





State, Local, and Education (SLED)

Organizations Face a Different Cybersecurity Reality

SLED organizations operate under constant pressure. They must defend critical services, public infrastructure, and sensitive citizen data while working with limited budgets and small security teams.

-  **Talent:** Security and IT professionals are difficult to recruit and retain. Many SLED organizations must protect large environments with only a handful of practitioners.
-  **Workload:** Security teams face a growing backlog of vulnerabilities, alerts, and compliance requirements. With limited resources, it's difficult to determine which weaknesses actually pose real risk.
-  **Regulations:** Government entities must meet a wide range of regulatory and audit requirements while maintaining day-to-day operational security.
-  **Targeted:** Municipalities, universities, and state agencies are frequent ransomware targets because disruption to public services creates pressure to resolve incidents quickly.



Hack, fix, verify, and repeat on-demand:

The NodeZero® AI-Native Proactive Security Platform helps SLED organizations continuously identify and eliminate the security weaknesses attackers can actually exploit. Instead of relying solely on vulnerability scans or point-in-time assessments, NodeZero safely performs real attack techniques across your environment to reveal how weaknesses can be chained together to compromise systems.

Helping the City of St. Petersburg Strengthen Its Cyber Defenses

After deploying NodeZero, the City of St. Petersburg, Florida gained visibility into how attackers could move through its internal networks.

Within 11 months, the city reduced security weaknesses across more than 3,000 internal hosts by nearly half and eliminated exposures that could have led to critical infrastructure compromise.

NodeZero uncovers security exposures that traditional tools often miss, including weak credentials, exposed data, misconfigurations, insecure policies, and ineffective security controls.

Every step of each attack path is fully documented, giving security and IT teams clear visibility into how an attacker could gain access and what actions they could take next. With detailed remediation guidance and the ability to quickly retest fixes, organizations can close security gaps faster and verify that their defenses are working as intended.

Capabilities include internal, external, cloud, and Kubernetes pentesting, AD Password Audit, Rapid Response testing, and Phishing Impact testing.





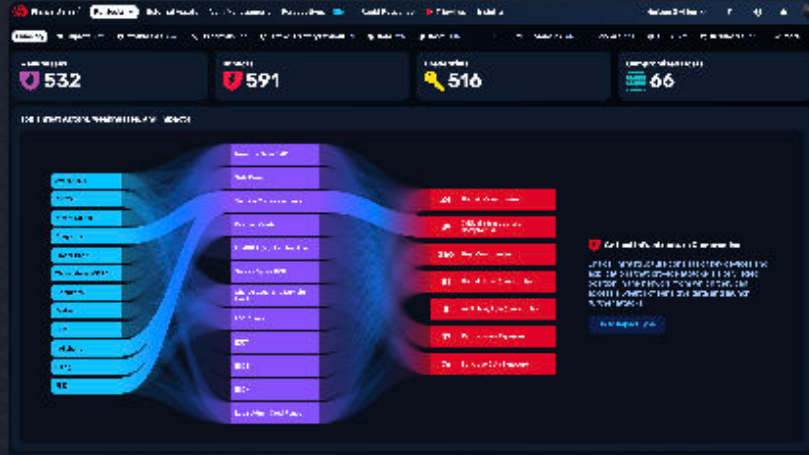
NodeZero Delivers Great ROI

NodeZero is widely adopted by SLED organizations because it is easy to use, cost-effective, and delivers measurable value.

A NodeZero subscription can cost about the same as a single manual pentest, but it allows organizations to run pentests whenever they need them.

This enables security teams to continuously hack, fix, verify, and repeat on-demand without the delays and costs of traditional penetration testing engagements.

For example, the Director of Technology at a public university in Victoria, British Columbia uses NodeZero to improve their cybersecurity posture and run weekly pentests to stay ahead of emerging threats.



Security is a journey and not a destination; being able to continuously run scans and pentests with NodeZero is great.

- Director of Technology, Public University



When the Desert Research Institute (DRI) in Reno, Nevada needed an affordable way to run penetration testing and vulnerability scanning, they turned to NodeZero.

“NodeZero has a complete process and looks for weak credentials and other holes, vulnerabilities, or misconfigurations an attacker could use to break into the system.” - Ryan Coats, Information Security Officer with DRI



NodeZero Maximizes Your Team’s Effectiveness

NodeZero helps security and IT teams work more efficiently by identifying the weaknesses attackers can exploit and providing clear guidance on how to fix them. Every finding includes detailed remediation steps, helping teams quickly understand what to address first.

By revealing systemic issues such as weak policies or misconfigurations, NodeZero can help eliminate multiple weaknesses with a single fix. Organizations can then retest quickly to confirm their defenses are working and track improvements over time.

With intelligence from Horizon3.ai’s attack research team, NodeZero helps organizations quickly determine whether emerging zero-day and N-day vulnerabilities impact their environment so they can take action sooner.

You can launch your first NodeZero pentest in minutes. Schedule a [demo](#) to see how it works. Horizon3.ai also offers [pentesting services](#) to support compliance requirements such as PCI, SOC, and NIST.