Advanced Threat Protection Buyer's Checklist

The checklist below will help you assess your current and proposed security posture with a look at your environment coverage, mix of security technologies and integration capabilities. The end result will provide you with a baseline set of requirements to ultimately ensure the right solution set for your organization.

I. EVALUATE ENVIRONMENT COVERAGE

- ☐ Determine the physical locations you want to cover, such as network ingress/egress/internal points, central email and file systems, mobile endpoints and cloud workloads.
- ☐ Decide which protocols you want to inspect at each of those points (e.g., http, SMTP, SMB and more, including encrypted versions).
- ☐ Assess the capacity that is required (e.g., 1 G, 10 G, 40 G Ports and/or 1 Gbps, 4 Gbps, 10Gbps or more, plus the number of objects per time period).
- ☐ Evaluate or review the most recent independent comparative tests that cover sandbox and related technologies to understand how they performed. Refer to test houses such as NSS Labs, Virus Bulletin, AV Comparatives and ICSA Labs.

These steps will help you properly size the necessary deployment and quickly see past loss leader, feature-limited point products that lead you down an expensive and unsustainable path as well as vendor marketing hype that hides insufficient effectiveness.

II. DETERMINE YOUR MIX OF SECURITY TECHNOLOGIES

- ☐ Understand what analysis techniques are utilized for prevention by location and protocol and ensure you have more advanced techniques in place to block as much as possible (e.g., signatures, heuristics, reputations, emulation and decryption).
- ☐ Learn what analysis techniques are used to provide advanced threat detection by location and protocol, including sandboxing, behavioral analysis and big data analytics.
- ☐ Identify the mitigation processes and tools you have in place to respond to incidents. This may include your response team, outside services, forensic tools and integration, as well as automated response between products.
- ☐ Identify the methods used to assess the effectiveness of your threat prevention, detection and mitigation (e.g., regular penetration tests, tracking production effectiveness, time of purchase PoC and independent test reports).

These steps will help you focus and balance your investment for maximum results across each of the three elements. It is important that you don't overlook ways to prevent more advanced threats before time-consuming detection and response are required. However, overlooking detection and relying solely on prevention is also folly as we have seen these past few years. Likewise, prevention and detection investments without the ability to respond will not effectively reduce your security risk.

III. DEGREE OF SYSTEM-LEVEL OPERATION

- ☐ Identify which prevention components integrate detection elements with each other (e.g., firewall integration across branch, HQ, core, cloud; email and web security, endpoint protection, web application firewall, SIEM, log management and others).
- ☐ Define how advanced threat detection components provide information for response (e.g., dashboards and reports, export data via APIs, established integrations to pass data and automatic signatures).
- ☐ Understand which assisted or automated responses can be taken by in-place components (e.g., quarantine devices, block sources or remove files).
- ☐ Identify how many central intelligence hubs, local threat exchanges and/or global research labs are required.

This will determine the degree to which all of your prevention, detection and mitigation elements, however good on their own, function efficiently and effectively as a cohesive security solution.

Rating the Strength of Advanced Threat Protection

To assess the general strength of your organization's defense against today's sophisticated threats, gauge the number of prevention technologies in place, measures to detect and mitigate advanced threats that may skip through, and integration points between all of these aspects.

A wide range of prevention with few advanced detection or mitigation components leaves organizations exceptionally vulnerable. Even many individual components will still leave gaps. See where you stand today and make informed choices to move toward an integrated system of prevention, detection and mitigation.

PREVENTION COMPONENTS

- ☐ Branch Firewall
- ☐ HQ Firewall
- ☐ Core Firewall
- ☐ Cloud Firewall
- ☐ Secure Email Gateway
- ☐ Secure Web Gateway
- ☐ Web Application Firewall
- ☐ Endpoint Protection
- ☐ Other

DETECTION COMPONENTS

- ☐ Network Behavior
- ☐ Network Forensics
- ☐ Endpoint Behavior
- ☐ Sandbox
- ☐ Big Data
- ☐ Other

RESPONSE COMPONENTS

- ☐ Response Services
- ☐ Endpoint Forensics
- ☐ Automation

INTEGRATION POINTS

- ☐ Firewall and Advanced Threat Detection
- ☐ Secure Email Gateway and Advanced Threat Detection
- ☐ Secure Web Gateway and Advanced Threat Detection
- ☐ Web Application Firewall and Advanced Threat Detection
- ☐ Endpoint Protection and Advanced Threat Detection