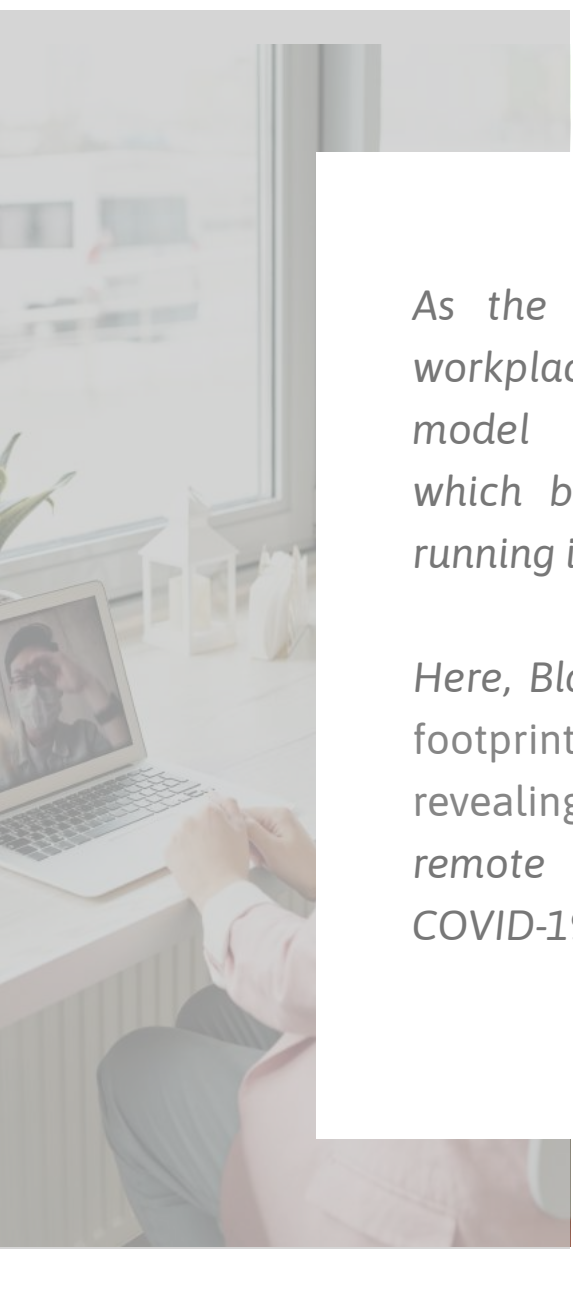
CRITICAL FINDINGS: THE CYBER POSTURE FOR VIDEO CONFERENCING TOOLS

A glance into the cyber-hygiene of video conferencing tools while remote work remains the new normal.

BLACK KITE

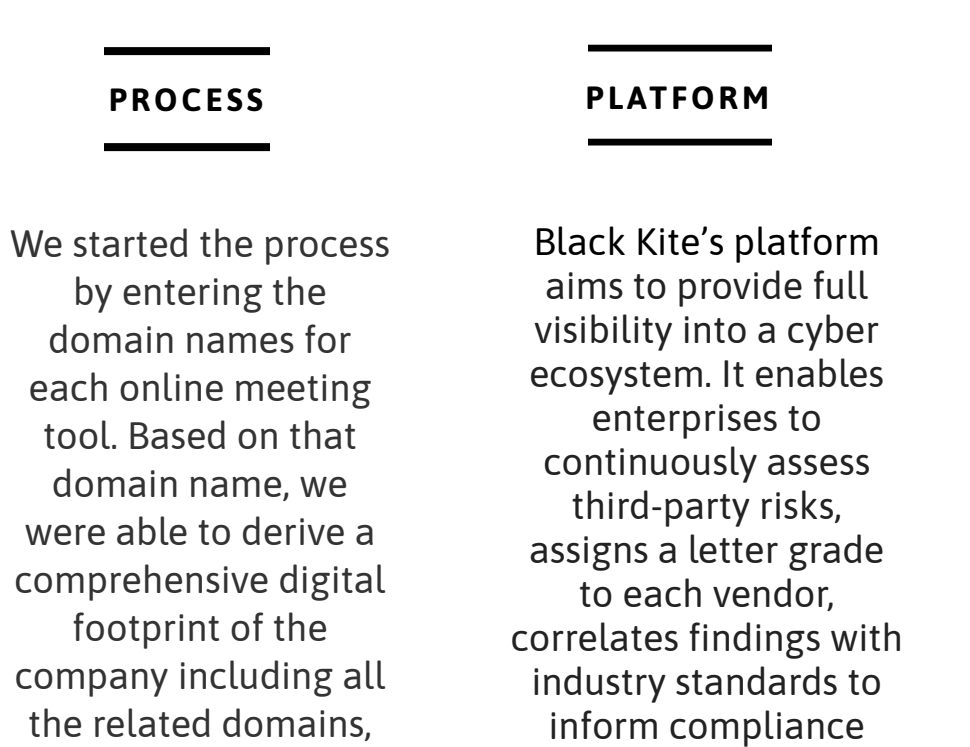


OVERVIEW

As the COVID-19 pandemic spreads worldwide, more workplaces are embracing remote working options. This model increases attention to ***third-party*** *SAAS, in which businesses leverage to keep operations up and running in this unanticipated climate.*

Here, Black Kite identifies the selected company's digital footprint based on their commercially facing domain and revealing the associated vulnerabilities, *as the use of remote working tools ramps up with the outbreak of COVID-19.*

Cyber Scores of the Top 11 Video Conferencing Tools



We made a list of eleven video conferencing tools based on TechRadar's and TrustRadius' Best Video Conferencing Software list. Taking this list, we assessed the external security health of each company's digital footprint based on their commercially exposed domain.

METHOD

PROCESS

We started the process by entering the domain names for each online meeting tool. Based on that domain name, we were able to derive a comprehensive digital footprint of the company including all the related domains, subdomains, IP addresses , services, emails, etc.

PLATFORM

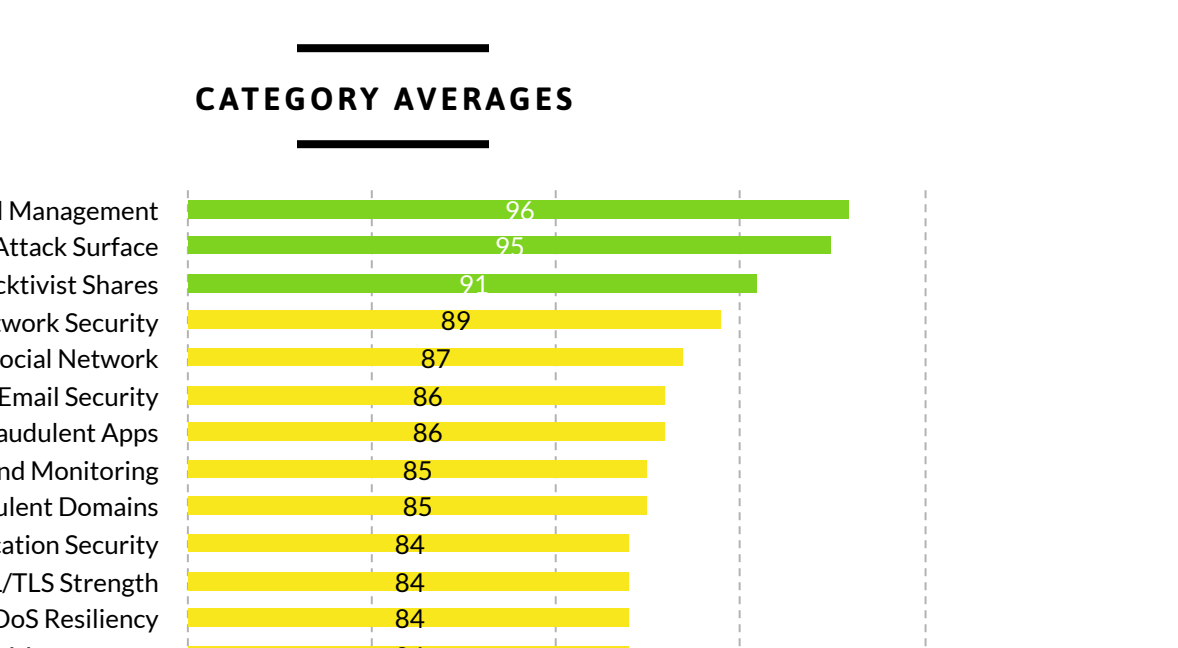
Black Kite's platform aims to provide full visibility into a cyber ecosystem. It enables enterprises to continuously assess third-party risks, assigns a letter grade to each vendor, correlates findings with industry standards to inform compliance requirements, and determines probable financial impact if a third-party experiences a breach.

REASONING

Due to the spike in online tools during the Coronavirus outbreak, video conferencing platforms are under attack through phishing campaigns targeting users, or by using inherent security vulnerabilities on these platforms. Threat actors use this bait to take advantage of companies forced to adopt a remote-working model.

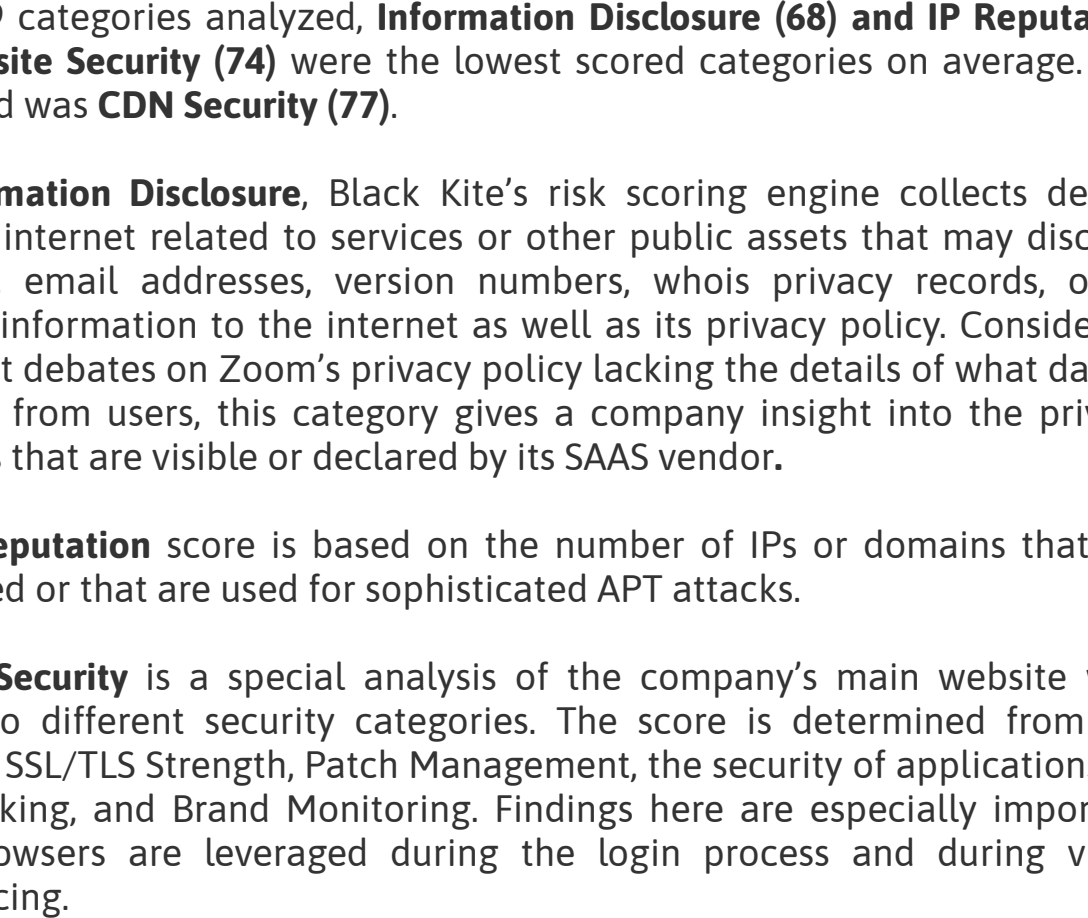
A recent popular attack vector against these platforms is credential stuffing. When successful logins are achieved on the platform, the leaked credentials in older data breaches are compiled into a list and shared on the dark web.

ARCHITECTURE OF VIDEO CONFERENCING TOOLS



Video conferencing applications are cloud-based solutions; whatever message sent through the application is accessible on every device registered under the same account. When users attempt to join a session, the endpoint application or client browser establishes one or more additional connections to communication servers, most of the time using SSL-protected TCP connections.

CATEGORY AVERAGES



Lowest Category Scores

Of the 19 categories analyzed, **Information Disclosure (68) and IP Reputation and Website Security (74)** were the lowest scored categories on average. Not far behind was **CDN Security (77)**.

For **Information Disclosure**, Black Kite's risk scoring engine collects details from the internet related to services or other public assets that may disclose local IPs, email addresses, version numbers, whois privacy records, other sensitive information to the internet as well as its privacy policy. Considering the recent debates on Zoom's privacy policy lacking the details of what data is collected from users, this category gives a company insight into the privacy measures that are visible or declared by its SAAS vendor**.**

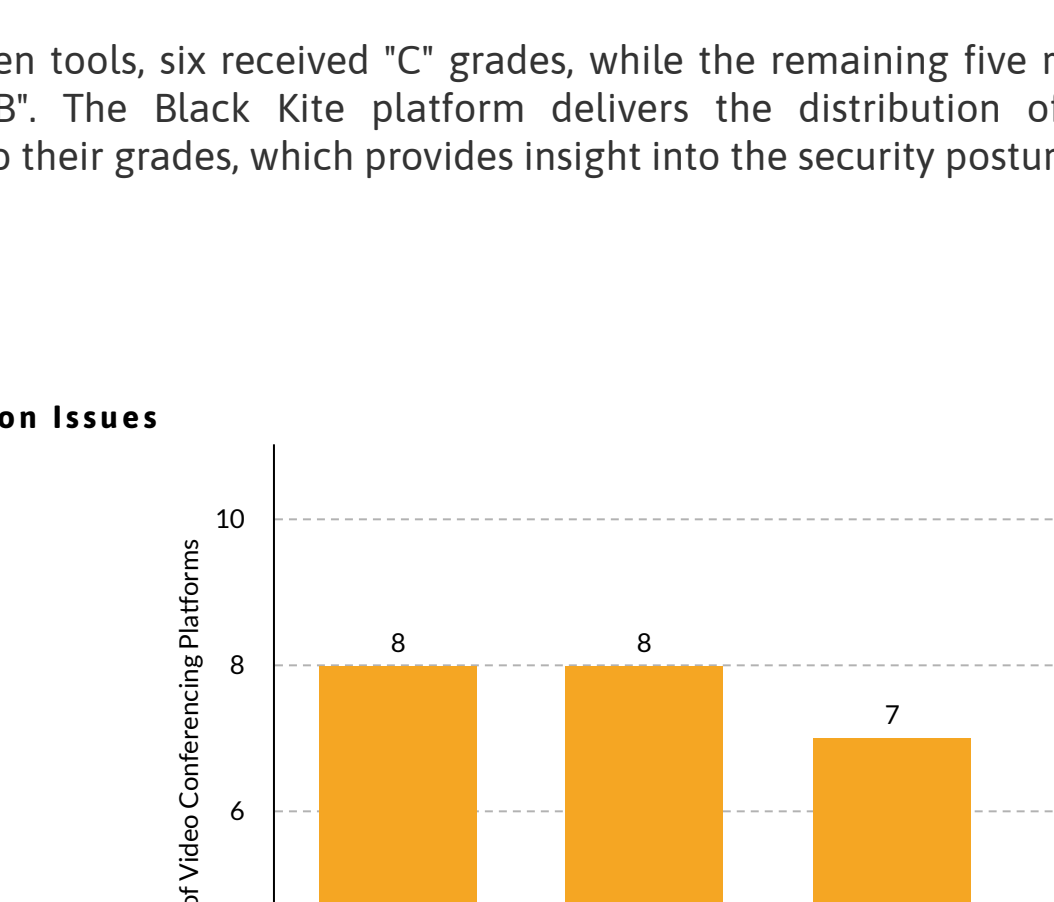
The **IP Reputation** score is based on the number of IPs or domains that are blacklisted or that are used for sophisticated APT attacks.

Website Security is a special analysis of the company's main website with regards to different security categories. The score is determined from the website's SSL/TLS Strength, Patch Management, the security of applications, its Web Ranking, and Brand Monitoring. Findings here are especially important when browsers are leveraged during the login process and during video conferencing.

A **Content Delivery Network** is a large distributed system of servers deployed in multiple data centers across the Internet. This architecture enables users to be served from the closest geographical data centers. Companies use CDNs for online javascript libraries like JQuery.

Some common findings in this category include vulnerabilities associated with *bootstrap* and *jquery* libraries. Using Javascript for hacking through code injections or XSS has become quite popular in hacker society. As in the famous hacker group, "Magecart's" attacks, hackers leverage CDNs or other compromised third-party suppliers to ignite their attacks.

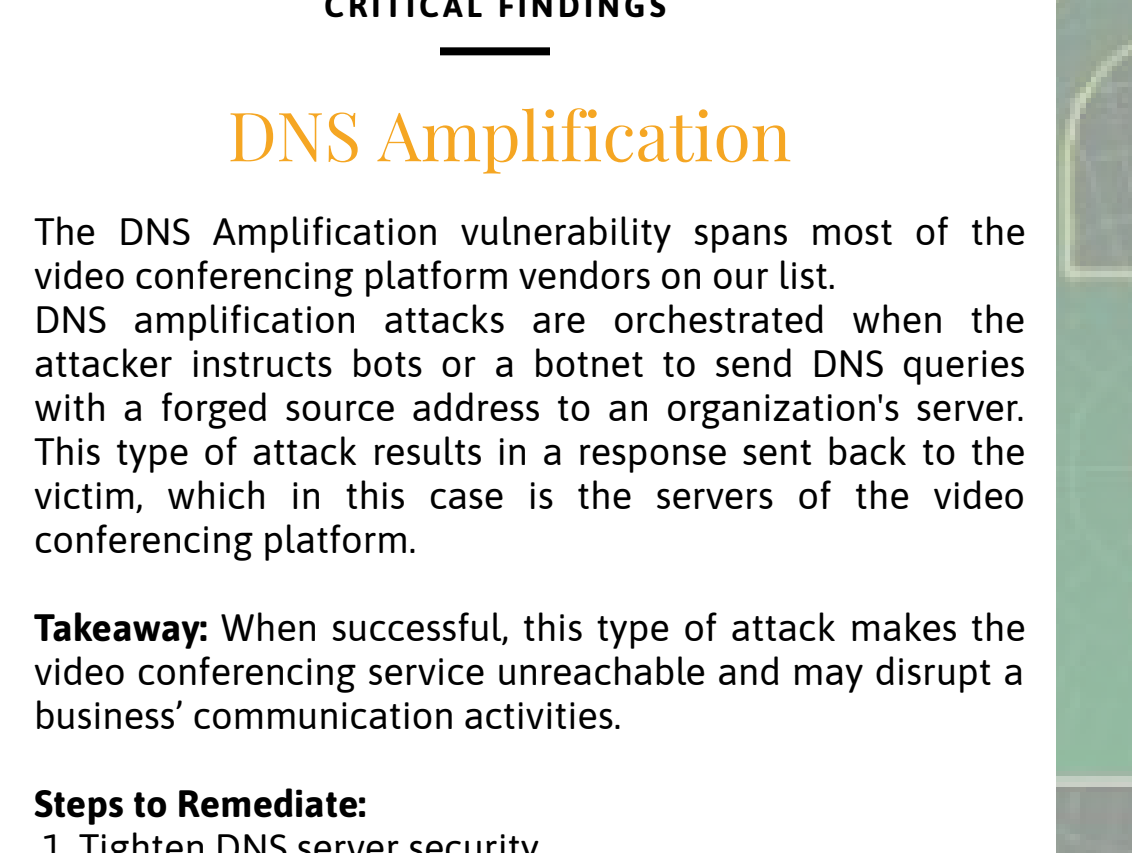
CATEGORY AVERAGES



Black Kite's **3D Vendor Risk @ Scale** SM platform provides easy-to-understand letter grades in each risk category. Here, we see the average weighted cyber score of our top ten online meeting tools list is "C+".

Of the eleven tools, six received "C" grades, while the remaining five received a grade of "B". The Black Kite platform delivers the distribution of vendors according to their grades, which provides insight into the security posture.

Most Common Issues



CRITICAL FINDINGS

DNS Amplification

The DNS Amplification vulnerability spans most of the video conferencing platform vendors on our list.
DNS amplification attacks are orchestrated when the attacker instructs bots or a botnet to send DNS queries with a forged source address to an organization's server. This type of attack results in a response sent back to the victim, which in this case is the servers of the video conferencing platform.

Takeaway: When successful, this type of attack makes the video conferencing service unreachable and may disrupt a business' communication activities.

Steps to Remediate:
1. Tighten DNS server security
2. Block specific DNS servers or all open recursive relay servers

CRITICAL FINDINGS

Invalid, Incorrect, Expired or Self-Signed SSL Certificates

Complications with SSL Certificates is one of the most frequent and critical issues we discovered on the digital assets. SSL protocol ensures user information travels safely through the internet in a secure manner if the certificate is trusted. This protocol helps prevent an ill-intentioned attacker from sniffing the network to steal confidential information like users' credentials

Takeaway: Lacking SSL controls on servers puts the privacy of the meeting, the content, messages, and transferred files at risk.

Steps to Remediate
Check whether the
· The certificate is revoked
· It is self-signed
· The certificate chain is broken or
· The domain specified in the certificate does not match the website.

Mitigate the reason(s) that apply to the system.

CRITICAL FINDINGS

Fraudulent Domains

As the third most critical finding, fraudulent domains and subdomains are look-a-like domains mimicking an application's original site. Domain name scams are types of Intellectual property scams or confidence scams in which unscrupulous domain name registrars attempt to generate revenue. These scams often involve tricking businesses into buying, selling, listing or converting a domain name extracted from the domain registration database.

Takeaway: Fraudulent or scam domains are frequently used by phishing attacks targeting a company's employees or customers. Security awareness is the first line of defense in preventing users entering fraudulent sites. Integrating fraudulent domains as blacklists to the SIEM infrastructure may help as well.

Steps to Remediate
- Educate your staff (Security awareness is the first line of defense in preventing users from entering fraudulent sites)
- Continuously check for look-a-like domains on community services

CRITICAL FINDINGS

Vulnerable Jquery libraries from Content Delivery Networks (CDN)

Some common findings we came across in the CDN security posture of video conferencing platforms include vulnerabilities associated with bootstrap and jquery libraries in which video conferencing servers leverage. The problem is mainly associated with jQuery libraries of versions before 3.0.0. These versions are vulnerable to Cross-site Scripting (XSS) attacks

Takeaway: Know your SAAS vendors. Know your CDNs as well as those of your vendors. Never execute responses from 3rd party origins by default and do not make it an option**.**

Steps to Remediate
1. Always use secure and up-to-date version of CDN resources
2. Never load CDN script via XMLHTTPRequests which may violate Cross Origin Resource Sharing (CORS) Policy

Why does the "Security Posture" matter?

With a drastic increase in remote work during the Coronavirus outbreak, video conferencing platforms are under attack through either phishing campaigns targeting users, or through inherent vulnerabilities in security. Threat actors use this bait to take advantage of companies forced to adopt a remote-working model. The cybersecurity rating Black Kite assigns provides insight into a platform's external cybersecurity posture through the eyes of a hacker.

This assessment takes place in 20 categories, from Credential Management and Application Security to Fraudulent Domains and Apps, giving a holistic view of a company's external security posture.

Why does the "Security Posture" matter?

End-to end Encryption Or Transport Layer Encryption

Individuals and businesses often expect end-to-end encryption during platform use. However, this feature is not available in every online meeting platform.
Apple's FaceTime is currently the only known application allowing end-to-end encryption in group communications.

A Zoom spokesperson recently announced, "Currently, it is not possible to enable E2E encryption for Zoom video meetings. Zoom video meetings use a combination of TCP and UDP. TCP connections are made using TLS and UDP connections are encrypted with AES using a key negotiated over a TLS connection."

Most of the time, only the user-server communication portion is encrypted, known as Transport Layer Security. The content is decrypted as it enters the Cloud. In reality, group video conferencing is difficult to encrypt end-to-end. The service provider needs to first detect who is talking, which then only allows the platform to send a high-resolution video stream from the person actively speaking.

Authentication

Most platforms enable role-based authorization, depending upon the ability to correctly identify and authenticate every user. For Zoom, the host is able to start a secured meeting with a password. When logging into the application or system, passwords with at least eight characters including both letters and numbers must be enabled to make them difficult to uncover.

Stored passwords should be resilient to offline dictionary attacks. Captcha protection is a recommended remediation against online brute-force attacks. Multi-factor authentication should also always be enabled as an extra layer of security against both bots and stolen credentials.

Network Security

It is also important which network controls are in place to secure the infrastructure and backend servers. With businesses leveraging these services as part of their business-as-usual activities, it means they are extending their perimeter to those of their SAAS vendors. Infrastructure security shall be continuously monitored both as an outside-in approach and internally.

For a detailed look into the recent debate on security of these tools , click here!

The Black Kite (formerly known as NormShield) platform's intuitive interface compiles reports and communicates risks in qualitative, quantitative, and easy to understand business terms for executives. The interface also allows IT-security teams to drill down to the technical details in each risk category.

With the alerting mechanism, the users of the platform become aware of the security vulnerabilities within a cyber ecosystem promptly and can take immediate actions.

W W W . B L A C K K I T E T E C H . C O M