BlueFort Security

Intelligence-led Cyber Visibility

White Paper

www.bluefort.com

Introduction

Few things stand the test of time. But when he was US Secretary of State for Defence, Donald Rumsfeld gave a speech which contained perhaps one of the most well-remembered, and often quoted phrases from the recent past:

> “We know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns — the ones we don't know we don't know. And if one looks throughout the history of our country and other free countries, it is the latter category that tends to be the difficult ones.”

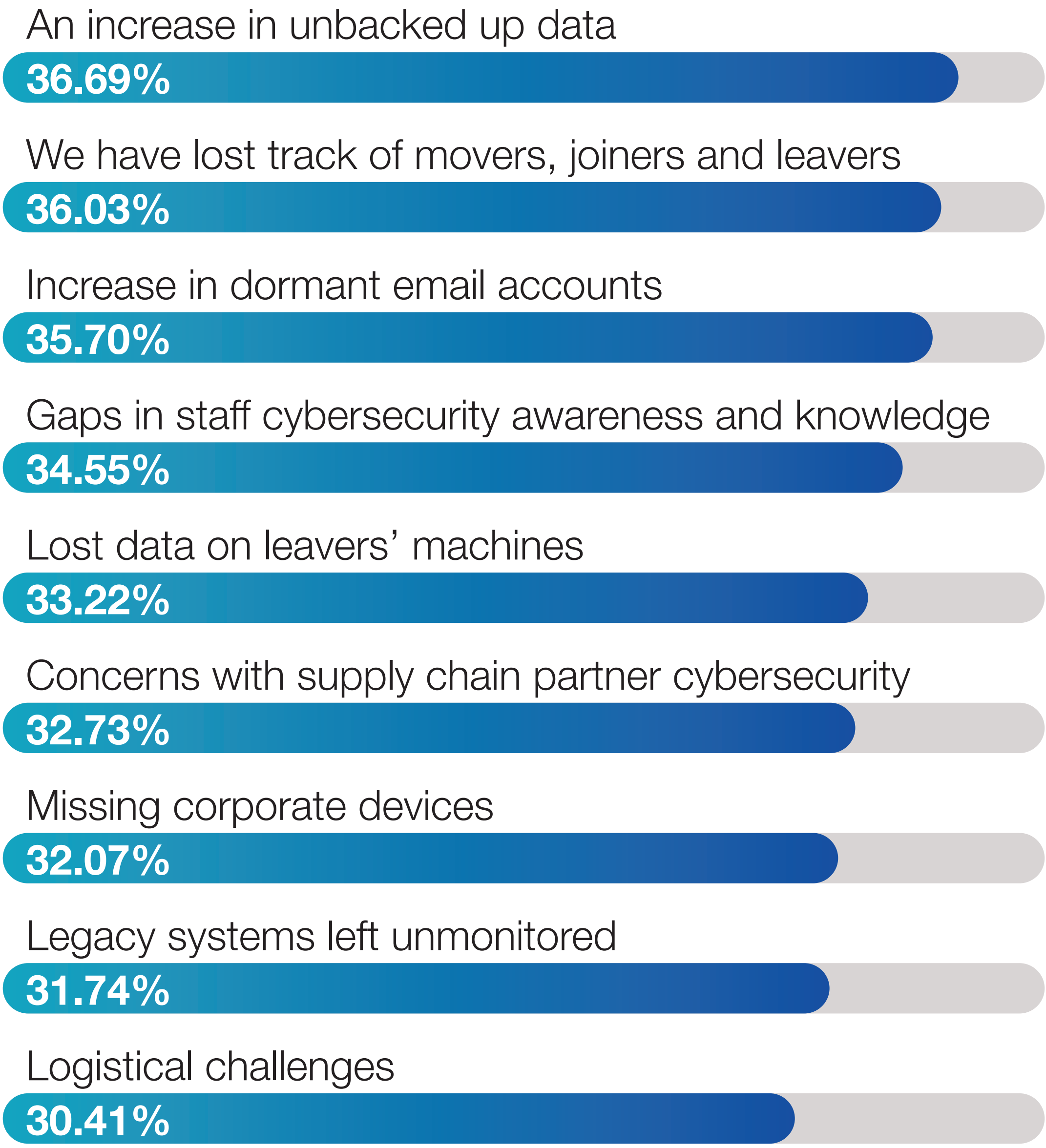
A bit of a tongue-twister perhaps but the essence of what Mr Rumsfeld said can be applied to all walks of life.

When it comes to cybersecurity, IT landscapes are complex, often untamed and usually unpredictable. There are many known unknowns, and there are even more unknown unknowns. In an environment where attack surfaces are increasing as fast as a workforce is dispersing and cyber criminals are becoming ever more sophisticated in their methods of attack, CISOs and IT security professionals alike are balancing on the precipice of losing control of their users, data, assets and being unable to protect their infrastructure.

BlueFort’s 2022 CISO Survey, which spoke to 600 UK CISOs, revealed the extent of the challenge, stating that many admit to lack of visibility, intelligence and control over much of their organisation’s estate. Over half (57%) admitted that they do not know where all their data is, or how it’s protected.

What security challenges, if any, have you experienced in the last 12 months?

(Bluefort CISO Survey 2022)



The lack of - or limited - visibility over their organisation's estate is the root cause to many of the challenges organisations are facing. If there is no clear visibility over the IT estate, it is not possible to gain accurate intelligence about it, nor have any control over it. Only when visibility is clear, can intelligence be wrapped around the "known" elements enabling positive controls to be put in place.

Visibility Roadblocks

Most security teams will be all too familiar with the common visibility roadblocks which typically stem from either too much, or too little, information. Intelligence-led visibility is about gaining insight and context that enables you to identify and prioritise the most important threats facing your business. If you are experiencing some, or all of the challenges below the chances are you don't have full visibility - and therefore control - over your IT estate.

Information Overload

With the plethora of tools available, it would be hard to find a security analyst who's short of information. The vast majority find themselves suffering from information overload. There's simply too much of it. They have lots of visibility - but they are not able to make sense of what is being presented to them and therefore they are not using it in the right way.

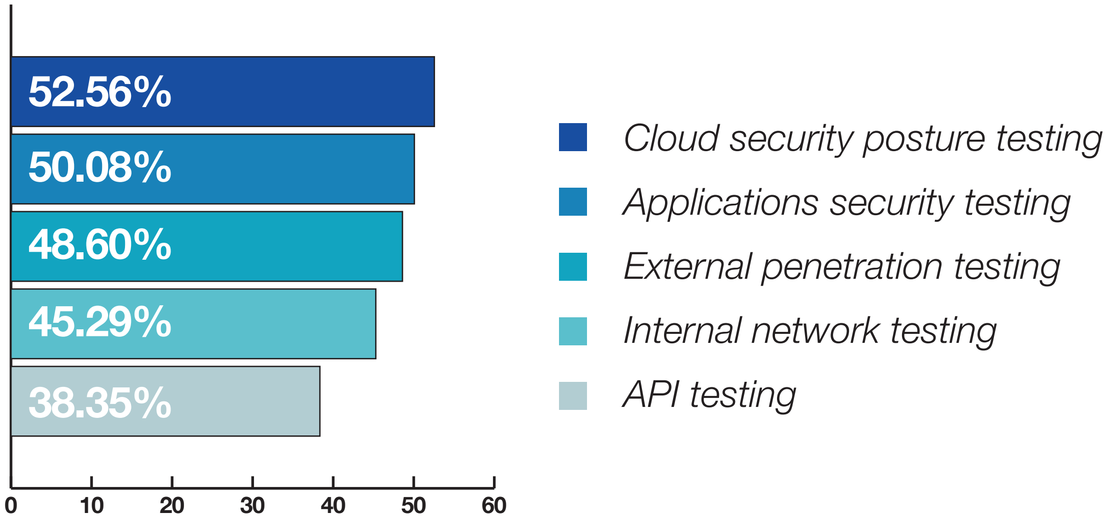
Cloud adoption

Enabling cloud transformation is now a key focus area for UK security leadership. BlueFort's recent CISO study found that more than half (57%) of organisations are using multiple clouds and 37% are using a single cloud environment. Securing the cloud and its (primarily cloud-based applications) must be a priority - yet it remains one of the biggest visibility roadblocks for organisations today. The same survey revealed that a significant proportion (42%) can only partially enforce cloud application security policies, while 5% are unable to at all. With people and assets spread around the world, enabling visibility of a firm's cloud environment has moved from effectively looking in one room, to looking in every building, in every street, in every city, around the globe. A mammoth task.

Skills gap

Compounding the effects of the information overload is a persistent cybersecurity skills shortage and the additional burden of regulatory compliance, which drains the already limited resources dedicated to threat detection and response. Churn: CISOs struggle to retain cybersecurity staff is exacerbated by limited resources available to cope with the basics of cyber security. Compounding this is the fact that most CISOs are also losing track of movers, joiners and leavers across the business. This is a common security challenge encountered by organisations, as is lost data on leavers' machines.

There are huge gaps in where CISOs have been focusing validation efforts for their security stack:



Employee working behaviour

Employees routinely and persistently practise insecure working behaviours - connecting to public WiFi, and not flagging suspicious or malicious emails, for example - which only serves to make the situation worse.

Changing external threat landscape

Cyber risks are on the rise. The volume and variety of attacks - particularly ransomware - is growing exponentially. On top of that, according to analysis by The Stack* of common vulnerabilities and exposures (CVEs) data, the number of critical vulnerabilities in 2022 was up 59% on the previous year. This is equivalent to a fresh CVE being created every 20 minutes. With new vulnerabilities identified every day and more and more organisations falling victim to cyber attacks, the effectiveness and efficiency of many cybersecurity activities must be questioned.

**Source: https://thestack.technology/analysis-of-cves-in-2022-software-vulnerabilities-cwes-most- dangerous/*

Effective visibility requires a transformational approach. What's needed is a clear understanding of which bit of visibility you are dealing with and then turn that information into contextual, actionable intelligence.

Visibility Journey

The goal is for visibility to be organic – removing manual processes and reducing noise to establish visibility of all data, threats, remediation opportunities and effectiveness of existing protection. While this might sound like an insurmountable task, breaking the journey down into priority-based steps provides a clear roadmap to build on over time. It's important to remember that improving visibility is not about seeing more problems that you can't solve but solving problems before you see them.

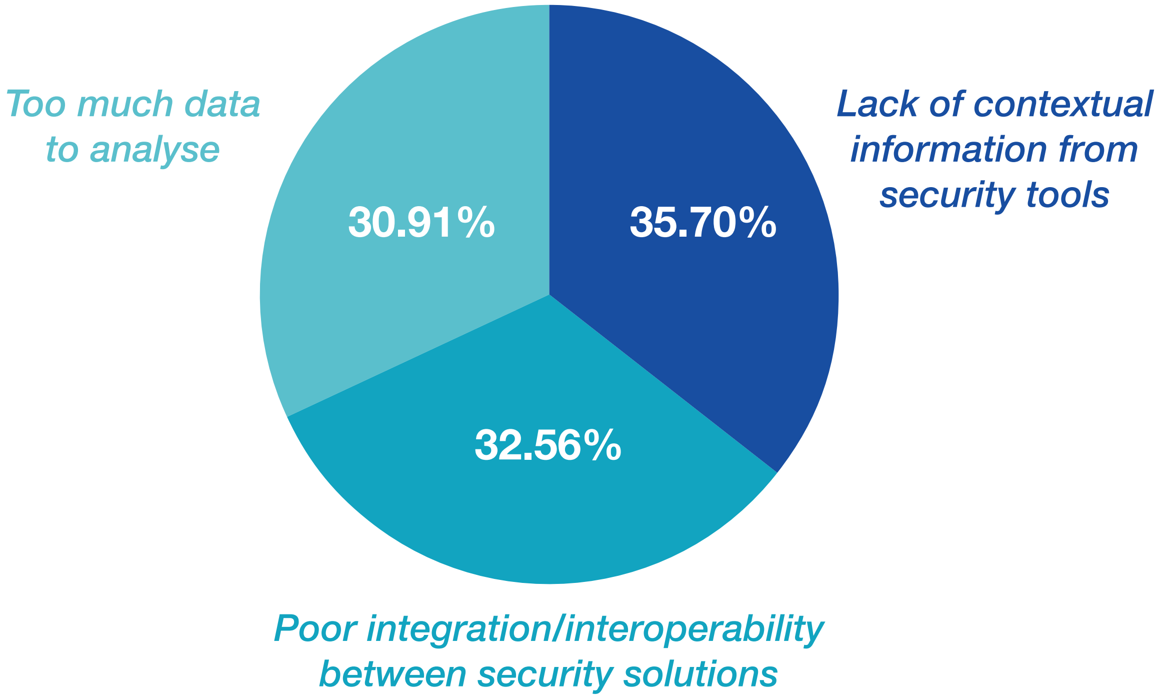
01 Establish a view of your external attack surface

The first step to gaining true visibility over your organisation’s cybersecurity estate is transforming the unknown into the known, by identifying what your attack surface looks like to an external threat actor. Only by looking from the outside in will you be able to establish a clear understanding of where the gaps are in your security estate and which areas are most likely to be exploited by an attacker.

However, this cannot be treated as an isolated exercise. Every organisation’s external attack surface is in constant flux. Changing users, devices, IT assets and digital infrastructure mean the external attack surface – and associated security risk – is constantly growing and changing. Older vulnerabilities remain unpatched, while new ones are continually added. This challenge is compounded by the unpredictability of the modern corporate network. While traditional attack surfaces centred on a single physical location, the work from anywhere trend has extended this on a global scale. The attack surface has become significantly more complex to both define and defend and this makes it one of the most important, and challenging, areas to establish true visibility.

Complete discovery, classification, and assessment of every aspect of the organisation’s fluctuating external attack surface must be organic – indeed automated - to be effective in the long term. After all, it is the ‘unknown unknowns’ that present the greatest threat to the organisation. Many security teams do not know where all their organisation’s assets are and it’s virtually impossible to look for something you don’t know is there. Indeed, as stated above, more than half (57%) of UK CISOs do not know where all their organisation’s data is and how it is protected - however, many have also lost track of corporate devices and left legacy systems unmonitored.

What barriers mostly inhibit your organisation from adequately defending against cyber threats?



A less obvious, but equally important aspect of the external attack surface is the organisation's wider supply chain environment. Third-party vendor environments are fast becoming a key target for sophisticated threat actors searching for a back door. The high profile SolarWinds supply chain intrusion attack demonstrated on a massive scale the risk potential for compromised supply chains. External attack surface management is a critical tool in establishing visibility into the extended supply chain IT ecosystem.

Gaining visibility into your external attack surface will uncover the mass of shadow IT that plagues virtually every organisation. These unmanaged – and in most cases unknown – assets will be the obvious entry point for an external threat actor. The attack surface management process is the first step in uncovering these issues before they are exploited.

02 Conduct robust internal testing

Once you have a continuous, automated process for the discovery of the organisation's systems and assets, the next step in the visibility journey is to start actively testing and validating. The aim of this process is to establish key strengths and weaknesses in the attack surface. Take the analogy of a house. It's not enough to simply establish how many doors there are and where they're located – security testing only begins by pushing each door to see if it opens and how far you can get in.

As with external attack surface discovery, an effective and sustainable internal testing and validation process must be continuous and automated, yet there is a clear lack of comprehensive validation across organisations in the 2023 CISO Survey data, with just 42% of CISOs continuously testing their organisation's security stack.

Point-in-time penetration testing can achieve good results, but the changing nature of the attack surface requires consistent testing and retesting. Automated security validation (ASV) provides just this - continuous testing and validation across the entire attack surface, both internal and external, emulating genuine tactics, techniques, and procedures (TTPs) that will be deployed against the organisation by malicious threat actors.

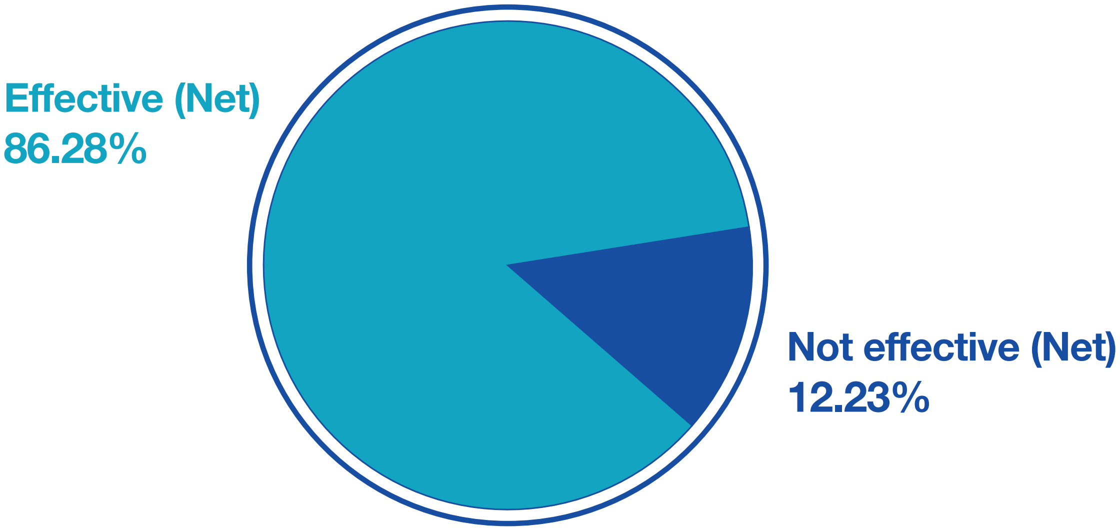
The effect ASV has on solving many of the roadblocks facing security teams in gaining visibility – from information and alert overload to persistent skills gap - is best described by the Pareto Principle of outcomes. This states that 80% of outcomes are the result of 20% of causes. The visibility ASV provides into risk and security exposure is extremely accurate, focusing first on prioritising and remediating the most likely weaknesses to be breached, in real time, as they are created. This process enables security teams to focus on the 5% of weaknesses that constitute 95% of the risk to the organisation.

03 Address and test critical cloud security issues

The widespread move to the cloud represents a fundamental shift in how IT and security teams need to approach visibility. Despite this, many security teams are still struggling to establish visibility and control in the new cloud era. The 2022 CISO Survey revealed cloud as a huge gap in where CISOs have been focusing validation efforts for their security stack, with just over half (53%) using cloud security posture testing.

Cloud security posture management is crucial for any organisation operating in one or several cloud environments – automating security and compliance validation across any cloud environment, from AWS, Azure, and Google Cloud to Kubernetes. The process identifies, prioritises, and remediates risks and provides complete coverage across vulnerabilities, malware, misconfigurations, lateral movement risks, weak and leaked passwords, and overly permissive identities. As with internal testing, the process provides clear visibility, rather than creating additional noise. Vulnerabilities are prioritised based on risk across the entire cloud environment and provided via a complete visual map of the organisation's cloud assets.

How effective, if at all, are your context aware security solutions?



With security misconfiguration cited as the number one cyber security threat experienced by CISOs over the last 12 months, neglecting cloud security issues presents a real and present danger to organisations. Cloud environments are becoming increasingly complex, so establishing true visibility in this area is a critical foundation to long-term security.

04 Assure identity across the organisation

Managing identities – including users, devices, and entities – is the cornerstone to securing an organisation's IT environment, preventing intrusions and maintaining compliance. However, this area is one of the biggest areas for concern in the post-pandemic business environment. The 2022 CISO Survey highlighted a plethora of identity challenges facing UK security teams. Many have lost track of movers, leavers and joiners, lost corporate devices and experienced significant increases in dormant email accounts. The dispersed workforce means the challenge of assuring identity across the organisation is becoming harder. Identities, whether users or devices have fast become the new perimeter.

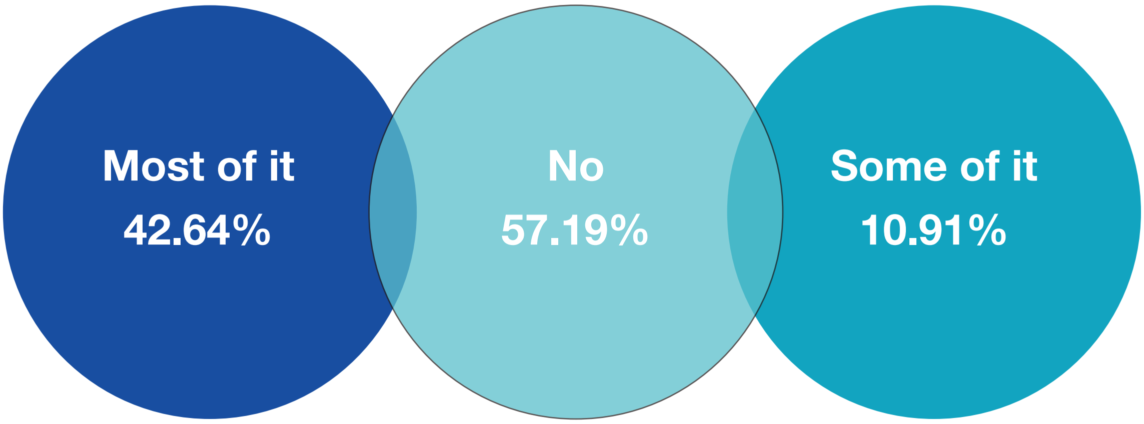
There has been significant innovation in identity and access management in recent years, harnessing machine learning, biometrics and automation. However, through the plethora of systems and tools available to security teams the objective remains simple – establish visibility and assurance of identity. Doing so via assurance tools such as single sign-on (SSO), privileged access management (PAM) and multi-factor authentication (MFA) strengthens perimeter defences and limits the potential for account compromise or credential hacking.

Assuring identity involves a comprehensive assessment of the IT environment and a combination of tools, technologies and services designed to centralise controls, simplify management and increase the granularity of access permissions. Crucially, this must be executed in a way that maintains and improves user experience. The goal is to make it harder for malicious actors to compromise the network while making processes quick and simple for legitimate users.

05 Move from intelligence-led visibility to control

The next – and arguably most important – step is linking all these aspects together. Only then can effective controls be put in place to mitigate the dynamic nature of the cybersecurity risks facing modern businesses. Visibility is an ongoing journey; no single tool, technology or process will deliver complete point-in-time visibility over this changing and often unpredictable IT security landscape. Any set of processes and solutions must be tailored to the specific needs and structure of the organisation. Even the tools and technologies available to better protect organisations from cybersecurity threats are constantly evolving.

Do you know where all your organisation's data is and how it is protected?



This framework offers a clear pathway to IT estate visibility but this is only the start of the journey. Visibility leads to intelligence, which leads to control. Only by covering the basics will it be possible to gain the actionable intelligence necessary to introduce effective controls.

Key questions to ask yourself today

- > *Are you confident you have visibility of your entire external attack surface?*

- > *Can you accurately discover and prioritise your cyber risk based on the level of threat posed to your organisation?*

- > *Are you certain you have visibility of all cloud assets, workloads and their associated policies?*

- > *Do you have a good understanding of where all your assets are and their status?*

- > *Can you continuously and autonomously test assets and infrastructure to discover vulnerabilities and misconfigurations?*

- > *Can you account for all joiners, movers & leavers and ensure the correct provisioning / de-provisioning of services?*

- > *Do you know where all your Intellectual Property (IP) and Personal Identifiable Information (PII) data is and that it is properly protected?*

If you have answered 'no' or are unsure of your answers to any of the above questions, contact BlueFort for an initial conversation and an assessment of your environment: info@bluefort.com

BlueFort Security

BlueFort Security is the UK's leading provider of cybersecurity solutions. For more than 16 years, BlueFort's team of highly skilled experts have been at the heart of cybersecurity technology. From helping executive teams set strategies that deliver effective security, to working closely with analysts and incident response teams fighting cyber criminals on the frontline, BlueFort stands shoulder to shoulder with its customers to understand and manage cyber security risks. BlueFort helps organisations run their enterprise with confidence.

BlueFort ensures that its customers have a complete view of their digital assets, the contextual awareness to understand the threats to them and the necessary controls to secure them from loss or harm.

www.bluefort.com | info@bluefort.com