How can you **transform IT security** if you don't know what you're securing?

Why complete visibility of your attack surface should underpin your security transformation

SKYBOX™ SECURITY

YOU CAN'T SECURE WHAT YOU CAN'T SEE

Skybox offers the kind of common sense structure and approach needed to understand your attack surface, achieve immediate results early in your security transformation, and create a trusted platform on which to mature and evolve your processes over time.

High profile cybersecurity attacks such as the WannaCry ransomware and NotPetya outbreak have focused the minds of many senior executives on the security of their organisations' networks, and how to **reduce the risks** of future attacks. As visible as these threats are though, they're just one of the many reasons why your organisation may be considering or engaged in a security transformation program tasked with reducing risk. For example, it might be that:

- You've appointed a new chief information security officer (CISO) who's identified an underinvestment in cybersecurity and wants to implement a fast track program aimed at delivering immediate improvements.
- You've deployed many different security technologies and are conducting regular audits, but you're struggling to continue to scale your IT security team, which in some organisations can grow to hundreds or even thousands of people.
- You've taken a highly tool-centric approach to cybersecurity, possibly including a security operations centre (SOC). But you have too much data, not enough people to manage it, your processes aren't sufficiently mature, or your operational approach to IT security simply isn't working for you.
- You've tried outsourcing your security, but this isn't delivering the anticipated benefits, because you've outsourced responsibility but not accountability; not enough thought has gone into the processes sitting between you and the outsourcer; or knowledge of your infrastructure is insufficient for the outsourcer's 'one size fits all' approach to be effective.
- You're finding it increasingly difficult to answer questions from senior executives such as where are we most at risk from an attack, what's being done, and what options do we have to prevent this?

Whatever your reasons, a common thread across all these issues is the search for an improved approach and processes to help you better utilise the resources including people, tools and infrastructure you already have. But if you don't know precisely what you're trying to defend, it's very difficult to plan an effective security strategy to achieve this. And without a central model, and a clear and detailed view of your infrastructure, the likelihood is that the technologies and processes you're trying to deploy are going to be very badly instituted or simply not work at all.

By comparison, Skybox offers the kind of **common sense structure** and approach needed to understand your attack surface, achieve immediate results early in your security transformation, and create **a trusted platform** on which to mature and evolve your processes over time.

To show how this works in practice, this short whitepaper summarises the key security challenges that Skybox can help you address. These include:

What do you need?

An improved approach to help you utilize your existing resources and infrastructure, more efficiently.

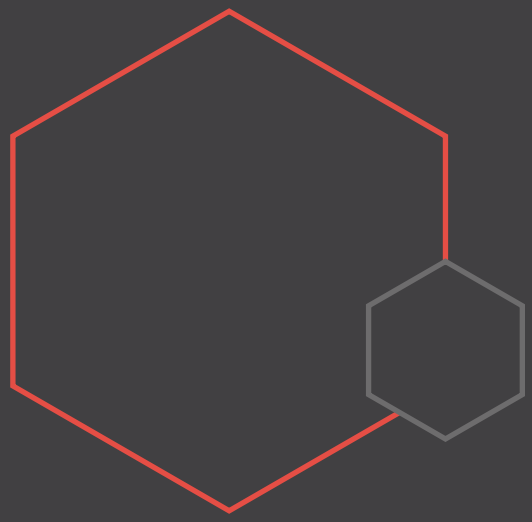
1. How it enables you to understand the context of your infrastructure and the threats and vulnerabilities to which it is exposed.

2. Helps you avoid the pitfalls of investing in a highly technology-centric solution.

3. Lets you identify immediate opportunities to reduce risk and increase resilience.

4. Delivers strategic benefits by being embedded within — and driving ongoing improvements to — your security processes over time.

THE CHALLENGES OF SECURITY TRANSFORMATION



Very poor context of the organisation's attack surface

When organisations start to invest in or want to reset their approach to cybersecurity, they often have a very poor context and understanding of their infrastructure and attack surface, due to its complexity, scale, heterogeneous technology, and use of cloud, outsourcers, etc. Their historical data is also often out of date, including network diagrams that may never have been correct, and audit data that is no longer current the moment the auditors have left the building. And typically, the perimeter simply is not known. Organisations do not know all their ingress and egress points, and so have multiple open paths into the environment — such as unsecured network connections, third parties with risky network access, exposed and high risk vulnerabilities etc. — which make building an effective defence strategy almost impossible.

The need to demonstrate a quick risk reduction

When an organisation decides to take a more concerted approach to security, the person responsible needs to demonstrate value back into the business very quickly. In particular they need to show that the steps they've taken will actually reduce risk and increase resilience. But to do that they first need to identify any gaps in compliance and exposure; their high risk vulnerabilities, and all ingress and egress points; and use this knowledge to prioritise these 'quick wins'.

Improving security and compliance by leveraging existing processes

While some organisations have invested in a SOC, many of these have so far failed to deliver the results expected due to the kinds of issues outlined in the introduction. The alternative is to build on the organisation's existing processes, which in turn creates its own challenges. These include how to turn their firewall change process into a first line of defence, ensure their patch process is serving the security needs of the business, embed compliance management within normal day-to-day operations, and improve existing processes without additional investment in resources.

Using security transformation to deliver increased business value

Many CISOs are under pressure to elevate their security operations team from functioning as a blocker to a strategic business enabler. They therefore want security transformation to add value and increase ROI, for example by using their existing technology more effectively, reducing costs and risks, and increasing automation, but also by improving a broader set of operational processes. In particular they're looking to act as an enabler of business agility, strategy and initiatives in areas such as cloud, digital transformation and resilience, de-risking outsourced environments, automating audits and compliance, security process maturity, SCADA, mergers and acquisitions, divestments etc.

How best to plan and manage the transformation program

The complexity of IT security means implementing change is itself a major challenge. What steps are going to be taken over a two- or three-year period to gradually mature the organisation's approach to security, and align these steps with its appetite to invest? How can this be given a strong foundation? At what point should a SOC or managed security service provider (MSSP) be introduced, and how can this investment be maximised? And crucially, how can the organisation avoid the mistakes made by early adopters who over-invested in technology?

SKYBOX'S PHASED MATURITY APPROACH

Skybox's three-stage Phased Maturity approach enables you to effectively deal with all these major challenges and more.

1

Resilience assessment

The first phase starts with a **resilience assessment** focusing on discovery and high-risk threat mitigation:

- Skybox will build a model of your complete organisational infrastructure, and provide context around all of the ingress/egress points and complexities of your network and assets, to give you a detailed understanding of what you're trying to defend.
- This model will be automatically updated on a daily basis, giving you an ongoing and always current view of your attack surface.

The model can then be regularly analysed to identify all of the opportunities to quickly reduce risk, increase resilience and deliver immediate results:

- After building the model of your environment, Skybox will conduct a risk analysis to identify weaknesses and vulnerabilities such as unprotected ingress/egress points, misconfigured network devices, firewalls with overly permissive rules, exposed assets, exploitable attack vectors etc.
- Following the initial resilience assessment, the riskiest characteristics of the environment can be remediated to reduce risk quickly and in a demonstrable way – for example by addressing parts of the infrastructure for which there are no firewalls or where these are configured incorrectly; vulnerability scanning blind spots; and high-risk vulnerabilities.
- Through this process your environment will immediately be more secure and resilient. But if there is an attack or outbreak of malware within the infrastructure, you'll also be much better prepared to respond quickly and effectively, and with greater context.

2

Standard process evolution

The second phase focuses on **evolving and improving your existing processes**, or instituting new ones in areas including compliance and policy management, firewall and change management, and vulnerability management. This includes:

- Automating and aligning audit processes, compliance and policy management across the network, including tracking exceptions and fixing any potential violations.
- Improving firewall change management from what is often a complex, manual, error-prone and operationally driven process, to one that is consistent and includes due consideration of risk. This involves automating the process, making it quicker and more secure, and embedding compliance within it. The result is a mature change process that is the organisation's front line of defence, rather than the weakest link in its approach to security.
- Improving vulnerability management, by bringing objectivity and consistency to the patching process, and allowing the organisation to manage vulnerabilities more effectively. This includes creating a better understanding of risk and the options available to mitigate it; improving communication with the relevant operational teams responsible for patch deployment; and providing a constantly updated view of where the high risks are so the teams know what they need to be fixing.

Doing this will also allow you to better understand where additional controls and re-architecture can be introduced to **increase resilience** on an ongoing basis, and provide the bedrock on which to establish more mature security operations, such as advanced SOC.

Advanced capability

The third phase is then about moving into more **advanced use cases** such as embedding Skybox into a SOC or computer emergency response team (CERT), using it to assist with outsourcing to a MSSP, or some kind of hybrid model.

As there's little point in outsourcing device management or monitoring until you have a clear view of what you're trying to defend, this could, for example, include the introduction of a weekly process based on **Skybox Attack Path Analysis**. This can be used to assess exposure, identify weaknesses within your infrastructure, and target and fix these proactively, with the results providing context for the MSSP in terms of what they should be looking for with the monitoring toolsets being deployed. This in turn can help address common issues with MSSPs, such as security information and event management (SIEM) monitoring services that fail to spot suspicious activity, and/or produce high volumes of false positives and other alerts.

Advanced SOC

If you're considering or have implemented a SOC, many organisations report that this can create significant challenges. Examples include too many unintegrated tools, resulting in too many alerts that they struggle to know where to look to fix, constant firefighting, and no way of assessing which alerts are most important. Also, when they do come across a major vulnerability, they take too long to react, because they don't have the context of the infrastructure needed to make quick decisions about how to block exfiltration of data, how to contain the attack, and how to stop it moving to other parts of their environment.

In addition to **threat monitoring**, what's therefore needed is **tighter integration** of security technologies, but also the more mature processes and workflows required to support proactive rather than reactive decision making — precisely what Skybox enables by allowing organisations to understand their exposures and where they're most at risk.

KEY BUSINESS BENEFITS

Skybox will help you deliver superior results from your security transformation

Whether or not you decide to move to this more advanced approach, Skybox will help you optimise your resources and enable key business initiatives by:

- Creating a central model of your organisation's entire infrastructure that can be used to join and de-risk processes across disparate technologies, regardless of how these are managed (e.g. in-house, outsourced, cloud).
- Embedding analytics within your existing processes, automating and reducing organisational overhead, while at the same time improving your security posture and resilience.
- Automating many important processes such as audit, change management, vulnerability management and security operations.
- Providing context to security monitoring tools and within incident response processes, thereby allowing a reduction in resource.
- Enabling business initiatives such as cloud adoption, digital transformation, mergers and acquisitions, divestments, outsourcing, insourcing and compliance.

To summarise, Skybox will help you deliver superior results from your security transformation by enabling you to:

- Identify and act on opportunities for quick risk reduction, and demonstrate the results to key stakeholders.
- Have visibility of your entire attack surface, right from the start of the program.
- Quickly generate ROI from your existing security tools and processes.
- Plan your security transformation in a structured and logical way.
- Automate, evolve and streamline critical processes — including maintaining compliance as part of the process.
- Increase resilience and de-risk further investments in security processes and technology.
- Reduce resource requirements compared to alternative technology-driven approaches.
- Take a more proactive approach towards security and improving and maintaining cyber hygiene.
- Use the Skybox model and process improvements to enable and add value to key strategic business initiatives.

WHERE TO START?

Skybox arms security leaders with a powerful set of integrated security management solutions that give unprecedented visibility of the attack surface and key indicators of exposure (IOEs), such as exposed vulnerabilities or with active or available exploits, unsecure device configurations and risky access rules.

By extracting actionable intelligence from data using modelling, simulation and analytics, Skybox gives leaders the insight needed to quickly make decisions about how best to **address threat exposures** that put their organisation at risk, increasing operational efficiency by as much as 90 percent. Skybox's award-winning solutions are used by the world's most security-conscious enterprises and government agencies for vulnerability management, threat intelligence management and security policy management, including Forbes Global 2000 enterprises.

To find out more about how Skybox can form the bedrock for your security transformation, please visit our **website**.

SKYBOX™ SECURITY