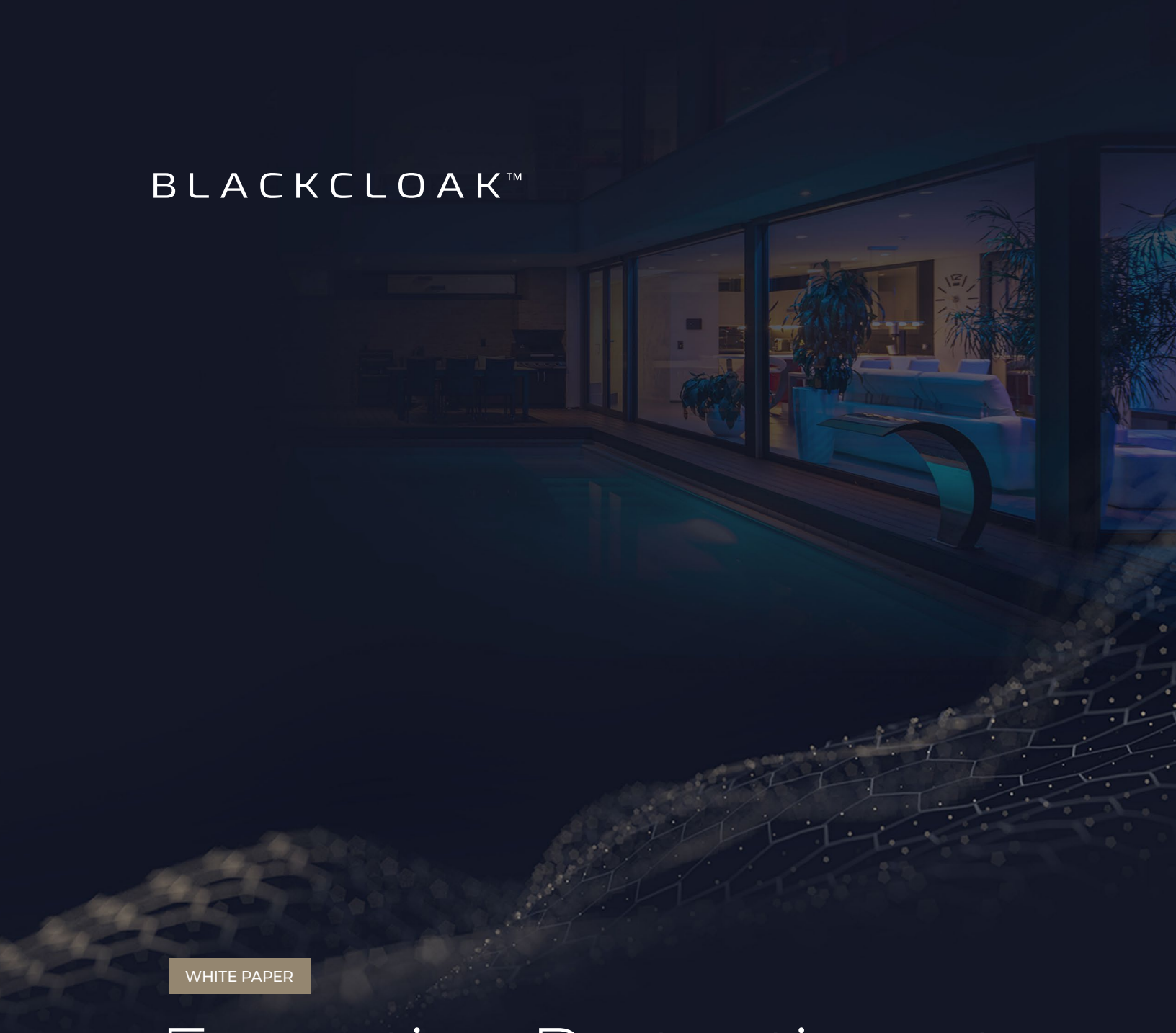
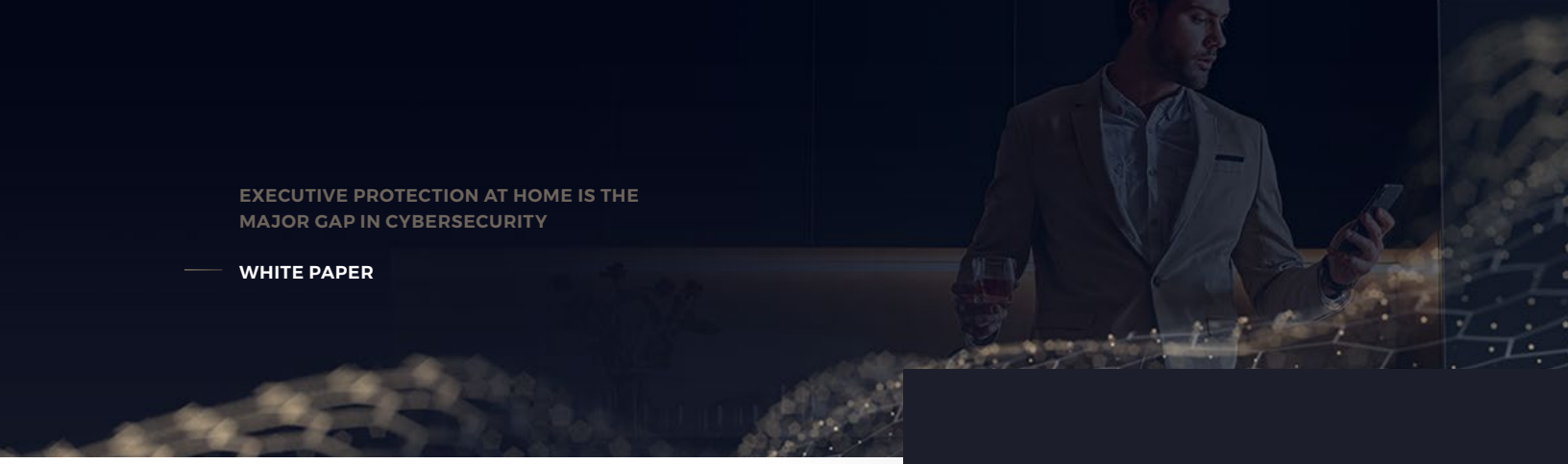
BLACKCLOAK™



WHITE PAPER

Executive Protection at Home is the Major Gap in Cybersecurity

www.blackcloak.io



INTRODUCTION

EVERYONE HAS SOMETHING OF VALUE TO A CRIMINAL.

While many of us do not realize it, industrious hackers are interested in gaining access to just about any set of personal and private data and assets so that these materials can be exploited. The level of the value lies in how much the payoff may be once the criminal steals the private data and puts it to work for nefarious purposes. For a key executive or board member, the pay off potential is obviously high.

That's why it is critical for the CISO to consider the home lives of key employees as part of the attack surface for the organization they want to protect. Although organizations invest millions of dollars in cybersecurity to protect corporate assets and keep employees safe when they use company tools, as soon as those employees head home each day or switch over to working on a family device or personal email account, the CISO loses control and the company is at risk.

Criminals are increasingly targeting employees at home – especially high-profile executives – with the knowledge that access to an employee with authority and high-level access through their personal life is invaluable.

Criminals are increasingly targeting employees at home – especially high-profile executives – with the knowledge that access to an employee with authority and high-level access through their personal life is invaluable.

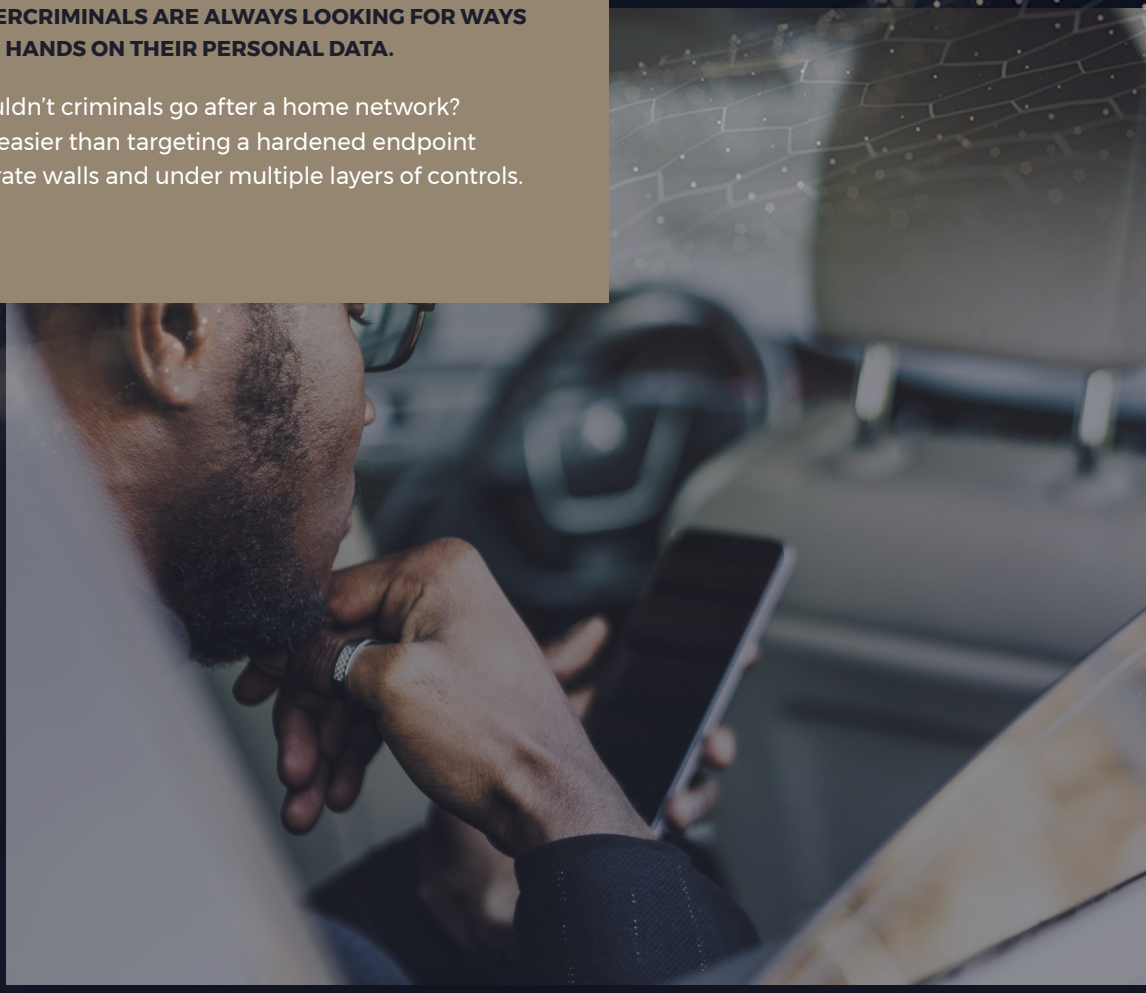
Unfortunately, it is very difficult for a CISO or corporate security leader to protect the personal lives of their executives once they leave the confines of the office. High-level individuals now have a single, unified digital life, and senior leadership working from home has become the soft underbelly of corporate cybersecurity. The attack surface of the organization increases every time an executive works remotely from home – and CISOs do not have nearly enough visibility into what goes on in the home of an executive; no insight into the security of the home network, the personal devices used, the personal email accounts, passwords, and privacy footprint of the executive when they are out of the office.

— SECTION 1

WHAT'S AT STAKE?

THE HIGH-PROFILE EXECUTIVE IS A TARGET WHEREVER THEY GO, AND CYBERCRIMINALS ARE ALWAYS LOOKING FOR WAYS TO GET THEIR HANDS ON THEIR PERSONAL DATA.

And why wouldn't criminals go after a home network? It is infinitely easier than targeting a hardened endpoint within corporate walls and under multiple layers of controls.



THE NUMBERS REVEAL JUST HOW VULNERABLE EXECUTIVES ARE AND HOW ATTRACTIVE THEY ARE TO HACKERS.

In fact, C-suite executives are 12 times more likely to be targeted in cyber attacks than other employees in their organization, according to Verizon's Data Breach Investigations Report. And the DBIR also finds cyber criminals targeting senior business leaders typically focus on financial rewards: 71 percent of C-suite cyberattacks were financially motivated, with attackers looking to make money from the company or employee data, intellectual property, or ransomware.

C-suite executives are

12 Times More Likely

to be targeted in cyber attacks

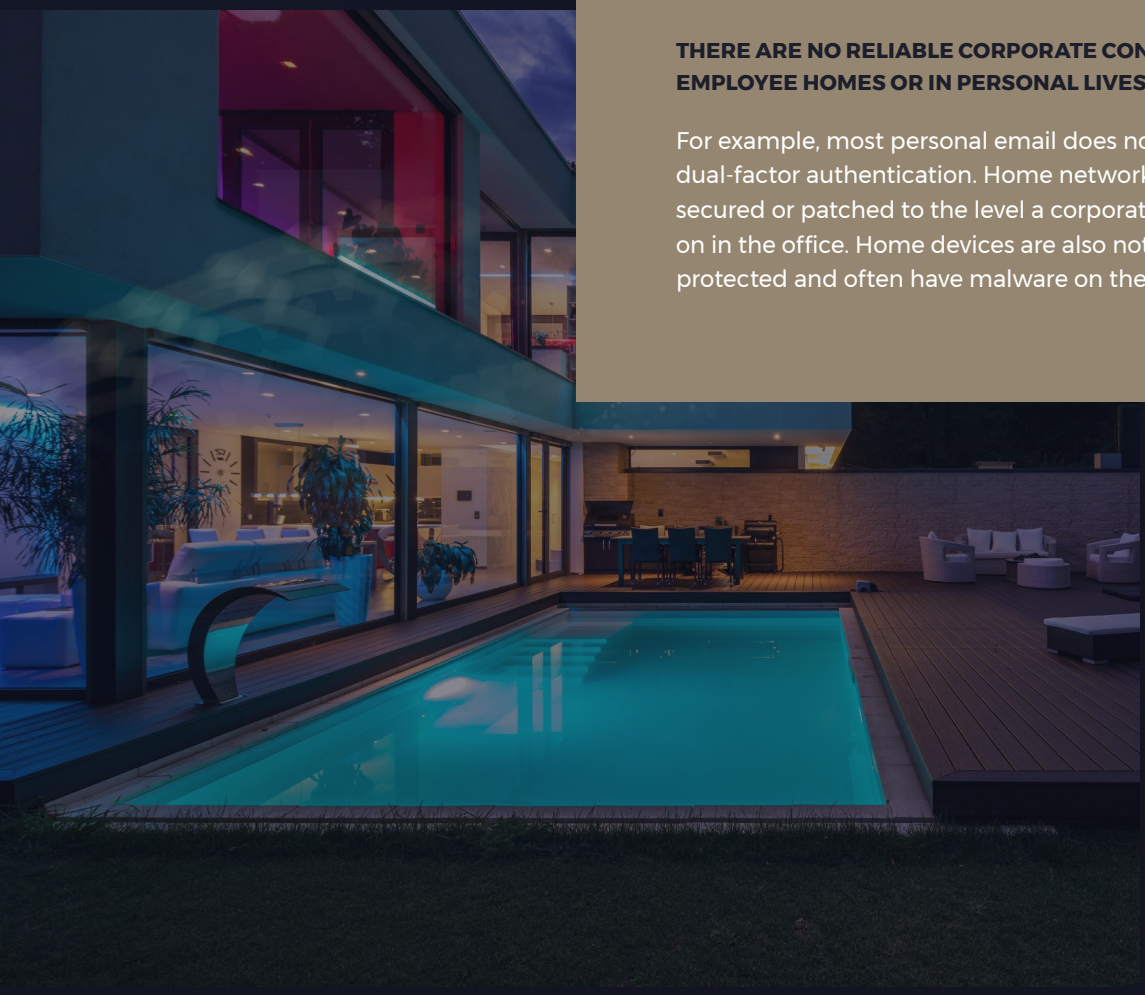
Meanwhile, malware is always evolving and becoming more sophisticated and stealth. According to the 2020 M-Trends report from cybersecurity company FireEye, 41 percent of malware deployed in 2019 was new and never seen before. A report from CyberCube titled Understanding Ransomware Trends finds organized criminals and hackers are moving away from high-volume, low-value methods of attack against private individuals and instead are targeting senior managers with access to bank accounts who can authorize payments.

CISOs simply can't afford to miss the potential of a home-based attack in today's environment.

If a criminal gains access to an executive and breaches private, corporate information or IP, or takes control of an executive account, the risks are numerous. *For example,* damage to reputation can occur if the targeted executive is embarrassed by the leak of personal information that can cast a bad light on the company. Other risks include intellectual property theft or even extortion. Productivity issues can arise as the hack can be distressing for both the executive and the company, which can cut into the executive's valuable time. There is also the possibility of public disclosure risk and, of course, serious financial loss.

— SECTION 2

THE THREAT LANDSCAPE AT HOME



THERE ARE NO RELIABLE CORPORATE CONTROLS AT EMPLOYEE HOMES OR IN PERSONAL LIVES.

For example, most personal email does not have dual-factor authentication. Home networks are not secured or patched to the level a corporation would insist on in the office. Home devices are also not adequately protected and often have malware on them.

As BlackCloak has onboarded new clients, we have observed that 39 percent of corporate executives have malware on their personal devices or have wide-open cameras and home networks. We have also found that a majority (59 percent) of the C-Suite does not have anti-virus on their personal devices. In 75 percent of cases we find computers either totally unprotected or they still have the default security settings, which is just as bad as no protection at all. And password hygiene is no better among executives, as we found 68 percent of the C-Suite is writing down their passwords on personal notebooks or storing them in their contacts list on the phone.

The lives of these executives have become frictionless between the personal and the professional. Gmail and LinkedIn accounts contain information that would be damaging if stolen and shared. Executive cybersecurity protection could be extended to the home front for a tiny fraction of the existing cybersecurity spend of many large companies.

Without the proper controls, criminals can easily hack into company resources using the executive as a conduit to sensitive information – and no executive is immune to these kinds of threats. Even Amazon billionaire Jeff Bezos had his mobile phone exploited. In a 2018 incident, after receiving a WhatsApp message that had apparently been sent from the personal account of the crown prince of Saudi Arabia, the encrypted message was purported to have included a malicious file that infiltrated Bezos's phone. Password reuse on different accounts may have been to blame in the incident, and, unfortunately, executives are not immune to making that very common mistake. But CISOs have no way of knowing if passwords are being reused between home and company accounts.

Even Amazon billionaire Jeff Bezos had his mobile phone exploited. In a 2018 incident, after receiving a WhatsApp message that had apparently been sent from the personal account of the crown prince of Saudi Arabia, the encrypted message was purported to have included a malicious file that infiltrated Bezos's phone.

75%

of cases we find computers either totally unprotected or they still have the default security settings

59%

of the C-Suite does not have anti-virus on their personal devices

39%

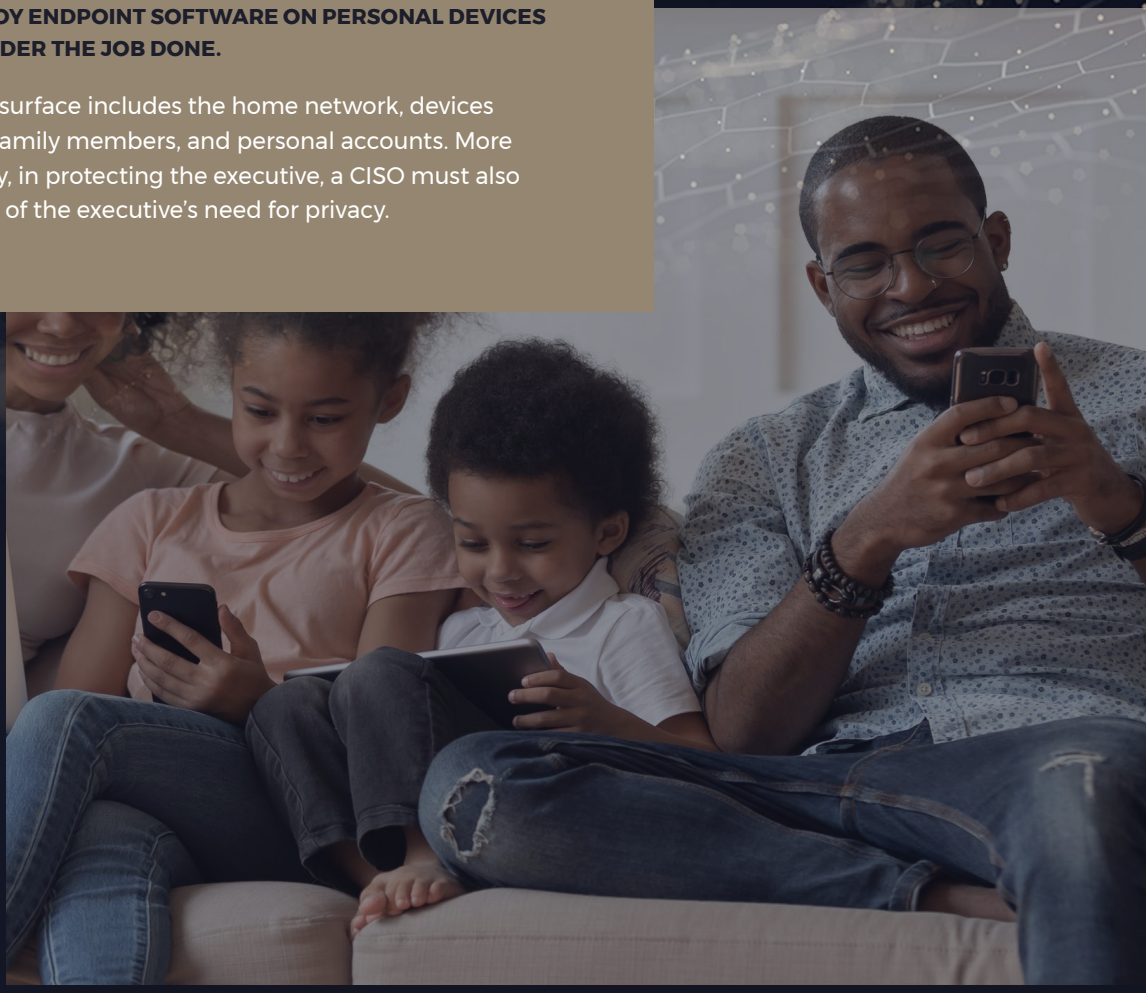
of corporate executives have malware on their personal devices or have wide-open cameras and home networks

— SECTION 3

THE CHALLENGES FOR THE CISO

UNFORTUNATELY, IN THEIR EFFORTS TO PROTECT EXECUTIVES AT HOME AND ON THE ROAD, A CISO CAN'T JUST DEPLOY ENDPOINT SOFTWARE ON PERSONAL DEVICES AND CONSIDER THE JOB DONE.

The attack surface includes the home network, devices shared by family members, and personal accounts. More importantly, in protecting the executive, a CISO must also be mindful of the executive's need for privacy.



CISOs should not monitor the home network of the employee because there is really no way to use corporate tools in the home environment without capturing data the company really should not see or have access to – everything from types of devices in the home to netflow data.

Consider these scenarios that introduce new risks to the company:

In monitoring, the CISO could capture data on the significant other, children, friends, or relatives. Some of which could be privileged and confidential data or sensitive.

While the CISO may use endpoint protection on the executive's personal laptop, they would not be fully protected unless all family devices are covered. For example, the CISO would also need to cover a shared tablet used by children or spouses, which may cross a line into violating privacy.

By using company personnel to monitor the home, it might bring any incidents under a corporate disclosure policy where they should not be.

THINK OF IT LIKE HEALTHCARE –
the company offers healthcare through a third party and the executives benefits, but the medical professionals are not employees of the company and it receives no specific information. It should be the same for personal cybersecurity for the executive.

The only way to provide the proper level of security to combat this risk is to do so with a concierge program that does the following:

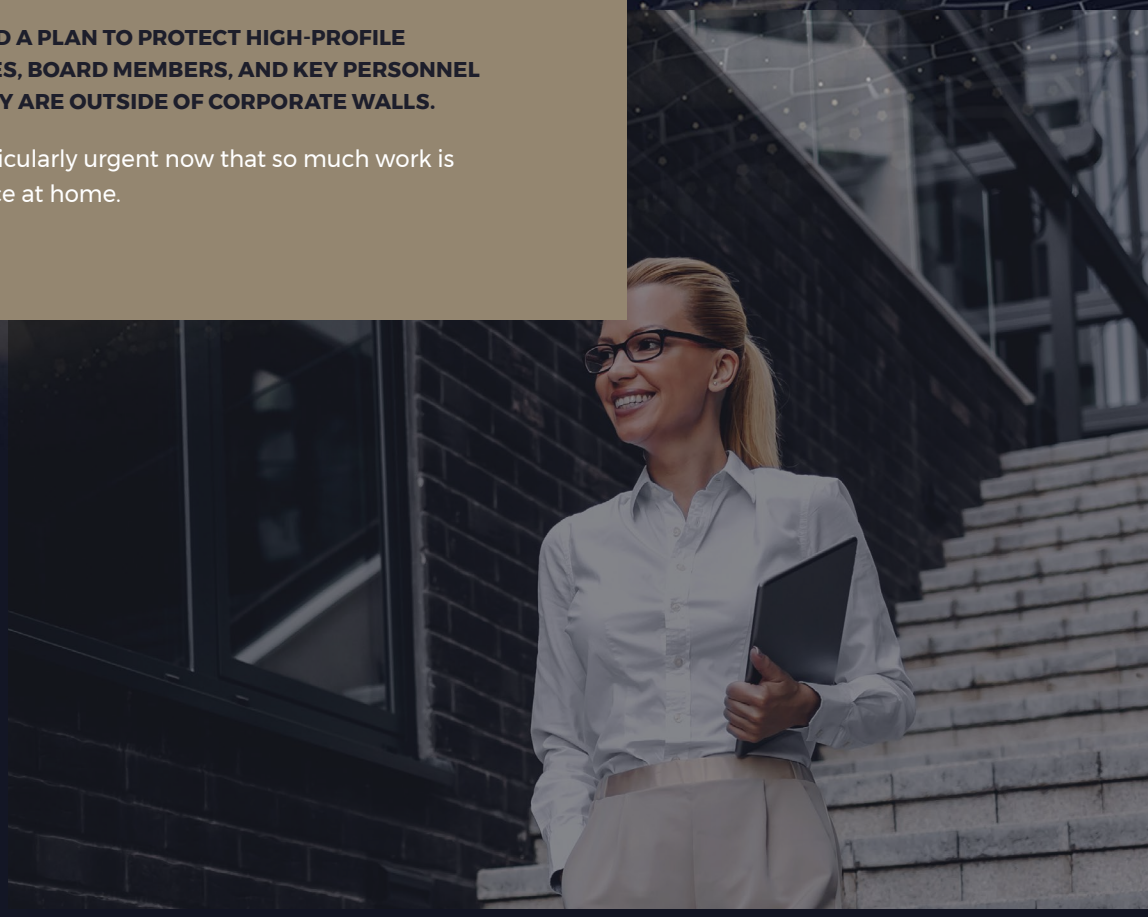
- → separates the executive's personal life and family from company personnel;
- → maintains service level agreements;
- → does not report back to the company on specific people or risks.

— SECTION 4

THE FOUR CIRCLES OF EXECUTIVE PROTECTION

CISOS NEED A PLAN TO PROTECT HIGH-PROFILE EXECUTIVES, BOARD MEMBERS, AND KEY PERSONNEL WHEN THEY ARE OUTSIDE OF CORPORATE WALLS.

This is particularly urgent now that so much work is taking place at home.



Protect Your **Executives**, Protect Your **Company**

We deliver a holistic program built on a comprehensive platform that enables you to Protect Your Company by Protecting Your Executives™ in four critical aspects of cybersecurity and privacy.

Protect Their
PRIVACY

We remove sensitive personal information from Internet Data Brokers, perform dark web searches for exposed personal credentials, and implement privacy settings to protect against data leakage and identity theft.

Protect Their
HOME

We perform penetration testing and regular scans of your home networks to detect compromised networks, weak cybersecurity, BotNets and other security issues, and to prevent decisions children and family make online from resulting in a compromise.

Protect Their
DEVICES

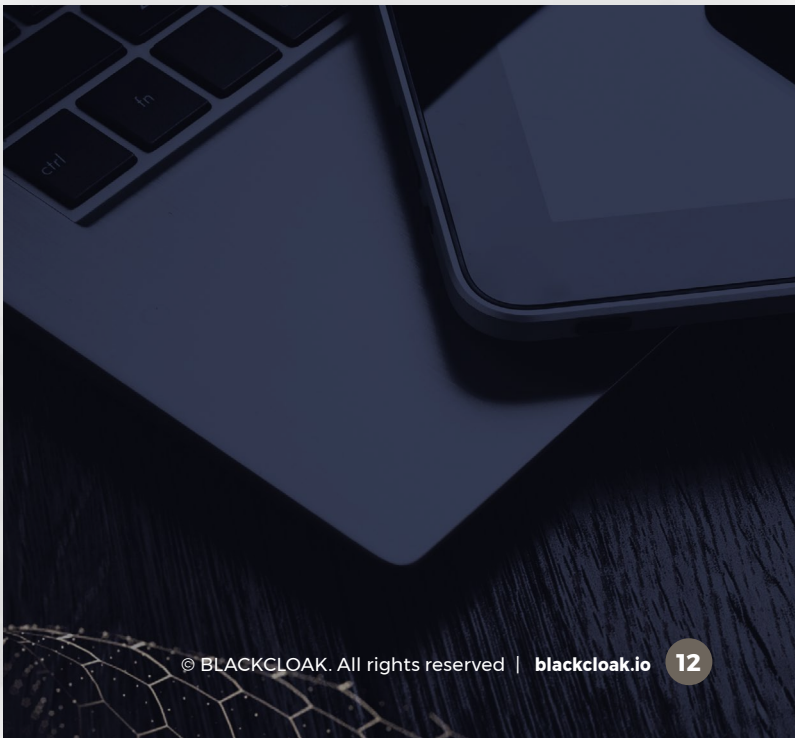
We monitor and secure personal devices, including cell phones, tablets and computers, using BlackCloak's proprietary technology and the same enterprise-grade tools to secure corporate networks and devices.

Protect Their
PEACE OF MIND

With BlackCloak as your trusted partner, you'll protect what matters most and have control over managing executive cybersecurity and privacy risk – and your team's personal cybersecurity advisor will always be just a call, tap, or text away.

A holistic plan considers all of the homes that the executive may frequent – including vacation homes. It should also include planning to protect family members and assistants who can be a conduit for criminals to gain access to private and sensitive data through their own digital habits and accounts. Finally, the holistic plan should be orchestrated with a platform that encompasses all the above factors in one place to ensure service level agreements are met for both the company and the executive.

Cybersecurity for executives at home can no longer be an afterthought as the line has thoroughly blurred between home and office. The protection of their digital lives must be 24x7. Similar to the way executives receive concierge healthcare and other executive perks to make their personal lives better, simpler, and easier to manage given all the other corporate stressors, so too must cybersecurity protection be offered as a corporate benefit. Companies must extend protection of the CEO's digital life and health in the same way—with a Concierge Cybersecurity solution.



CONCLUSION

CISOS HAVE A MASSIVE UNDERTAKING DAILY IN SECURING THEIR CORPORATE NETWORKS AND ASSETS.

The last thing they need to worry about is protecting executives, board members, and key personnel at home. Yet, if the executive home is overlooked, it leaves a major gap in overall security strategy.

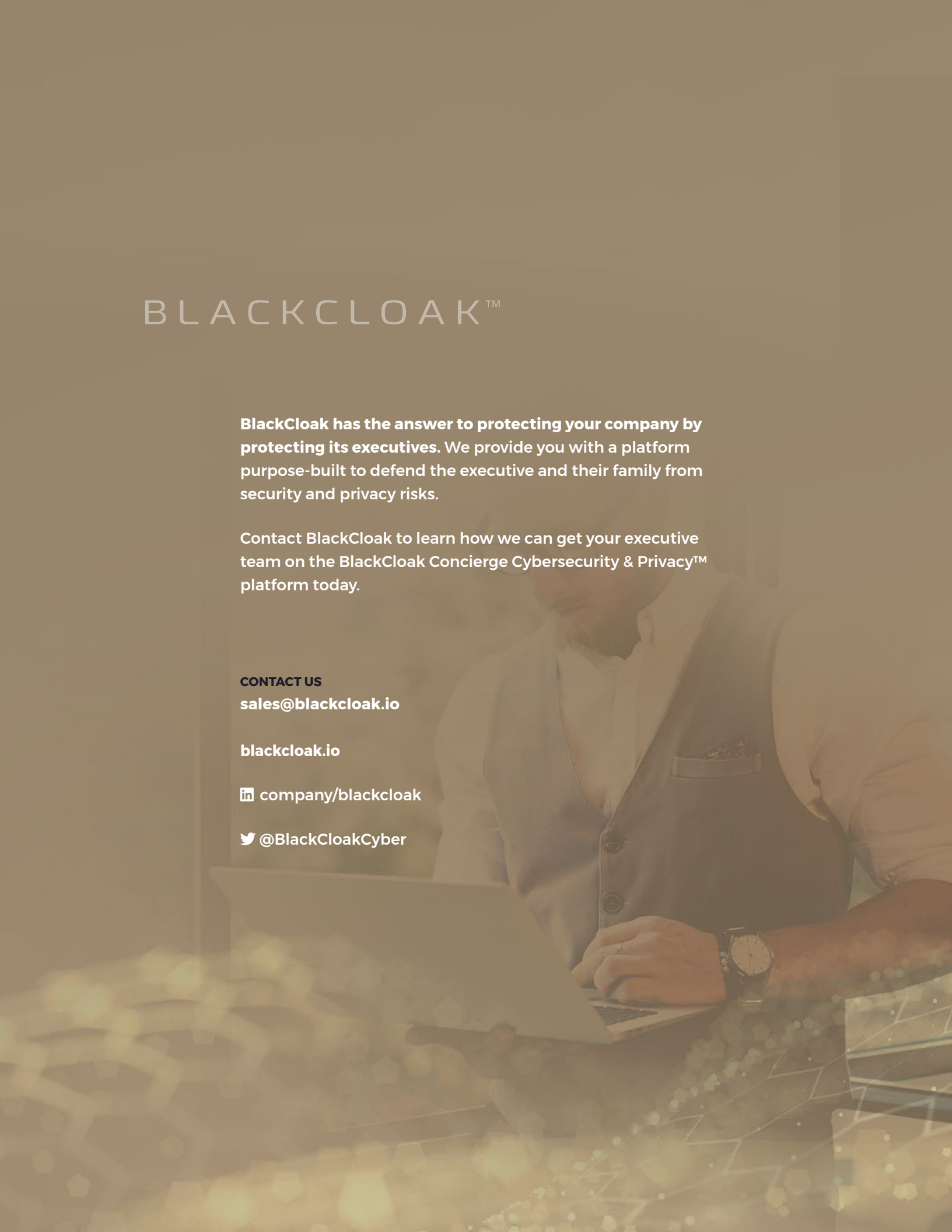
CISOs need a guide to help them navigate the critical elements of executive protection at home so they can focus on the job of securing the company. With a trusted solution partner, CISOs can rest assured the executives and therefore the company are protected, while saving themselves both time and the distraction from their overall security strategy. And, because it is an outsourced provider, the executive can maintain their personal privacy.

With a trusted solution partner, CISOs can rest assured the executives and therefore the company are protected, while saving themselves both time and the distraction from their overall security strategy.

BLACKCLOAK™

BlackCloak has the answer to protecting your company by protecting its executives. We provide you with a platform purpose-built to defend the executive and their family from security and privacy risks.

Contact BlackCloak to learn how we can get your executive team on the BlackCloak Concierge Cybersecurity & Privacy™ platform today.



CONTACT US

sales@blackcloak.io

blackcloak.io

company/blackcloak

@BlackCloakCyber