by the growth in the global cybersecurity market, (now a massive $173B), organizations know the importance of protecting their IT infrastructure from cyberattack. With dozens of security tools deployed across IT departments, why are so many organizations still being held to ransom and generating headlines for breaching data privacy regulations?

It is clear the cybercrime is rising, cybercriminals are getting smarter and ransomware pays, so the risks associated with cyberattacks will continue to escalate. What we need to address is why these attacks are still so successful, and is it possible for IT departments to stay ahead of cybercriminals and prevent data loss?

Privacy and Data Breach Facts

273
GDPR fines



97% of Companies
report benefits from their privacy investments

Average annual privacy spend
$1.2M

47% Increase
in insider threats

A New Paradigm

Defensive based approaches are no longer effective. The new paradigm is based on the assumption that hackers will get in and focuses on preventing the removal of data.

In the past, organizations have relied on traditional defensive approaches to protection such as perimeter-based firewalls and endpoint based anti-virus software. An approach that is simply not effective in preventing the types of cyberattacks we see today. Despite the best efforts of IT departments, around 80% of successful cyberattacks bypass existing cybersecurity systems. In fact, recent research from BlackFog has discovered that newer malware routinely disables existing security services before even mounting an attack.

This defensive based approach is no longer effective. The new paradigm is based on the assumption that hackers will get in and focuses on preventing the removal of data. If an attack cannot communicate bidirectionally with another server to activate, download payloads, exchange keys or exfiltrate data, then they are effectively disarmed.

Insider Threats

When we think of data breaches and cybercrime in general, we mostly think of hackers and faceless cybercriminals. However, a 2019 study from Verizon reported that more than a third of the 40,000 breach incidents they analyzed involved internal actors. Just as cybercriminals have ramped up their attacks on businesses amid coronavirus-related disruption, many companies have been forced to focus on the threats within their own organization.

Disgruntled employees are certainly nothing new, but as the Coronavirus crisis lingers and many corporations look to reduce their workforce, many employees are becoming increasingly nervous of their job security, and with that the likelihood of employees going to the dark side increases. Combine this with already stretched IT departments trying to manage new remote workforces, and it's unsurprising that insider threats are a significant cause for concern.

Malicious employees that steal intellectual property or commit intentional sabotage are among the costliest threats to organizations. Gartner's insider threat statistics suggest almost a third of criminal insiders commit theft for financial gain, and according to IBM, it takes on average 77 days to recover from an insider incident at an overall cost of around $11 million.

Risk Mitigation

A dispersed workforce has always posed significant risks and challenges for those responsible for IT security within their organization.

Many organizations are highly vulnerable to data theft as data exfiltration occurs silently in the background, with the victim not realizing it has occurred. In most cases cybercriminals are focused on valuable corporate information that can be sold or used to extort businesses for monetary gain.

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.

In an outsider threat scenario, a cybercriminal will insert malware onto a device. 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.

In the insider scenario, consider a disgruntled sales executive who is currently working through a notice period. He knows it's advantageous to his next role to steal sensitive company information. By using a proactive tool that focusses on behavioural analysis while controlling the exfiltration of data outside the network, his efforts to sabotage his employer would be easily blocked.

By monitoring the flow of outbound traffic in real time, organizations can prevent the loss of data from all endpoints and mitigate the risk of a data breach.

Managing a Remote Workforce

A dispersed workforce has always posed significant risks and challenges for those responsible for IT security within their organization. The challenge has never been greater than with the onset of Coronavirus. For many organizations, particularly those in the technology sector, working from home was already common practice and they have faced little to no disruption with the onset of remote operations. However, for those organizations who had no programs or systems in place there has been a significant increased risk of cyberattack.

To prevent cyberattacks and data breaches, organizations must focus on the remote worker endpoints. The ability to adequately monitor data exfiltration, threats, and data flow regardless of location or device is critical in the fight against data loss.

Prevention as a Form of Defense

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

Companies relying on VPN's should be aware of their limitations. Firstly, they assume that users actually turn on the VPN on their device, which is often not the case as recent reports suggest that only 46% of users actually do.

It's also important to note that VPN's don't actually prevent an attack on a device, and are still prone to the same vulnerabilities as a normal device. They can still download malware, become infected by ransomware and be subject to a data breach. From a security perspective, VPN's have become a new attack vector for cybercriminals, with several reports suggesting that hackers have been targeting VPN's from major vendors to infiltrate and plant backdoors into corporations all over the world.

More Products ≠ More Security

With the average IT department trying to manage over 57 different security tools it is not surprising that this often causes more problems than it solves. It suggests that many organizations feel that more products equate to more security, when in fact it only serves to increase complexity, management, overhead and most notably 'alert fatigue'. With so many systems working to secure multiple devices throughout an organization, IT professionals are forced to deal with an overwhelming number of security alerts. A 2019 research report found that 70% of security professionals investigate more than ten alerts every day, with 78% saying it takes more than 10 minutes to investigate each one. This becomes a major issue when organizations do not have the resources to adequality focus on the incident reporting, making such reactive approaches largely ineffective.

By taking a preventative approach to the problem, IT professionals can receive alerts that do more then tell you a problem has been identified but proactively take action to fix it. BlackFog Privacy for example, alerts IT departments that a threat was identified and blocked, enabling the IT professional to review detailed analytics of impact assessment across their entire organization.

Hackers Will Always Find a Way In

A hacker who is intent on infiltrating a device or network will eventually find a way in. The challenge is preventing an attack in the first place and ensuring attackers or insider threats cannot remove data from the device, eliminating data breaches all together.

Preventing cyberattacks and data breaches can be effectively managed using a multi-layered approach involving a combination of defensive and preventative techniques. Monitoring data exfiltration provides a unique approach to data security, unauthorized data profiling and data collection. Tools that monitor the flow of outbound traffic and stop attacks in real-time will ensure that no unauthorized data falls into the wrong hands.

This new approach together with the right tools, will help CISO's and their security teams out manoeuvre cybercriminals and malicious insider threats. Preventing them from becoming the next statistic and a data breach headline.

BlackFog's Multiple Layers of Defense

Suspicious

Facebook

Profiling

Cryptomining

Malvertising

Application Gateway

Forensics

Geofencing

Ransomware

Dark Web

Malware

Powershell

BLACKFOG

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

www.blackfog.com