PROTECTWISE™

WHO IS PROTECTWISE™?

Denver-based cloud security company led by veterans from McAfee, Palo Alto Networks, and Symantec. Founded in 2013. Raised more than $70 million in funding to disrupt the industry with an innovative platform.

WHAT DO THEY DO?

The ProtectWise Grid™ is changing security—providing visibility from network to endpoint, automated threat detection and unlimited network analysis—on demand and delivered entirely from the cloud.

WHAT MAKES THE PROTECTWISE GRID UNIQUE?

- **Pervasive visibility.** Only ProtectWise provides centralized visibility network to endpoint—in the DMZ, core, remote offices, cloud and industrial environments.
- **Unlimited forensics.** Full fidelity PCAPs stored for as long as needed create a lasting memory of your network. Only ProtectWise offers indefinite retention of forensic data.
- **Multi-faceted threat detection.** Multiple analysis techniques run in parallel to reliably detect threats in real-time, including ones that can't be identified by deterministic means like signatures and rules alone.
- **Automatic retrospection.** Historical network traffic is replayed against the latest threat intel continuously to find past exploits of newly discovered vulnerabilities to reduce dwell time. Only ProtectWise enables security teams to determine with confidence if their organization has ever been impacted.
- **Complete correlation.** All threat observations (i.e., alerts) are correlated to security events (i.e., incidents) for context that explains why an event was generated. Technology integrations with the security ecosystem pull in additional context.
- **Immersive visualizations.** A video game-class UI elevates the investigation and hunting skills of all analysts, allowing them to cut through noise so they can interact more intuitively with massive volumes of data.
- **Frictionless deployment.** Lightweight software sensors can be deployed anywhere and can be delivered to customers by email so they can start seeing value in 15 minutes or less.
- **Open platform.** Use RESTful and streaming APIs to incorporate analytics and enriched forensics, including full-fidelity PCAP data from the platform, into existing incident response workflows.

WHAT ARE ITS PRIMARY USE CASES?

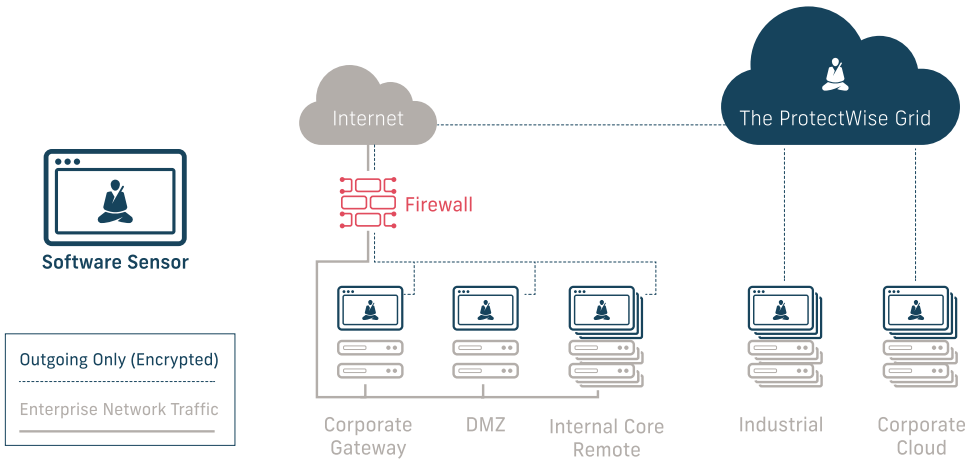
Intrusion detection: Highly reliable threat detection that extends the coverage area of intrusion detection systems (IDS) beyond the perimeter to include cloud and industrial environments.

Security Analytics: On-demand cloud security analytics for more effective forensic analysis, incident response and threat hunting.

SIEM for Incident Response: Full-fidelity PCAPs correlated to logs for context to prioritize investigations and actionable detections of known and unknown threats on any network can be presented in any SIEM.

Threat Hunting: Security data, enriched by analytics models trained on billions of attributes and supported by PCAPs, is consolidated into an easily accessible cloud haystack to enable faster discovery of new threats.

Orchestration/SOC: Integrations with the security ecosystem enables use of highly reliable detections for more effective and automated detection-triage-response workflows.



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

HOW DOES IT WORK?

1. An unlimited number of lightweight software sensors can be deployed in enterprise, cloud or industrial environments. For cloud environments where there is no practical network tap, software forwarding agents deliver traffic to sensors. Prepackaged AMIs are available to ease AWS deployment.
2. Sensors capture, optimize and stream full-fidelity PCAP, metadata, or flows to The ProtectWise Grid for analysis and indefinite storage.
3. A hierarchy of expert systems (e.g., threat intelligence including third-party, customer-provided (i.e., Bring Your Own Intel or BYOI) and custom intel, machine learning, anomaly detection, file analysis, heuristics) analyze huge volumes of data and run in parallel to detect threats in real time. Performance scales invisibly as traffic grows. PCAP data is correlated to events and accessible with one-click from anywhere in the platform.
4. New threat intel triggers automatic retrospective analysis. Historical PCAP data is replayed and security events are generated if there is a match.
5. Technology integrations pull in additional context including endpoint and firewall to aid investigations and to enable automatic triage and resolution.
6. Results are displayed in a unique presentation layer that provides a comprehensive view of network health. From there it's easy to pivot into incident investigation or threat hunting. The UI facilitates more accurate decision making and faster response than if using multiple legacy security product interfaces.

SALES QUALIFICATION QUESTIONS

- Do you have a PCAP, IDS, Security Analytics or SIEM project scheduled for the near future?
- Do you currently have a full PCAP solution?
- How satisfied are you with your IDS? Is it able to detect multi-stage attacks? Can it provide more forensics than just the PCAP that triggered a rule?
- Is alarm fatigue an issue for your security team? Do your detection products provide an effective way to prioritize investigations?
- Do you have cloud assets or are you migrating your infrastructure to the Cloud? How are you getting visibility into threats there?
- Security wasn't a consideration when designing industrial systems. How are your industrial environments protected?
- Would you like the ability to store PCAPs for 3/6/12 months—without paying an "appliance tax"?
- What monitoring products do you use now? Would you like to know how the power of PCAP can make them more effective?
- Can any of your security products confirm that your organization was not impacted by a threat during a specified time period?
- Does your business encompass multiple locations and/or geographies? How long did it take to completely deploy your security monitoring products? What's the ongoing overhead for implementing new product features?
- For how long are you capturing network traffic, at what fidelity (full PCAP, netflows, metadata), and in what kind of storage solution?
- Do you use other security products? We integrate with solutions like ArcSight, Carbon Black, Demisto, ELK, Gigamon, Ixia, Palo Alto Networks, Phantom, Splunk, and have APIs available for additional integrations.

CUSTOMER PROFILE

- Fortune 2000
- Final Approver: CISO
- User: Security Analyst
- Influencer: Security Architect, SOC Manager

CUSTOMER REFERENCES

References across a range of verticals including Energy, Entertainment, Financial Services, Healthcare, High Tech and Manufacturing are available.

KEY COMPETITIVE PRODUCTS

- DarkTrace
- Cisco (Sourcefire and Lancope)
- RSA (Security Analytics/NetWitness)
- Symantec (Security Analytics Platform)
- Vectra

YouTube www.youtube.com/c/ProtectWise

LinkedIn www.linkedin.com/company/protectwise-inc

SlideShare www.slideshare.net/ProtectWise

@protectwise
twitter.com/protectwise

facebook www.facebook.com/protectwiseinc

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