Product Brief

Threat Intelligence Service

Identify vulnerabilities and mitigate potential exploits within your hybrid networks

Challenges

To deploy limited resources in the right places and the right ways, firewall and network security teams need a complete picture of their vulnerabilities, along with appropriate context from their networks and the overall threat landscape. Without threat intelligence at their fingertips, teams can find themselves overwhelmed with too many data feeds and not enough actionable data to accomplish their goals of improving security posture.

Solution

The Skybox Threat Intelligence Service is an essential component of the Skybox Vulnerability Control (VC) module, and also enhances the Skybox Security Policy Management (SPM) modules by adding vulnerability insights. It enables an organization to correlate vulnerabilities in their environment with the latest threat intelligence from Skybox security analysts. Skybox Threat Intelligence is included with VC. Customers with SPM can add the Threat Intelligence service with a yearly subscription in addition to Skybox SPM module licensing and support costs. Intelligence data is updated daily based on an aggregation of dozens of public and private security sources. Network and security teams can leverage the Threat Intelligence Service to pre-emptively identify vulnerabilities in firewalls and network infrastructure devices that could pose a significant business risk.

Capabilities

- **Get automatically aggregated threat data from multiple sources, including:**
  - National Vulnerability Database (NVD)
  - Published vulnerability repositories
  - Vulnerability scanners
  - Threat intelligence feeds and platforms
  - Vendor IPS signature feeds (Cisco, Fortinet, HP, McAfee, Palo Alto Networks)
- **Identify vulnerabilities in standard operating systems, browsers, software, and databases**
- **Integrate intelligence data with network security operations without scanning**
- **Correlate vulnerabilities in the environment with those being actively exploited in the wild**
- **Model how network changes could impact security or compliance**

Identify, detect and remediate vulnerabilities

Detect firewall vulnerabilities

With Skybox Threat Intelligence, firewall admins gain visibility into vulnerabilities, including a list of vulnerabilities per firewall device along with severity and mitigation options. Administrators can act quickly to remediate firewall vulnerabilities and mitigate potential breaches.

Detect network device vulnerabilities

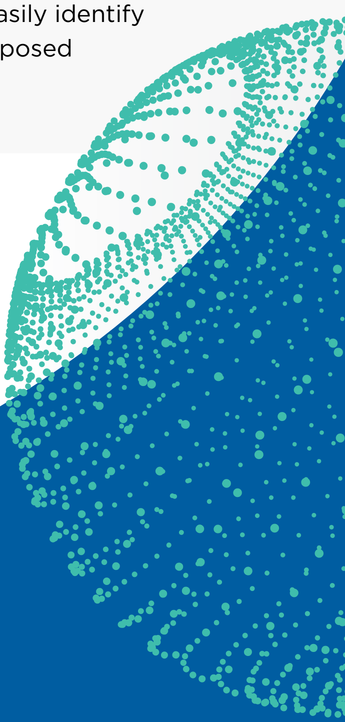
Skybox Threat Intelligence provides network administrators with visibility into network device vulnerabilities in traditional, hybrid, and cloud networks. Administrators can see a list of vulnerabilities per queried access path along with severity. They can mitigate attacks that use lateral movement by analyzing the path from the point of egress to the organization network or from a network within the environment.

Assess the risk of network changes

Skybox Threat Intelligence provides network security operations teams with increased visibility and understanding of how network changes impact security. With aggregated vulnerability data at their fingertips, administrators can more easily identify potential vulnerabilities based on proposed network changes.

Contact an expert

Schedule a demo ⋯>



ABOUT SKYBOX SECURITY

Over 500 of the largest and most security-conscious enterprises in the world rely on Skybox for the insights and assurance required to stay ahead of their dynamically changing attack surface. Our Security Posture Management Platform delivers complete visibility, analytics and automation to quickly map, prioritize and remediate vulnerabilities across your organization.