You Can’t Secure What You Can’t See
Visibility in Cloud Networks

Tony Turner, Director of Professional Services Delivery
Skybox Security
Challenges

**Visibility is the starting point.**

**Understanding Risk**
Obtaining accurate visibility of cloud networks and understanding overall business risk.

**Increased Complexity**
How to maintain business resilience of an increasingly complex and fluid environment.

**Shared Responsibility**
Understanding and managing the shared responsibility for security with CSP.

**Processes**
Extending existing operational and security processes to seamlessly include cloud environments at a low cost.

**Secure Transition**
Transitioning infrastructure and services into the cloud — securely and quickly to enable CIO strategy.

**Compliance & Privacy**
Visibility to ensure CSP and/or internal teams are meeting obligations around segregation of data, controls, privacy and compliance.
Modeling the Attack Surface
• “Collection Task” via API
• Pulls details of all elements
• Normalizes the data
• Display in the Skybox model
Skybox Visualization of AWS Environment
Inventory Devices
Continuous Vulnerability Assessment and Remediation
Malware Defenses
Limitation and Control of Network Ports, Protocols and Services
Secure Configuration for Network Devices
Boundary Defense
Controlled Access
Application Software Security
Pen Testing

CSC 19: Incident Response and Disruption Management
CSC 20: Penetration Tests and Red Team Exercises
CSC 21: Inventory of Authorized and Unauthorized Devices
CSC 22: Inventory of Authorized and Unauthorized Software
CSC 23: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
CSC 24: Data Recovery Capability

CSC 18: Application Software Security
CSC 17: Security Skills Assessment and Appropriate Training to TIE Gaps
CSC 16: Account Monitoring and Control
CSC 15: Wireless Access Control
CSC 14: Controlled Access Based on the Need to Know

CSC 13: Data Protection
CSC 12: Boundary Defense
CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
CSC 10: Malware Defenses
CSC 9: Limitation and Control of Network Ports, Protocols, and Services
CSC 8: Malware Defenses
CSC 7: Email and Web Browser Protections
CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs
CSC 5: Controlled Use of Administrative Privileges
CSC 4: Continuous Vulnerability Assessment and Remediation
CSC 3: Critical Security Controls
Applying Visibility and Intelligence

Security Policy Management

Vulnerability/Threat Management

Attack Surface Management

Rule Life Cycle Management

Risk Reduction Tracking

Change Management

Remediation

Policy Compliance

Analysis/Prioritization

Optimization/Cleanup

Discovery
Example 1: Impact of Visibility

Understanding Access
End-to-End Path Analysis

Quickly assess connectivity + info on path

• Network and application connectivity shown across on-prem and multi-cloud environments

• Ad hoc queries showing connectivity for applications
  o Between any source and destination

• Detailed path analysis on the devices, access rules, etc. along the path
Access Path Analysis Queries
Access Path Analysis Result = Blocked

<table>
<thead>
<tr>
<th>Security Tag</th>
<th>#</th>
<th>Original Rule ID</th>
<th>Source</th>
<th>Users</th>
<th>Destination</th>
<th>Sources</th>
<th>Rule AY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dev_BE_Servers</td>
<td>1</td>
<td>10.4.10.0/24</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>PostgreSQL</td>
<td>Any</td>
</tr>
<tr>
<td>Dev_BE_Servers</td>
<td>2</td>
<td>10.4.10.0/24</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>SSH</td>
<td>Any</td>
</tr>
<tr>
<td>Dev_BE_Servers</td>
<td>3</td>
<td>10.4.10.0/24</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>MySQLaur...</td>
<td>Any</td>
</tr>
<tr>
<td>Dev_BE_Servers</td>
<td>4</td>
<td>10.4.10.0/24</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>All-ICMP</td>
<td>Any</td>
</tr>
<tr>
<td>Dev_BE_Servers</td>
<td>5</td>
<td>10.4.10.0/24</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>DNS-UDP</td>
<td>Any</td>
</tr>
<tr>
<td>Dev_BE_Servers</td>
<td>6</td>
<td>10.4.10.0/24</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>All-ICMP</td>
<td>Any</td>
</tr>
<tr>
<td>deny Implicit_inbound</td>
<td>7</td>
<td>10.4.10.0/24</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td>deny Implicit_outbound</td>
<td>8</td>
<td>10.4.10.0/24</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
</tr>
</tbody>
</table>

Security Group and Associated Tags

AWS-DEV
Example 2: Impact of Visibility

Vulnerability Management
Vulnerability and Threat Management

Discovery, prioritization and remediation

• Show all vulnerabilities and exposures — physical, virtual and cloud

• The most complete discovery of vulnerabilities
  o Integration with cloud-approved vulnerability scanners
  o Scanless vulnerability discovery and assessment

• Threat-centric vulnerability prioritization
  o Correlates vulnerabilities in your environment to those that are being targeted by cybercriminals
  o Enables prioritization with context of your network and business
Challenges of Scanning Only Approach

- CSPs limit scanning
- Require network-based scanners have a user account on target virtual machines
- Customers lack ability to centrally manage such accounts
Vulnerability Detector

ASSET/PATCH MGMT.
SCCM, Altiris, Satellite, EPO

ACTIVE SCANNER
Qualys, Rapid7, Tenable, McAfee

NETWORKING DEVICE
Cisco, Juniper, Check Point, HP

PRODUCT PROFILING

SKYBOX VULNERABILITY DATABASE

VULNERABILITY DETECTOR TASKS

PRODUCT CATALOG (CPE)
OS version and patch level, application version

VULNERABILITY OCCURRENCE LIST (CVEs)
Remediation and Oversight

- Remediation – Imminent Threats First
  - Apply patches
  - Or Block paths
    - IPS signatures, access rules, segmentation, etc. to block paths

- Track Progress
  - Analyze trends – where are more resources needed?
  - Monitor remaining vulnerabilities
    - Changes in exposure
    - Change in threat landscape – have vulnerabilities increased in criticality because of “use in wild?”
Benefits of Visibility

• A single view of exposures across entire attack surface
  • Decrease security risks when transitioning
  • Gain visibility of security controls
  • Understand the security posture of entire network
  • Reduce complexity of new infrastructure
  • Facilitates in extending processes to cloud environments
  • Makes managing security you are responsible for easier
Skybox Security Suite

Integrated Security Management

- Total visibility of the attack surface
  - Physical, virtual and multi-cloud IT networks
  - OT networks
- Built for large, complex networks
- Security Analytics
  - Vulnerability and attack vector intelligence
- Automation of critical security operations workflows
Thanks