PROTECTWISE™
Security Enlightened™

Whitepaper

ProtectWise™

Advanced Trust, Security and Privacy by Design

ProtectWise shifts network security to the cloud to dramatically improve the visibility and detection of threats, while enabling effective incident response. ProtectWise gives enterprises a compelling way to place an unlimited number of lightweight software sensors that passively capture, optimize and replay network traffic into the ProtectWise secure cloud platform. This creates a long-term network memory in the cloud—the ProtectWise™ Cloud Network DVR—for continuous analysis, replay and automated retrospection of network traffic. By harnessing the cloud, ProtectWise delivers unique advantages over current network security solutions, including an unlimited retention window with a full-fidelity forensic capacity, the industry's only automated smart retrospection, one-of-a-kind security visualization, and the ease and cost savings of an on-demand deployment model.

However, for many organizations, these benefits must be weighed against the trust, security and privacy concerns presented by any cloud technology.

ProtectWise understands these concerns, which is why we've designed our cloud platform to provide the highest levels of trust, security and privacy available.

Third-Party Certifications

We know it's imperative that our customers have the utmost confidence in our ability to safeguard their data. And we understand that this requires more than just taking our word for it. It requires third-party verification. We're working with leading organizations to achieve the following certifications:

Information Security Management System ISO 27001

U.S. • EU SAFEHARBOR U.S. DEPARTMENT OF COMMERCE

TRUSTe CERTIFIED PRIVACY

This begins with our commitment to empowering customers with complete control over their data. This commitment is based on a set of key features that:

- Enable flexible network coverage models so that customers can deploy the sensors at the gateway, in the DMZ, in the corporate cloud and at the network core.

- Provide the flexibility to configure sensors to capture netflow, metadata, truncated flows or full-fidelity PCAP by protocol and application via Adaptive Network Capture. Customers also get the ability to control visibility to any network flow through locally enforced policy.

- Preserve and persist encryption.

- Ensure security for data at rest and in motion.

- Scatter and obfuscate data across our cloud platform using our patent-pending Network Shattering™ technology.

Built from the ground up by a team of software-as-a-service security (SaaS) security industry veterans, the ProtectWise Cloud Network DVR is no ordinary cloud platform. Security isn't an add-on; it's the foundation of what we do. From the outset, we baked trust, security and privacy controls into the architecture, the application and the day-to-day operations of ProtectWise so that they're at the heart of our platform.

Controls range from the ordinary and expected to the extraordinary and innovative. Customers can depend on all of the industry-standard controls that they'd anticipate from any secure cloud platform, including encryption of data at rest and in motion, role-based access control and thorough background checks on employees operating the ProtectWise cloud infrastructure. Customers are also backed by the assurances of protections less frequently found in cloud solutions, including customer key management and policy-based data access, wipe and export functions.

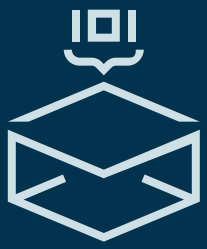
In addition to these controls, we're bringing the assurance of a new layer of security found in no other cloud offering.

We call it Network Shattering™. It's a patent-pending data scattering and obfuscation technique that fragments customer data and randomly spreads it across our secure cloud architecture so no one repository will ever contain consolidated data from a single customer.

Let's take a look at all of the controls, along with our unique Network Shattering, so you can understand ProtectWise's commitment to the security and privacy of your data.

Protection You'd Expect

The rock-solid security of the ProtectWise platform rests on security technology and processes built into the foundations of the service.



ARCHITECTURE

Security starts, of course, with the architecture of the ProtectWise cloud. We understand that strong encryption is a required fundamental of data security—whether in the cloud or on premises. So we ensure protection of the data we safeguard through AES 256-bit data storage encryption for data at rest. Meanwhile, data in motion is protected with Perfect Forward Secrecy when it is being streamed from customers into the ProtectWise cloud, as well as by TLS encryption when data is moving internally or being replayed via our Cloud Network DVR. In addition, we provide protection within our infrastructure through architectural design, segmenting systems to achieve multitenant data isolation.

APPLICATION

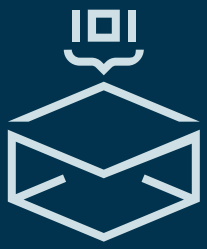
On the application front, we help customers stick to principles of least privilege and audit-trail requirements by maintaining an application that enables role-based access control. This is done through rich API connections for ProtectWise access control features and tokens to tie into enterprise identity and access management (IAM) systems. However, organizations don't need their own IAM systems to tap into ProtectWise's built-in access control features, such as multifactor authentication for access into the cloud system and for exporting any data from the system, with plenty of granularity to determine different levels of access based on the role of the user. All of these access control features then tie back into ProtectWise's reporting functionality, which keeps track of access and usage by user for a complete audit trail.

OPERATIONS

ProtectWise also understands that the protection of security data sent into the cloud requires ultimate trust in the people who administer that cloud infrastructure. As a result, we've built in a number of checks and balances. Among those are thorough background checks conducted on all of our data center employees, along with strong role-based access control for these ProtectWise employees as they interact with customer cloud infrastructure. All of their moves are tracked and audited.

Going Above And Beyond

Those ground-floor protections are pretty good for most cloud services. But because ProtectWise is dealing with some of the most sensitive data an enterprise handles, we felt it was necessary to build on them.



ARCHITECTURE

Our built-in encryption mechanisms for data at rest and in motion are unique compared to many cloud services due to the way we handle key management. ProtectWise offers an added level of privacy assurances by handing key management over to the customer. Our philosophy is that we'd like to offer the end user as much control as possible with regard to data privacy and protection, and it starts with key management. If a customer is ever worried about the safety of his data on our infrastructure, all he needs to do is revoke the keys and that data will be rendered unreadable.

APPLICATION

In the same vein, we also up the game for customer control through our application's policies for data retention. Customers are given the power to set very fine-grained policies by sensor for how much data is retained. The application can profile more than 4,000 different network protocols and applications, and it contains flexibility to determine policies to define what sensors can capture and send to the cloud repository, depending on the sensitivity of the data. So customers can configure some sensors to track full Packet Capture (PCAP) data, while for others it may make sense to limit risk and only retain NetFlow metadata or stream heads. If very sensitive data exists in a certain location on your network, it is easy enough to choose not to capture that information, thus reducing risk in the process. Similarly, too, customers can establish policies to govern who replays data from which sensors. In addition, we rounded out our added customer control features for data privacy by providing on-demand data wipe and export, with dual approval and authentication required for data export.

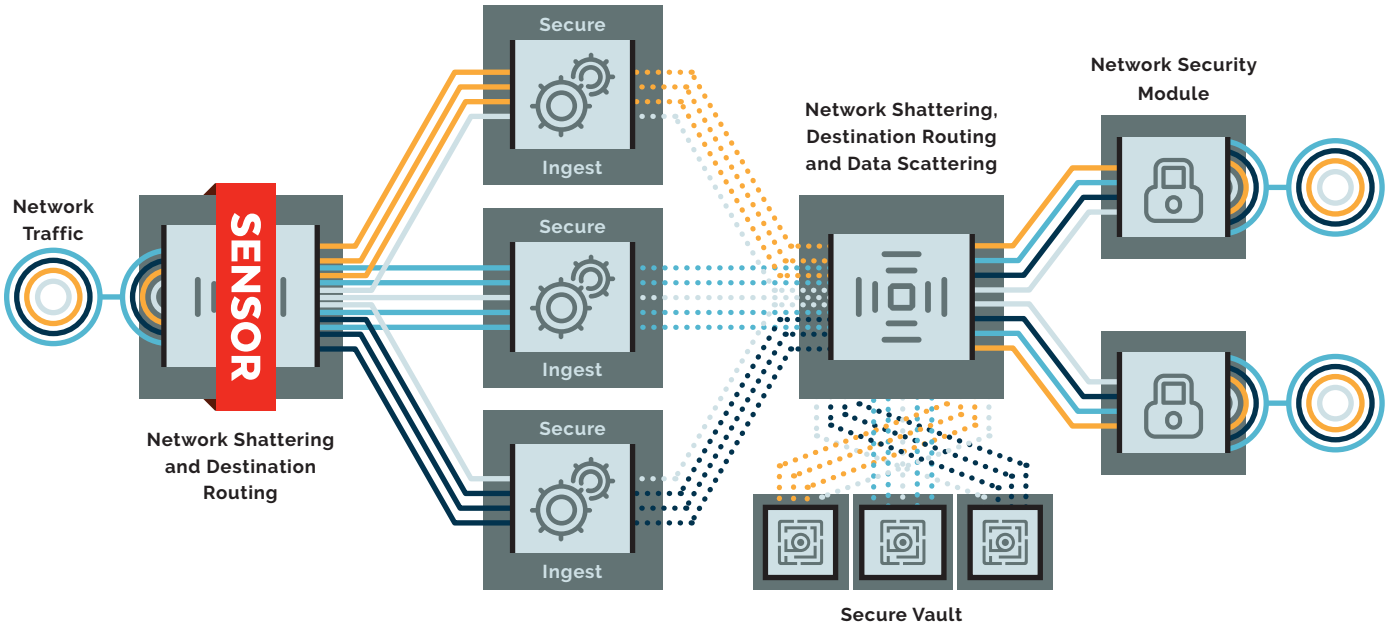
OPERATIONS

We understand that a software platform is only as secure as the code it is written in. That is why we've built our software using secure software development life cycle principles. All of our code goes through a rigorous testing process that includes third-party vulnerability testing.

The Protectwise Advantage: Network Shattering™

We strive to provide state-of-the-art data protection and continually re-examine our existing safeguards to identify areas where we can innovate on industry best practices. As a result, ProtectWise offers a feature no other cloud service has offered before.

Our secret weapon is called Network Shattering. Network Shattering works by dividing up data sent to the ProtectWise cloud platform, rerouting components within it and scattering data across our storage infrastructure. So even if an attacker could access and decrypt a hard drive, it would be impossible to reconstruct that data—and it would be unclear who the data even belongs to.



Conclusion

ProtectWise understands that no data is more sensitive than the vitals recorded from network monitoring. We've built our platform with trust, security and privacy in mind from the start. Customers can rest assured that our platform introduces no additional risk to the process of analyzing security data.

See For Yourself

Have questions about how ProtectWise can ensure the security and privacy of your data? Email us at info@protectwise.com to set up a demo or request more information.

About Protectwise

ProtectWise™ is disrupting the network security industry with its Cloud Network DVR, a virtual camera in the cloud that records everything on the network. The service allows security professionals to see threats in real time and continuously goes back in time to discover previously unknown threats automatically. By harnessing the power of the cloud, ProtectWise provides an integrated solution with complete visibility and detection of enterprise threats and accelerated incident response. The Cloud Network DVR 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. Founded by a team of security and SaaS industry veterans from McAfee, IBM, Mandiant and Proofpoint in April 2013, the company is based in Denver and was named to Network World's list of "10 Security Start-Ups to Watch."

TRUST, SECURITY & PRIVACY BY DESIGN

ARCHITECTURE

- TLS Encryption for Packet Replay and Internal Traffic
- Perfect Forward Secrecy
- AES 256-bit Data Storage Encryption
- Customer Key Management
- Multitenant Data Isolation
- Network Shattering™ Data Scattering and Obfuscation

APPLICATION

- On-Demand Data Wipe and Export
- Policy-Based Sensor Replay
- Retention Policies per Sensor
- Multifactor Authentication for Access and Export
- Dual Approval for Data Export
- Role-Based Access Control
- API Access Control and Tokens
- Access and Usage Audit Trail
- Host-based Cloud Sensor Deployment
- Hypervisor TAP Sensor Deployment

OPERATIONS

- Background Checks
- Access by Role
- Third-Party Vulnerability and Code Testing
- Secure Software Development Lifecycle Management

1555 Blake Street • Suite 450 • Denver, CO 80202 • 1.303.625.6802
www.protectwise.com • *sales@protectwise.com*