PROTECTWISE™
Security Enlightened™

"Once we had the sensor up and running, it immediately opened our eyes to activity on our network we'd previously been blind to."

ProtectWise Customer

Solution Brief

PERVASIVE VISIBILITY WITH THE PROTECTWISE GRID

Security spending may be up across enterprises, but the number of breaches and incidents is definitely not coming down, and security events are going undetected for longer periods of time. Unfortunately, the more organizations spend to add point products to their costly mix of detection and analytics tools, the less effective they seem to be.

The trouble is, point products don't integrate well. And the prohibitive cost of hardware to retain event information and correlate threat intelligence, not to mention limited forensic windows, keep organizations from seeing beyond false-positive ridden real-time alarms. What's more, today's enterprise security teams operate as islands, with very little outside context of current attack techniques and a limited situational view riddled with blind spots. As a result, security analysts are deluged with alerts but have no way to correlate and prioritize them.

According to industry research, the typical IT threat goes undetected an average of 201 days

The combination of these factors makes it impossible to get pervasive visibility into current and past security events. Without that holistic view, incident responders continue to operate in doubt, never knowing for certain whether their networks have been compromised. Ultimately, that creates a security process that is expensive, slow and ineffective at identifying, prioritizing and responding efficiently to high-profile events.

SEE EVERY CORNER OF YOUR NETWORK, IN THE PAST AND RIGHT NOW

The ProtectWise Grid offers a new, secure on-demand delivery model that makes it possible to record, retain and retrospectively analyze full-fidelity network data for a potentially unlimited forensic window at a compelling price point, delivering unmatched value with industry-de-fining visibility, detection and response capabilities. ProtectWise's on-demand delivery model means rapid deployment and time to value via the compression of dwell times between the identification of security events and effective response to them.

The ProtectWise Grid harnesses the power of the recorded network to detect and analyze both new threats and previously unknown threats

HOW PROTECTWISE WORKS: PAST. PRESENT. PEACE OF MIND.

ProtectWise gives enterprises a way to place an unlimited number of lightweight sensors at the gateway, in the DMZ, in the corporate cloud and at the network core. Each sensor passively captures, optimizes and replays network traffic into the ProtectWise Grid, essentially creating a high-fidelity network memory in the cloud—the ProtectWise Network Memory—for continuous analysis and retrospection of network traffic.

ProtectWise leverages cloud economies of scale to deliver powerful threat detection unlike any solution currently on the market. The ProtectWise Wisdom Engine continuously refines analysis from the ProtectWise Network Memory to identify and prioritize threats no one else can see. Based on many different sources, including indicators provided by the ProtectWise threat research team, best-of-breed third-party intelligence and intelligence crowdsourced from ProtectWise's customer base, the Wisdom Engine uses a computational model that functions like a neural net. It's continuously cross-analyzing, correlating and finding patterns in intelligence that may have no natural relationship to each other.

This is supplemented by ProtectWise Time Machine, which use real-time intelligence updates to go back in time and automatically rescore and classify historic network data. The industry's only automated retrospection engine, the ProtectWise Time Machine chronicles threats from their source to any point in time, whether they occurred days, weeks, months or even years ago.

Because ProtectWise is a cloud-based service, there is no need to store massive amounts of data on-premises or manually conduct retrospection. All the heavy lifting is done in the cloud quickly and cost-efficiently. It provides the peace of mind that comes with quickly determining whether your network has been impacted by the latest vulnerability, exploit or threat.

Finally, ProtectWise pushes the information distilled by the Wisdom Engine into the intuitive and powerful ProtectWise Visualizer. The Visualizer gives users an immersive, intuitive experience of the network, starting with an at-a-glance view of the entire enterprise network that expands into a deeper forensic workbench for effective kill-chain analysis. Network security engineers and incident responders can use the console to manage alarms, review situational reports and investigate network activity and threat observations. They can also manage sensor deployments, define capture and replay policies for specific traffic, manage users and create policies for notification of threat alerts.

In addition, ProtectWise provides publicly documented, secure APIs to offer the flexibility of integration with existing security tools and workflow. Organizations can send outside data streams and analysis to the Visualizer for an even richer dashboard display. Or they can link ProtectWise data and analytical feeds into their own proprietary visualization tools.

PROTECTWISE AT A GLANCE

NETWORK MEMORY

Lightweight software sensors quickly deploy anywhere in the network to capture everything that's happening to establish a high-fidelity memory in the cloud

VISUALIZER

Advanced threat visualization offers at-a-glance, real-time situational analysis, alarm management, and a deeper forensics workbench with kill-chain charting, network connection graphs, event timelines and more. Forensic capabilities manage policies for sensors, replay traffic and users, and create alert notifications

WISDOM ENGINE

Continuous, correlated real-time threat detection combined with the ability to go back in time to uncover previously unknown threats

Correlates Network Memory data against proprietary research and commercial threat intelligence feeds, advanced network intelligence and advanced traffic analysis

Emerging threat intelligence automatically triggers retrospective analysis of network data for continuous discovery of old but unknown indicators of compromise

VISIBILITY
See Everything.

- Visibility into netflow, metadata, truncated flows and full-fidelity PCAP by protocol and application
- Long-term retention allows for analysis of security events and observations now and in the past days, weeks, months and even years

DETECTION
Detect What Matters Most.

- Continuous threat detection and analysis in real-time and retrospectively—finding threats that were previously unknown
- Correlated, community-scaled threat intelligence and analysis

RESPONSE
React Faster and More Effectively.

Quickly identify and respond to priority events, manage alarm events, review situational reports and investigate network activity and threat observations

Rapidly access full PCAP to conduct deep-dive, comprehensive forensic investigations and reduce the dwell time between security events and effective response

THE PROTECTWISE ADVANTAGE

Offers visibility that no other solution does, while working in concert with solutions an organization already uses.

A cloud subscription model allows for unlimited sensors and the provisioning of services at compelling price points

Continuous analysis drives collective intelligence and delivers a highly distilled and prioritized threat signal

The platform reduces the mean time to know and frees up security teams to focus on the highest priority threats

FEATURES LIST

ProtectWise™ Network Memory

- Unlimited network packet capture, replay and storage for long-term retention and analysis
- Flexible deployment models at the gateway, in the DMZ, in the corporate cloud and at the network core
- Adaptive network capture (netflow/metadata, stream heads or full PCAP)
- Centralized repository for all types of network capture data, threat detection and analysis
- Fast, searchable index of network data
- Infinite sensor support and flexible sensor deployment options
- Rapid cloud evaluation and deployment
- APIs for integration with existing security tools

ProtectWise™ Wisdom Engine

- DPI and extraction of metadata from 4,000-plus protocols and applications
- Proprietary and third-party threat intelligence for IDS and reputation based on URL, DNS and IP
- Advanced network intelligence based on contextual flow analysis, advanced protocol discovery, kill-chain analysis and community-scaled detection
- Advanced traffic analysis includes correlation, heuristics and machine learning
- Continuous, correlated threat analysis and detection
- Automated, continuous, collective and real-time and retrospective threat analytics, detection and prioritization
- Automated smart retrospection triggered by new indicators of compromise, so traffic is constantly analyzed with the latest threat intelligence
- Analysis of payload, IDS, metadata reputation, network TTP heuristics and DNS

ProtectWise™ Visualizer

- Beautiful, powerful security visualization moves beyond status quo of security consoles
- SOC Heads-Up Display situational dashboard reporting
- Advanced forensics visualization allows analysts to interact with data through kill-chain analysis, network connection graphs and event timelines
- Integration capabilities to feed threat data into custom SOC and forensics dashboards
- Intuitive, rapid search capability
- Quick management of policies for sensor deployment, packet capture (netflow/metadata, stream heads or full PCAP and replay), user management and alert notifications

Try ProtectWise

Looking for a better path to complete network visibility, threat detection and faster, more effective incident response? Sign up to try ProtectWise at **www.protectwise.com** or contact Sales at **sales@protectwise.com** or **+1 855-650-0209**

ABOUT PROTECTWISE

ProtectWise™ is disrupting the security industry with The ProtectWise Grid™, its enterprise security platform that captures high fidelity network traffic, creates a lasting memory for the network, and delivers real time and retrospective alerting and analysis in a rich, innovative visualizer. By harnessing the power of the cloud, The ProtectWise Grid provides an integrated solution with complete detection and visibility of enterprise threats and accelerated incident response. The ProtectWise Grid delivers unique advantages over current network security solutions, including an unlimited retention window with full-fidelity forensic capacity, the industry's only automated smart retrospection, advanced security visualization, and the ease and cost-savings of an on-demand deployment model. For more information, visit www.protectwise.com.

PROTECTWISE™
Security Enlightened™

1601 Wewatta St • Suite 700
Denver, CO 80202
1.303.625.6802

www.protectwise.com
info@protectwise.com

20170228