PROTECTWISE™

GARLAND TECHNOLOGY
See every bit, byte, and packet®

Joint Solution Brief

Key Benefits

- 100% network visibility and access
- Easy collection and visualization of netflow, metadata, truncated flows and full-fidelity PCAP by protocol and application
- Long-term retention for retrospective analysis and correlated event creation
- Continuous, automated threat detection and analysis in real-time and retrospectively
- Community-scaled threat intelligence and analysis
- See packets before and after they go through active, inline security tools with historical look-back
- Deliver and analyze decrypted SSL, TLS and SSH traffic
- Collect unidirectional traffic, that does not go back into the network

The Challenge

Moving enterprise workloads to the cloud creates stumbling blocks for security teams as they no longer have the visibility needed to be effective. These busy professionals can't sacrifice on accuracy or the time it takes to work across multiple solutions to see and respond to threats to their physical and cloud workloads.

The ProtectWise and Garland Technology Joint Solution

The Garland and ProtectWise™ solution provides 100% network visibility with an end-to-end infrastructure that eliminates network blind spots. Garland's network TAPs and purpose built packet brokers tap the live wire for 100% packet capture which is delivered to The ProtectWise Grid™. Delivering security entirely from the cloud, The ProtectWise Grid provides automated network detection and response across time for any network. The joint solution gives security teams a single place to get end-to-end visibility across enterprise, cloud and industrial environments.

Record Everything

The ProtectWise Grid creates a lasting high-fidelity memory of enterprise activity on any network. It captures, optimizes and stores full-fidelity traffic into a single haystack in the cloud, giving you the ability to know whether threats have ever impacted your environment. It combines unlimited visibility with detection of complex threats that develop over time so security teams can hunt for and investigate threats strategically at every attack stage. The ProtectWise Grid also provides search at unparalleled speed so analysts can sift through large volumes of historical data quickly for more efficient threat hunting.

See Everything

The ProtectWise Grid uses a finely tuned hierarchy of expert systems to analyze network traffic and to provide threat detection standalone appliances cannot. Cloud economies of scale enable The ProtectWise Grid to apply a range of techniques in parallel on massive amounts of live data to detect known and unknown threats in real time. These techniques include machine learning, intrusion detection, retrospective analysis, customer specific event modeling and heuristics.

Historical data is automatically and continuously re-assessed via retrospective analysis to detect prior exploits of newly discovered vulnerabilities. This means you can measure the full impact of newly discovered attacks going back into weeks, months or even years of past data.

The ProtectWise Grid correlates intelligence from proprietary research, flow-based traffic algorithms, and multiple third party intelligence feeds. Collective correlation of security events across customers creates a feedback loop that eliminates noise in the security environment. It's a shared brain that constantly learns and adapts to reduce alarm fatigue caused by false positives.

Seeing every bit, byte and packet with The ProtectWise Grid starts with collecting 100% of the live wire data. Garland's network TAPs (test access point) are instrumental in enabling this visibility and enabling ProtectWise to perform real-time and reliable data capture.

Garland's network TAPs and purpose built packet brokers are scalable for increased network speeds from 1G, 10G, 25G, 40G and 100G and allows you to filter, aggregate, and load balance

to one or many monitoring ports. Garland provides the flexibility to make policy changes based on live real-time data, determine baseline traffic, eliminate risk of oversubscribed SPAN ports all while sending data flows, transactions and sessions to The ProtectWise Grid.

The ProtectWise Grid also integrates with a variety of security products including firewalls, gateways, endpoints and SIEMs to add context for streamlined incident response.

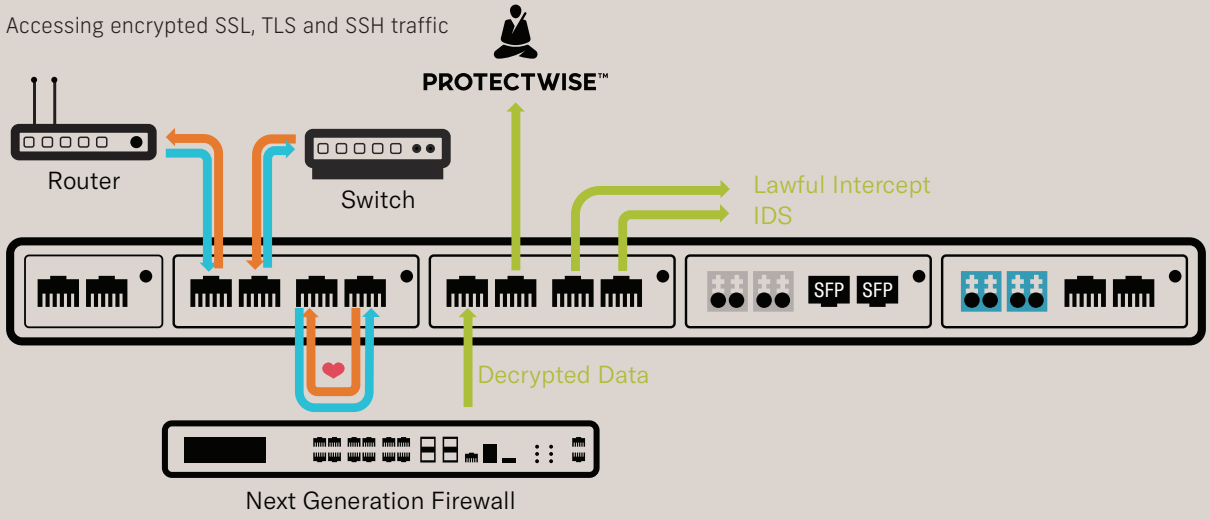
Experience Immersive Security

The ProtectWise Grid provides analysts with an immersive security experience that cuts through the alert noise via advanced security visualizations. This one-of-a-kind user interface enables intuitive interaction with petabytes of data and efficient incident response and threat hunting.

Analysts get an at-a-glance view of an organization's entire network, see events by kill chain stage across past and current timelines, and more. They can pivot easily into a deeper forensic workbench that includes deep packet exploration, policy replay for applications and protocols, and PCAP data downloads for more advanced threat hunting.

Deployment Options

Use Case 1: Accessing encrypted SSL, TLS and SSH traffic



Use Case 2: See packets before and after they go through active inline security tools

PROTECTWISE™

1601 Wewatta St • Suite 700 • Denver, CO 80202 • 1.303.625.6802
www.protectwise.com • info@protectwise.com