HORIZON3.ai

~~TRUST BUT~~ VERIFY

# Defense in Depth

## What's Missing in Layered Defense?

## Layered Assessments.

**Defense in depth is a proven strategy for protecting systems and software from insider and external attacks.** An organization usually starts with perimeter security, keeping malicious actors from accessing systems and monitoring data entering externally facing applications. Primary defenses should also include limiting and managing privileged accounts, endpoint detection and response, and identifying and protecting sensitive data from unauthorized access. More advanced defensive measures likely include log monitoring using a SIEM and security orchestration, automation, and response (SOAR).

## Assessing Security Measures

The effectiveness of these defenses is often measured through penetration tests, or pentests. Pentests can be automated or manual. In the former, tools target specific IP addresses, identify inputs, and "fuzz" data to identify common vulnerabilities like SQL injection and cross site scripting that can be used against the defenders. Alternatively, vulnerability scanners identify unpatched commercial applications and the presence of "known vulnerabilities" in operating systems, databases, and commercial applications.

Manual pentests are more comprehensive and employ skilled ethical hackers using commercial and proprietary tools (and extensive experience) to identify weaknesses an adversary could exploit to gain access to systems and steal data or install ransomware or other malicious applications. In a professional penetration test, "attackers" first perform reconnaissance to understand the system under test, then identify application or device-specific threat vectors. Next, they must devise exploits for any suspected weaknesses.



# Layered Defenses Require Layered Assessments.

No organization has unlimited resources. Assessments of an organization's security posture should match the risks present in the environment. "Layered Assessments" – focusing on attack vectors that pose ongoing risk in a rapidly changing network and application environment – allow organizations to test defenses and adjust quickly when weaknesses are identified. **They leverage automation to frequently assess attack patterns used most frequently by attackers, reserving scarce and more expensive security resources to assess lesser used attack patterns.** Layered Assessments allow organizations to scale assessments across their entire portfolio.

## Challenges

### Traditional pentests, whether automated or manual, present several challenges to organizations:

- **Incomplete** – Automated pentests are limited to the rules employed by the vendor to test a system. Manual pentests can be more complete, but since they are time-based (more time is more complete, but also more expensive) organizations often limit the scope of the tests. To compensate for this, the attackers are often provided credentials to accelerate the tests.
- **Scalability** – As noted, a thorough manual pentest is time based, often costing $30,000 to $50,000 for a test/retest engagement. This limits manual pentests to infrequent assessments, usually once or twice each year.
- **Timeliness** – Manual pentests are measured in weeks. Attackers are always present and evolving their tactics.
- **Remediation** – The results of a pentest provide detail on the vulnerabilities identified. Automated pentest results are notoriously "noisy" – filled with false positives and minimally important findings with little (if any) remediation information. Manual pentests can provide more evidence of how an attacker exploited a weakness. Both, however, represent a point-in-time representation of a system's security.
- **Real Adversaries Seek Minimum Effort** – While nation-state actors have the resources and patience to research zero-day attacks in proprietary applications, today's threat space is largely populated by financially motivated adversaries. They prioritize threat vectors that are simpler to exploit and more likely to succeed. They do not require credentials to begin their attacks and instead look for attack vectors that allow deeper reconnaissance, then chain weaknesses to gain credentials, escalate privileges and execute attacks.

# Prioritizing Layered Assessments

As noted, malicious actors seek to accomplish their goals efficiently. Identifying and exploiting zero day vulnerabilities in externally and internally facing applications requires greater research, skills, and persistence. Identifying and exploiting unpatched systems, known vulnerabilities, and misconfigurations is quicker and simpler. **Layered Assessments should be prioritized to match this risk, as follows:**

1. **Unauthenticated Internal Assessments**
A core tenet of Zero Trust is to assume an attacker can breach your perimeter. This could be through a poorly configured RDP server, open SMB share, or other resource that is not properly secured. Unauthenticated penetration tests can identify these critical "footholds" and quickly improve an organization's security profile.

2. **Unauthenticated External Assessments**
Like Internal Assessments, unauthenticated external pentests close gaps that make an adversary's task easier.

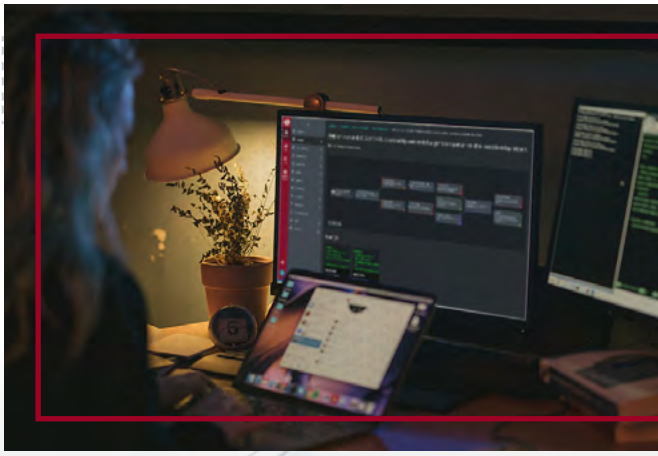
3. **Web Application Penetration Tests**
Identifying Zero days in externally facing applications require significant research by attackers. For most organizations, these present lower risk than unauthenticated weaknesses.

4. **Authenticated Internal Penetration Tests**
While zero day vulnerabilities may exist in internally facing applications, these also require long-term persistent access to systems and significant research by attackers.

**In short, organizations should focus layered assessments on those attack vectors that present the most risk. While zero days do present risk, this is far outweighed by simpler to exploit weaknesses that can be accessed by unauthenticated attackers.**

## NodeZero Enables Continuous, Autonomous Assessments.

Just as organizations layer their defenses, a layered approach to assessments also enables better security. It allows organizations to scale assessments without the cost and time required by manual assessments. It takes minutes – not weeks – to identify attack vectors with proof of exploitability. No false positives.





HORIZON3.ai
~~TRUST BUT~~ VERIFY

# Autonomous Red Teaming

NodeZero is a true self-service SaaS offering that is safe to run in production and requires no persistent or credentialed agents. It assesses systems as would a manual pentester, but faster, more completely, and with more actionable results. By starting with unauthenticated access to a system, NodeZero mimics the approach used by your adversaries.

**Reconnaissance** – The first step in an assessment is to map and catalog the environment. NodeZero starts with unauthenticated access to the system, then creates a Knowledge Graph, identifying all hosts, misconfigurations, open ports, and searches for credentials.

**Maneuver Loop** – NodeZero acts as an Advanced Persistent Threat (APT), orchestrating over 100 offensive tools to harvest credentials, exploit vulnerabilities, and exploit default and misconfigurations to execute attacks.

**Verified Attack Plans** – The results are provided as "Proofs" with graphical and textual representations of each step of a successful attack, including tactics used, how credentials were obtained, paths taken to gain privileges, and access to systems.


**Impact** – Like a determined attacker, NodeZero surfaces data at risk across physical and virtual environments it was able to access with read/write privileges, including SMB shares, NFS shares, FTP shares, cloud storage, vCenter servers, and databases.

**Contextual Scoring** – Instead of relying on CVSS scores, NodeZero evaluates each weakness by its role in the successful attack. Organizations can quickly identify those weaknesses that present the greatest threat and must be addressed immediately, and which can be safely deferred.

**Actionable Remediation** – NodeZero provides precise and actionable remediation guidance, allowing security and operations to resolve issues at the root cause.

## Ready to Learn More?

NodeZero is an Autonomous Penetration Testing as a Service (APTaaS) that helps organizations **find and fix attack vectors before attackers can exploit them**. It is safe to run in production and requires no persistent or credentialed agents.

- **Sign up for your free demo today.**
  https://pages.horizon3.ai/demo



HORIZON3.ai
TRUST BUT VERIFY