SECURITY BRIEF

Traverse:
Product Security Overview

At Kaseya, securing customer's information is our top priority. We work to ensure that your data and intellectual property is protected by the highest levels of security. Since data security is crucial to all our customers—and so, to us—we created this guide to provide an overview of the security features of the Traverse product.

Encrypted Administrative Web Interface

All traffic between the administrator's web browser and Traverse is encrypted using industry standard Transport Layer Security (TLSv1.0, TLSv1.1 and TLSv1.2) protocol with AES and 3DES Cipher Suites.

User Authentication

Users must authenticate through the administrative web interface via a username/password combination that has been configured for them by the Traverse administrator. Alternatively, Traverse can be configured to authenticate users against a customer's existing Active Directory environment. Utilizing Active Directory for user authentication ensures that your existing password policies and user onboarding/termination processes are extended to Traverse and this configuration is recommended for high-security environments.

Application Security

Traverse uses role-based access control (RBAC) to provide a robust and flexible security model to govern user access to resources. Fine-grained access control provides a powerful least-privilege model to ensure that users only have access to the data necessary to perform their required job functions. Access control is enforced across multiple layers of the solution and can be configured to grant user privileges based on functions (no access, read, read/write), departments (what organizations they have access to) and specific objects.

Database Security

The Traverse database is located on the server where the product is installed.
This server should be secured to limit access to only individuals responsible for installing and maintaining the product and all user access should be limited to the administrative web interface. Additionally, control traffic between the central location and Traverse's Data Gathering Engines is encrypted using Transport Layer Security (TLS), but database updates use industry-standard SQL commands which may contain limited information about the network devices that are being monitored.

Third-party Testing

Traverse undergoes periodic third-party vulnerability assessments and identified vulnerabilities are remedied or mitigated.

ABOUT TRAVERSE

Traverse is a next-generation monitoring solution from Kaseya, a global software solution provider with over 10,000 customers globally. Traverse's patented technology offers a distributed, scalable monitoring platform with rich data analytics and unified cloud & network management. Traverse allows enterprises and Managed Service Providers to optimize their IT operations with faster mean time to resolution for slow or failed IT services within their infrastructure. Customers leveraging Traverse include the Fortune 100 as well as small-sized and medium-sized businesses worldwide. For more information, visit **www.traverse-monitoring.com**

Rev 122815

TRAVERSE by Kaseya