Product Brief

Vulnerability Control

Build a mature vulnerability program and zero in on what matters

The modern cybersecurity battlefield is fraught with many landmines. While companies accelerate cloud adoption and secure a newly distributed workforce, the volume and complexity of vulnerabilities have also increased. Capitalizing on these changes, attackers have successfully staged more sophisticated attacks.

The attack surface has also become more complex. In 2020, OT vulnerabilities increased by 30% while correspondingly, IIOT vulnerabilities jumped by over 300%. To gain control, organizations must:

+ Visualize their entire attack surface across IT/OT, datacenter, campus and cloud environments
+ Understand which vulnerabilities are exposed and susceptible to immediate and imminent attack
+ Utilize a combination of scan-less and scanning technology to ensure full coverage of the environment, while minimizing business disruption
+ Relentlessly and consistently capture and update vulnerability repositories for an accurate view of their risk posture.

With Skybox Vulnerability Control, you can get the full context of your attack surface across the network, cloud and security infrastructure. You can find where you are exposed to cyber-attacks, quantify the risks of exploitation, prioritize vulnerabilities and provide optimal remediation options to reduce the highest levels of risk.

“We can drive operations to mitigate only the most critical vulnerabilities — the ones that require immediate attention. It’s vitally important that the agency be able to view risk from an operational and business perspective, and we needed to know if low or medium vulnerabilities were actually creating more risk than the agency had intended to accept.”

— Program manager, USAID ISSO team

1Vulnerability and Threat Report, Skybox Security, February 2021
Why is a network model important?

A scalable and accurate network model crystallizes and produces actionable insight, reduces manual effort, and produces quick time to value when prioritizing and remediating critical vulnerabilities.

Think differently about vulnerability management

While scanners are an integral part of strong vulnerability program, scanner deployments typically provide partial and infrequent coverage of the organization’s entire threat landscape, including IT, OT and cloud. Additionally, traditional methods of prioritizing vulnerabilities for patching over time fail to provide immediate remediation. Alternative methods to sealing off and resolving high risk vulnerabilities must be considered.

The Skybox Vulnerability and Threat Management solution includes Vulnerability Control and daily feeds from Skybox Threat Intelligence. Collectively these products discover and prioritize vulnerabilities on devices that cannot be scanned, while minimizing business disruption.

Skybox Vulnerability and Threat Management

An intelligent approach to full-lifecycle vulnerability threat management

See everything in a single dashboard

Skybox Vulnerability Control collects, aggregated and normalize data from your existing security and network infrastructure tools. This data provides the foundation for a robust network model that enables real-time visibility into high risk vulnerabilities and imminent threats on your network.

Single source of vulnerability truth

Vulnerability Control integrates with over 150 leading network, security, asset management, SIEM, Service Management and other tools. It collects vulnerability data across campus, datacenter, cloud, IT and OT environments, breaking down information silos and producing a single source of truth.

While an attack is occurring, a single vulnerability dashboard is vital to see all systems involved in a coordinated attack, and to modify access rules to reduce the blast radius. Skybox Vulnerability Control gives you that enterprise-wide view of the attack surface, increasing visibility and optimizing reaction time.
Act on what matters

By combining daily threat intelligence feeds with the rich context acquired from across your corporate security stack, Skybox Vulnerability Control builds a unique risk score that highlights critical vulnerabilities on assets are of high importance. Furthermore, it places a higher priority on those critical vulnerabilities that are exploited in the wild and are exposed to threat actors, whether internal or external.
**Using intelligence and context to drive remediation decisions**

Many mission critical devices cannot be taken offline to be patched. A thorough model of the network will intuitively recognize pathways to and from the vulnerable asset and can recommend access modifications to cordon off and protect the device.

**Fix and confirm**

Skybox Vulnerability control integrates with leading ticketing systems to orchestrate and validate remediation of high priority vulnerabilities. For example, security teams can raise a ticket that sends an alert to ServiceNow. The ticket appears in the dashboard and the status of the ticket can be monitored and reported on until the remediation is complete.

Intelligent trend widgets help to track remediation success over time, thus providing insight into change management procedures that can be optimized to further improve remediation time.

**Think outside the box for remediation success**

How do you know how well you’re doing? Are your key remediation metrics improving? Are your SLAs being met? A vulnerability and threat management solution can provide you with instant visibility into your entire vulnerability realm and keep teams accountable for meeting and exceeding SLAs. However, this also requires strategic planning with a team that has the expertise to take you through the entire journey.

Skybox Professional Services uses deep subject-matter expertise and a proven, flexible deployment methodology so you can gain immediate value from your deployments and embed the solution in ongoing security processes. With over 20 years of experience with large and complex networks, our team quickly learns your environment, designs and customizes your view of the product to quickly meet your needs.
Audit and oversight

As you adopt a mature vulnerability management program, it will be critical to consistently validate and refine the data aggregation processes that build and maintain the corporate network model. Accurate reporting and an understanding of trends over time will improve the predictability that is vital to successfully preventing attacks.

The Skybox Vulnerability Control dashboard reports on trends over time and emphasizes downward trends that could negatively impact risk scores such as:

+ Decrease in scan frequency
+ Decrease in the number of machines scanned
+ Increase in high-risk vulnerabilities or exposed vulnerabilities

The Skybox® Research Lab is a team of security analysts who scour data daily from dozens of security feeds and sources and investigate sites on the dark web. The research lab validates and enhances data through analysis, based on their knowledge of attack trends, cyber events, and the TTP of today’s attackers. Their ongoing investigations determine which vulnerabilities are being exploited in the wild and used in distributed crimeware, such as ransomware, malware, exploit kits, and other attacks exploiting client and server-side vulnerabilities. This analysis is incorporated into Skybox Vulnerability and Threat Management solution, which prioritizes the remediation of exposed and actively exploited vulnerabilities.