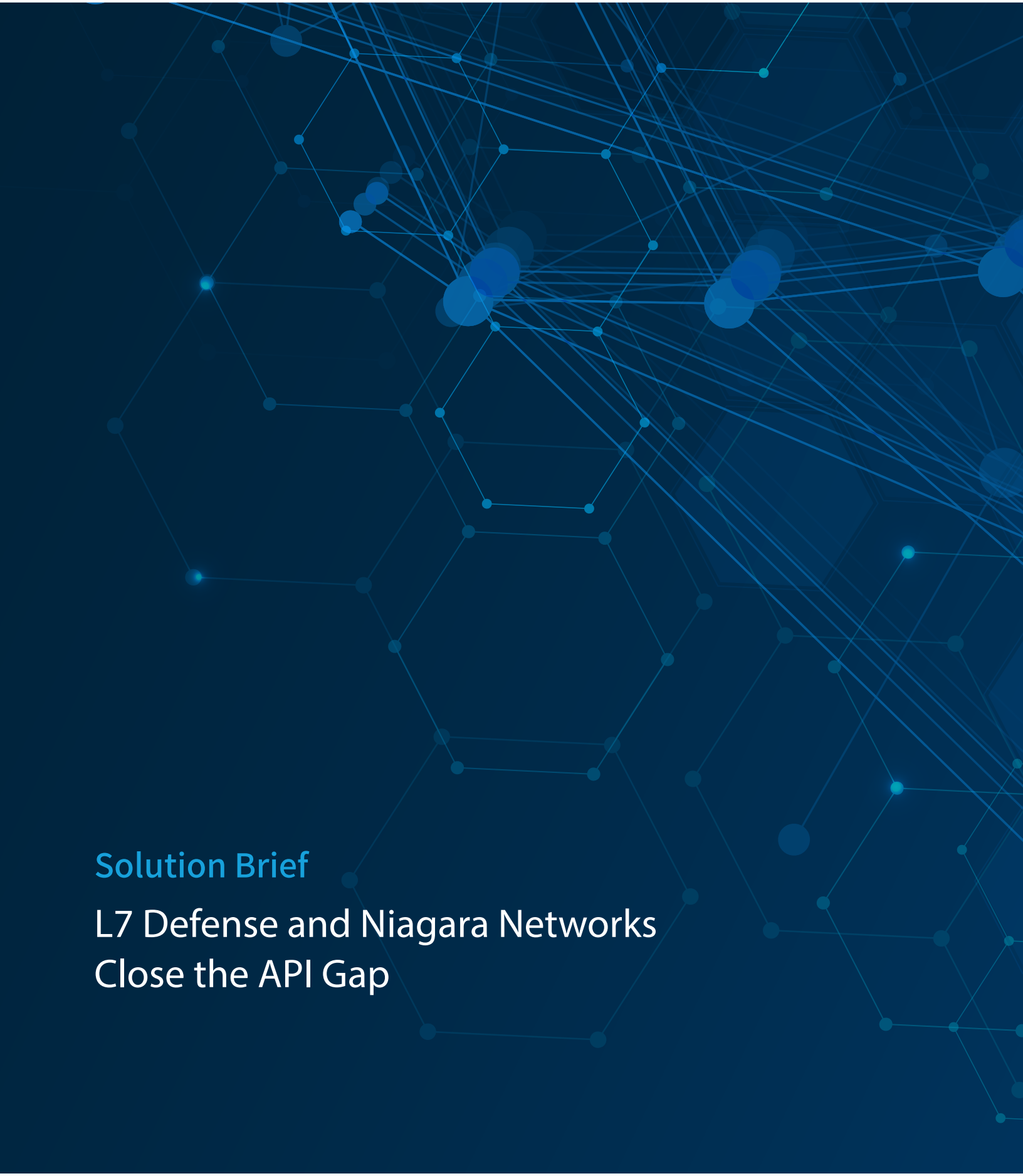
NIAGARA NETWORKS

L7 DEFENSE



Solution Brief

L7 Defense and Niagara Networks Close the API Gap

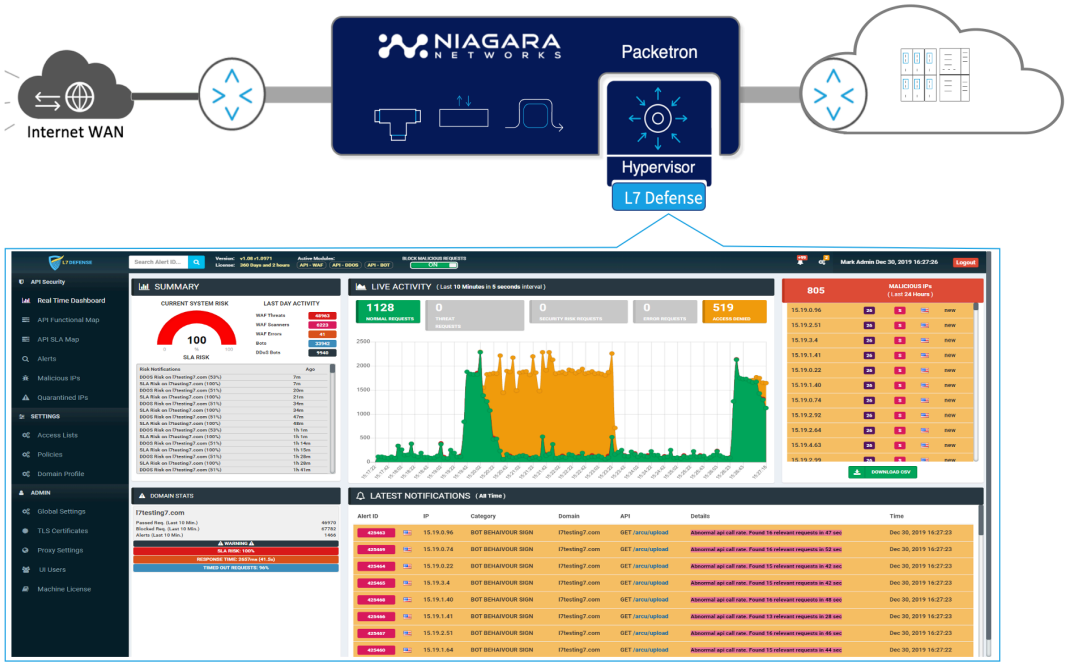
L7 Defense and Niagara Networks Close the API Gap

APIs exponentially expand the attack surface of the enterprise

Gartner: “By 2022, API abuses will be the most-frequent attack vector resulting in data breaches for enterprise applications.”

Nine out of ten top vulnerabilities in the current OWASP report apply to APIs. Denial of service and botnet attacks can be directed at APIs through websites, apps and other related interfaces.

In addition to the OWASP10 vulnerabilities, APIs present a set of new vulnerabilities, not handled by current tools.



Challenges: APIs require a new security paradigm

Authentication and rate limiting are today’s core API security features, ensuring resources are securely accessible by internal groups, partners, and third-parties. However, credentials are insufficient to protect APIs – attackers with compromised credentials look exactly like valid clients.

Identifying suspicious activity amidst a sea of API traffic is a major challenge. Attempting to Identify a single malicious transaction amongst tens of thousands of API calls is futile.

Can the enterprise protect what is being opened?

Can it trust what’s coming in?

Can it control what’s going out?

Joint Solution benefits

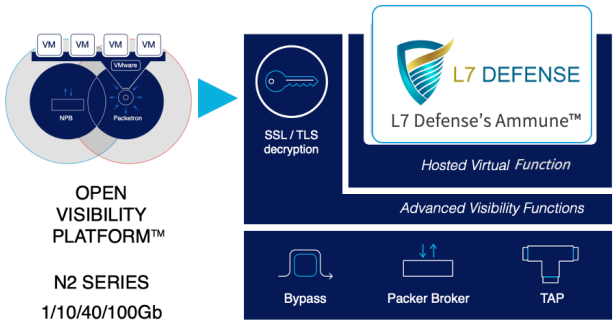
L7 Defense and Niagara Networks have joined forces to offer L7 Defense’s Ammune™ API-Bot, API-WAF and API-DDoS as a unique integrated solution on the Niagara’s Network Packet Broker. L7 Defense is fully protecting financial services, e-commerce, gaming, media and critical infrastructure from the most advanced, AI-driven, API-Borne Threats.

L7 Defense and Niagara Networks Close the API Gap

- With L7 Defense Ammune's unique, real-time ***unsupervised learning*** technology, attacks are mitigated on-the-spot, preventing application server downtime that results in heavy operational expenses and lost revenues.
- Accuracy. Organizations gain extremely accurate, early-response laser-focused protection, targeting malicious attacks in a highly complex landscape of mixed innocent and malicious internet traffic.
- Unprecedented and unrivaled NPB & API defense Integration. Niagara Networks captures all traffic of interest from anywhere in the network and provides full packet visibility to L7 Defense's agile API-Bot/ WAF/DDoS protection platform.
- Simplified Deployment. The joint L7 Defense Ammune and Niagara Networks solution is the perfect solution for midsize-to-large network deployments or remote locations for any bandwidth from 1/10/40/100G.
- Integrated N/APM NPB Visibility. Niagara Networks can host L7 Defense's Ammune on its native x86 host platform as a pre-integrated solution.
- Niagara Networks' integrated NPB redirects API traffic flows to Ammune for inspection. This also decrypts TLS traffic for inspection and re-encrypts it before forwarding it to protected servers. The process is fully transparent to the client and the protected servers. Full analysis of the incoming requests is performed through a unique, application-aware process.
- Identification. Ammune isolates the exact attacking vectors in real time. This capability is not constrained by the number of simultaneous attack vectors.
- Sensitivity. Detection sensitivity is not limited by the attack amplitude, overall traffic volumes or the length of the attack.
- Signature. Ammune generates on-the-spot signatures optimized for the discovered attacking vectors.
- Mitigation. Ammune automatically loads the optimized signatures to its filtering module in order to mitigate bad requests. The signatures can also be exported to other solutions in the customer's network stack.
- Architecture flexibility. You can install Ammune inline in L2FWD/L3FWD mode or in out-of-band mode where Ammune receives only a copy of the traffic and sends its mitigation signatures to third party solutions like IPS, FW, WAF, API GW, etc. In inline installations robustness of the setup is guaranteed via the H/W bypass component of the Niagara Networks solution.

Open Visibility Platform Value Proposition - The Road to Deployment Agility

- OVP provides an open, high performance unconstrained deployment hub for hosting virtualized solutions combined with intelligent network traffic delivery capabilities to unlimited security and networking solutions.
- Address the NetOps & SecOps challenge - the ability to deploy a security or a networking solution in the network has been a long, complicated process – one of the least agile in the enterprise.
- Freedom to choose - not tied to closed garden offerings of a particular vendor.
- Deployment Hub - enables agility and flexibility by providing a deployment hub to easily host and serve multiple security and networking solutions. The deployment hub is a high performance/ high-reliability appliance that meets stringent demands for the core networking reliability, scalability and performance required by networking teams.
- Getting the Right Traffic the Right Way - intelligently deliver traffic and configure policies and rules to establish traffic flows to and from solutions. Determine the logical sequence of traffic being sent to the hosted applications as needed. Policies, actions and traffic steering can be triggered to address host application failure and failover conditions.



N2 - Modular multi-purpose Terabit packet broker

About L7 Defense

L7 Defense is the first company to apply the "innate" immune model to cybersecurity. L7 Defense's Ammune™ is a top-of-the-line unsupervised-learning defense technology, upon which a family of defense products are built . The Ammune technology protects from major API-borne, AI-driven bot, DDoS and WAF attacks, which define the next-wave of fatal cyber-attacks. It is an INLINE advanced machine-learning solution that protects APIs from the most advanced attack types, with no impact on traffic.

About Niagara Networks

Niagara Networks™ is a Silicon Valley based company that pioneers the Open Visibility Platform™ to bring desperately needed agility to network security.

Niagara Networks provides high-performance, high-reliability network visibility and traffic delivery solutions for the world's most demanding service provider and enterprise environments.

We Design, Develop and Manufacture our Products in Silicon Valley, USA.

NIAGARA NETWORKS TECHNOLOGY ALLIANCE

2020 Ver 4.1

NIAGARA NETWORKS

150 E Brokaw Road
San Jose, CA 95112, USA

www.niagaranetworks.com
info@niagaranetworks.com

Tel: +1 408 622 0354
Fax: +1 408 213 7529