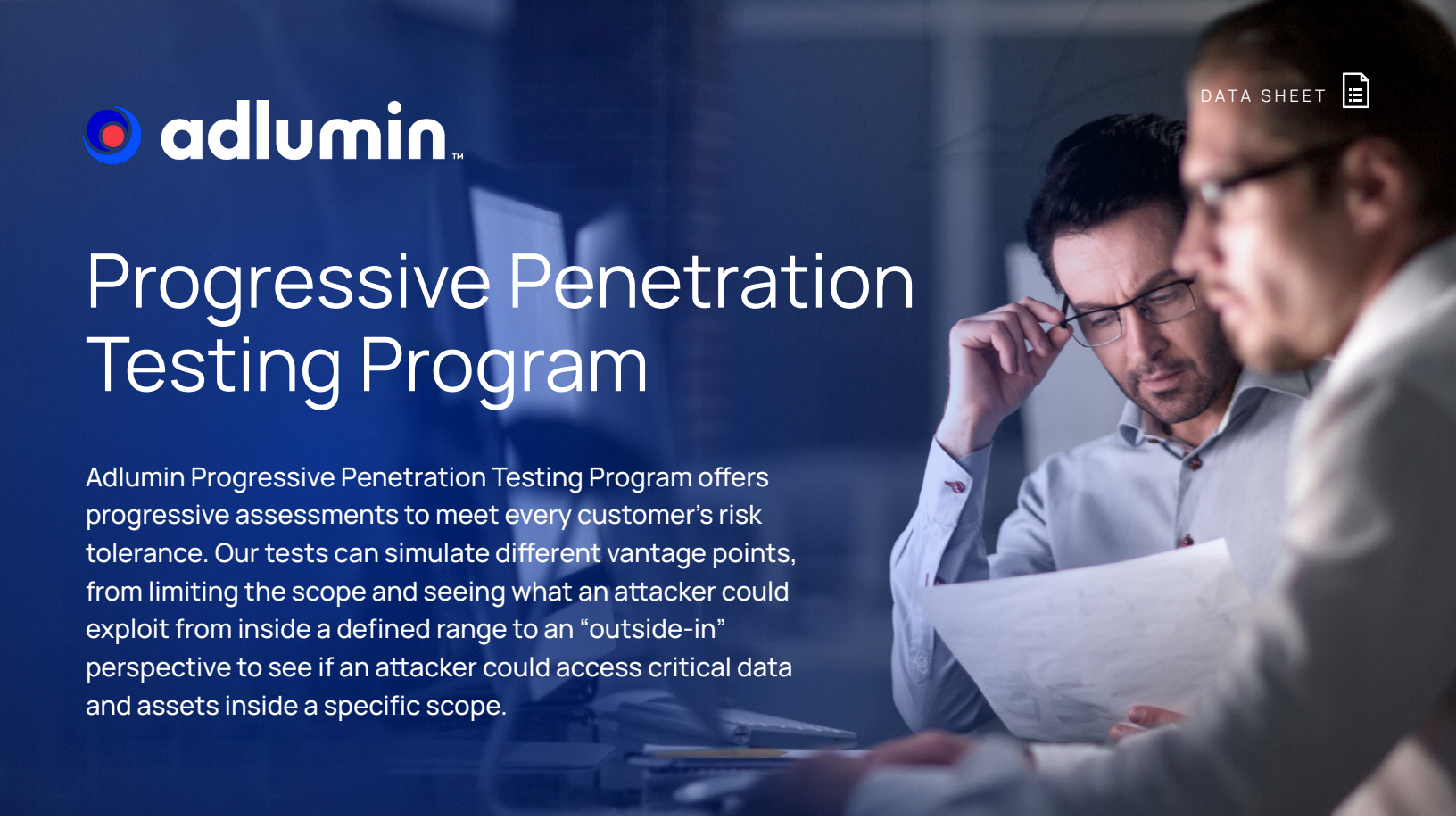
DATA SHEET

Progressive Penetration Testing Program



Adlumin Progressive Penetration Testing Program offers progressive assessments to meet every customer's risk tolerance. Our tests can simulate different vantage points, from limiting the scope and seeing what an attacker could exploit from inside a defined range to an "outside-in" perspective to see if an attacker could access critical data and assets inside a specific scope.

Industrialized criminals use sophisticated tactics, techniques, and procedures (TTP) that exploit vulnerabilities across accounts, remote access points, administrative tools, and core network infrastructure. With limited resources, most organizations struggle to identify these exposures, prioritize vulnerabilities, and align to business objectives that protect and meet the obligations of the management of protected assets.

Many organizations and regulatory frameworks, require annual penetration tests to identify exposures. These tests no longer match the capabilities of cyber adversaries. Annual tests provide a snapshot of an organization's cybersecurity health. New systems and users, patches and application updates, and fluid configuration render the penetration test results irrelevant within in days.

Traditional penetration tests use limited formulaic methodologies testing known-known criminal tactics, and not the evolving threat landscape facing organizations. The cybercrime ecosystem leverages a diverse set of skills and creativity a valuable amount of time and motivation to gain access to an asset. Typical tests stress single points and controls rather than criminals' complex and multi-step exploitation.

Limited scope, high costs, and a short shelf life contribute to the need for a new method to test an organization's defenses.

Adlumin Progressive Penetration Testing Program recognizes that criticality is a function of exploitability and Impact and operates under the thesis that customers in a specific industry segment that continue to use traditional pentest methodologies may be elevating their risk-posture unnecessarily.

Adlumin's Progressive Penetration Testing Program provides real-world penetration scenarios that cover industry-specific threat assessments and offers rapid results with actionable recommendations. An audit trail provides a reverse-engineered blueprint to demonstrate how testers could access the environment, move laterally, gain access to critical systems and "capture the cyber flag" to prove the efficacy of the testing.

Benefits of the Adlumin Progressive Penetration Testing Program

Core Functionality

Requires no persistent or credentialed agents

Scopes specific IP ranges to scan or IP ranges to avoid

Intelligently identifies the scope for you

Enables or disables specific attacks

Use cases

Enables understanding of the security posture across several dimensions so cybersecurity teams can:

FIND

Proactively discover, leverage, and chain exploitable weaknesses to:

Prove out the potential critical business impacts with proof-of-exploit in hand.

Understand the attack vectors leading to critical impacts to know exactly what to fix to disrupt the kill chain.

FIX

Focus on efficiently mitigating or remediating weaknesses that can be exploited instead of chasing down unexploitable vulnerabilities and false positives

VERIFY

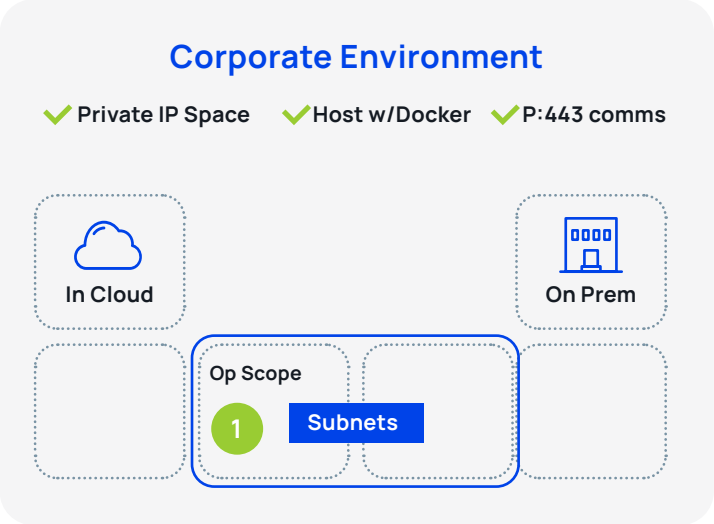
Validate those mitigations or remediations were implemented and remain implemented.

CONTINUAL

Continuously assess the security posture and quickly compare results to see what new weaknesses have been added or fixed.

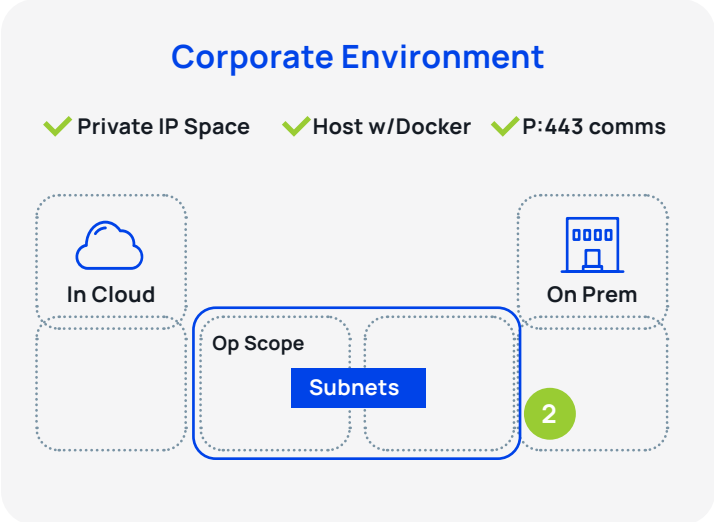
Deployment options - Your operation launch point matters

	Custom Scope			Intelligent Scope	RFC 1918	OSINT
	1	2	3	4	5	6
NodeZero placement	Inside the Scope	Outside the Scope	Outside @ endpoints (i.e. /32s)	Attack starting point	Full private scope	NOTE:CloudZero launches externally
Intent	I want to limit the scope and see what an attacker could exploit from that defined range	I want to limit the scope to see if an attacker can access host and data inside	I want to look at specific endpoints to check for host vulnerabilities misconfigurations	I want to see what an attacker can discover and access from a specific starting point	I want to search every nook and cranny of private IP space accessible in my environment	I want to see what publicly available data makes our business vulnerable to an attacker
Will enumerate and exploit	In-scope hosts, services domain, web, credentials, & data resources Pro-tip: ensure a DC is "in scope"	In-scope hosts, services, web credentials (except MITM and PTH attacks) and cloud assets	Specified hosts, ports, services, web and certs, exploitable vulnerabilities	Discovered hosts, services, domain, web, credentials & data resources	Discovered hosts, services, domain, web, credentials & data resources	Publicly available user names, subdomains, (from TLDs), and web facing attack surface
Won't execute	On anything outside the prescribed scope	Man-in-the-Middle attacks	On infrastructure nor chained vulnerabilities misconfigurations that could lead to compromise	On inaccessible hosts, services, domain, web, credentials	On inaccessible hosts, services, domain, web, credentials	On internal assets *Note: When combined with an internal op w/ access to a DC, will verify user/ password access
Use Cases	• Internal Pentest • SOC SLAs • Verify policies • Verify EDM/ SIEM	• Internal Pentest • Verify Segmentation • Verify access to a sensitive VLAN • Third party security assessment	• Test EDR • Assess endpoint vulnerabilities	• Internal Pentest • Verify segmentation • Verify policies • Verify EDM/SIEM • Test Blast Radius • Test ZeroTrust	• Internal Pentest • Environment & Asset Discovery • Assess hybrid env • Verify policies • Verify EDR/ SIEM	• Public-facing reconnaissance • Company Recon • User recon • Subdomain recon • *Cred Stuffing



1 Inside Custom Scope

If you want to limit the scope and see what an attacker could exploit from inside that defined range, you will place the Node host within the scope you want to test.

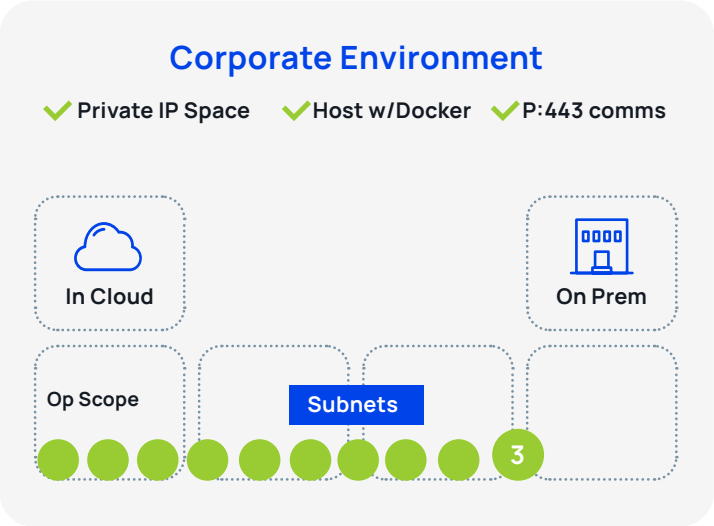


2 Outside Custom Scope

But if you wanted an "outside-in" perspective to see if an attacker could access critical data and assets inside a specific scope, you will place the Node host outside the scope you want to test.

When you set up the scope for your Pen Test, the Node host is NOT within the specified CIDR range(s) for the test.

NOTE: When Node is not in the same IP range as the scope, it will not execute Man-In-The-Middle and pass-the-hash attacks. This is your unrestricted assessment, providing true insight into what is accessible, valuable, and vulnerable from any starting point.



**NOTE: With #2, when Node is not in the same IP range as the scope, it will not execute Man-In-The-Middle and pass-the-hash attacks. Further, with this restricted scope, Node will not chain weaknesses or paths as you have limited the scope to a specific endpoint for this assessment*

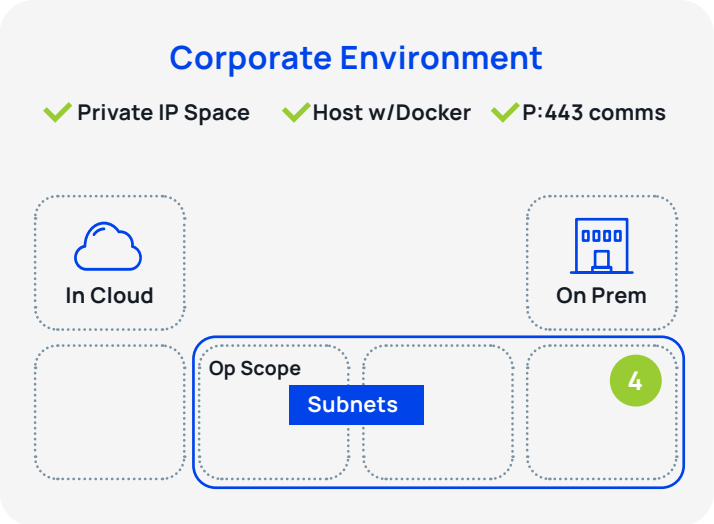
This is your restricted assessment; a quick turnaround op to verify your fix-action was implemented, and a vulnerability less severe to your attack surface.

3 Endpoints Only Scope

Once in a while, you may want to quickly verify if the vulnerability you just remediated had the desired effect. In this case, you can select a single host or range of hosts by /32s

When you set up the scope for your Pen Test, make sure the Node host has access to the specific host identified by the /32 CIDR range(s) for the test.

When you set up the scope for your Pen Test, just make sure the Node host is NOT within the specified CIDR range(s) for the test.

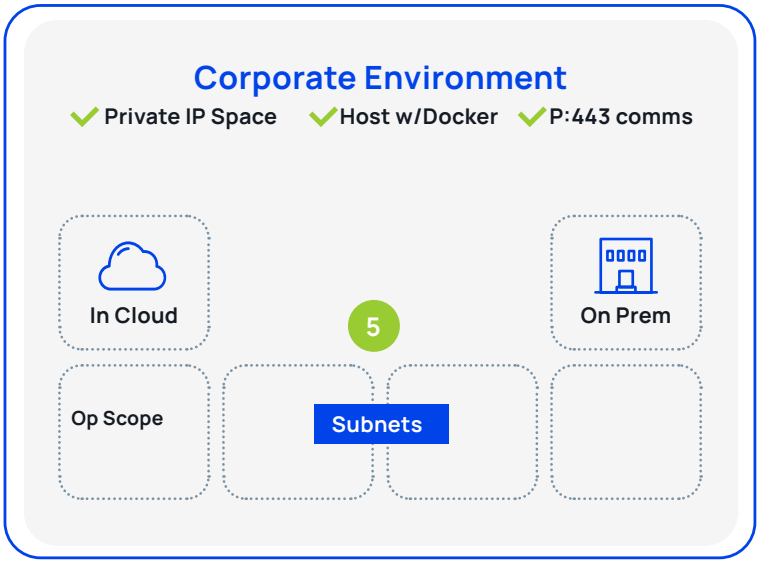


4 Intelligent Scope

Let's say you wanted to see what an uncredentialed attacker could enumerate and exploit from a specific starting point in your network – "black box" pen test – this calls for Intelligent Scope.

When you set up the scope for your pen test, leave the "Include" box blank. Node Zero's host subnet will provide the initial scope and expand organically during the pen test as more hosts and subnets are discovered, just like an attacker would.

This is your proactive assessment; providing accurate insight into what is accessible, valuable, and vulnerable from any starting point.



NOTE: This op may take a bit longer as Node enumerates any IPs and DNS names it can access…including edge routers; if yours are misconfigured for routing private IPs, Node may attempt to enumerate those external private IPs.

PRO TIP: if you want to see EVERYTHING, put Node in an unrestricted ACL so it can discover every nook and cranny online in your environment. This is your unrestricted and holistic enterprise assessment–and should be run regularly.

5

All Private IP Scope (i.e., RFC 1918)

And when you are really ready to roll, you'll love the ability to run an RFC 1918 full private scope pen test, enumerating everything accessible quickly and safely.

Deliverables:

The complete results of the penetration test are documented in four separate reports.

1. Executive Summary report
2. Pentest technical report
3. Segmentation Report
4. Fix Actions report

The comprehensive results document and explain each vulnerability, impact, evidence, observed instances, and remediation recommendations. Exploits are visually documented to demonstrate impact and ensure a complete understanding of how the exploit is performed.

The Portal and Adlumin Integration:

Adlumin operates under one application, one license concept delivering a command center for security operations to our customers. Customers must be able to come to the Adlumin portal and receive data and reporting on critical information about the service and the performance of the service itself. The most standard here is being able to convey to the customer accurate statistics about the performance and results of the service, for example:

1. Date of the last Pen test
2. Monitoring the status of a pentest while it is running
3. Retrieving pentest reports after completion

Every customer must be able to come to Adlumin to produce an executive-level report that contains all these statistics as well as visually see results and service performance metrics in a dashboard.

What you can't see poses the greatest risk to your organization. Your exposures lurk in the cloud, hybrid environments, and the darknet. There are countless gaps where threats can hide before they lead to business disrupting events like ransomware shutdowns or massive data breaches.

Adlumin Inc. is a patented, cloud-native Security Operations Platform plus Managed Detection and Response Services. The platform focuses on advanced cyber threats, system vulnerabilities, and sprawling IT operations to command greater visibility, stop threats, reduce business risk, and automate compliance. The command center for security operations, Adlumin leverages powerful machine learning, identifies critical threats, orchestrates auto-remediation system updates, and provides live continuous compliance reporting. Don't let your IT organization be caught in the dark.

Illuminate Threats, Eliminate Risks, and Command Authority with Adlumin. www.adlumin.com