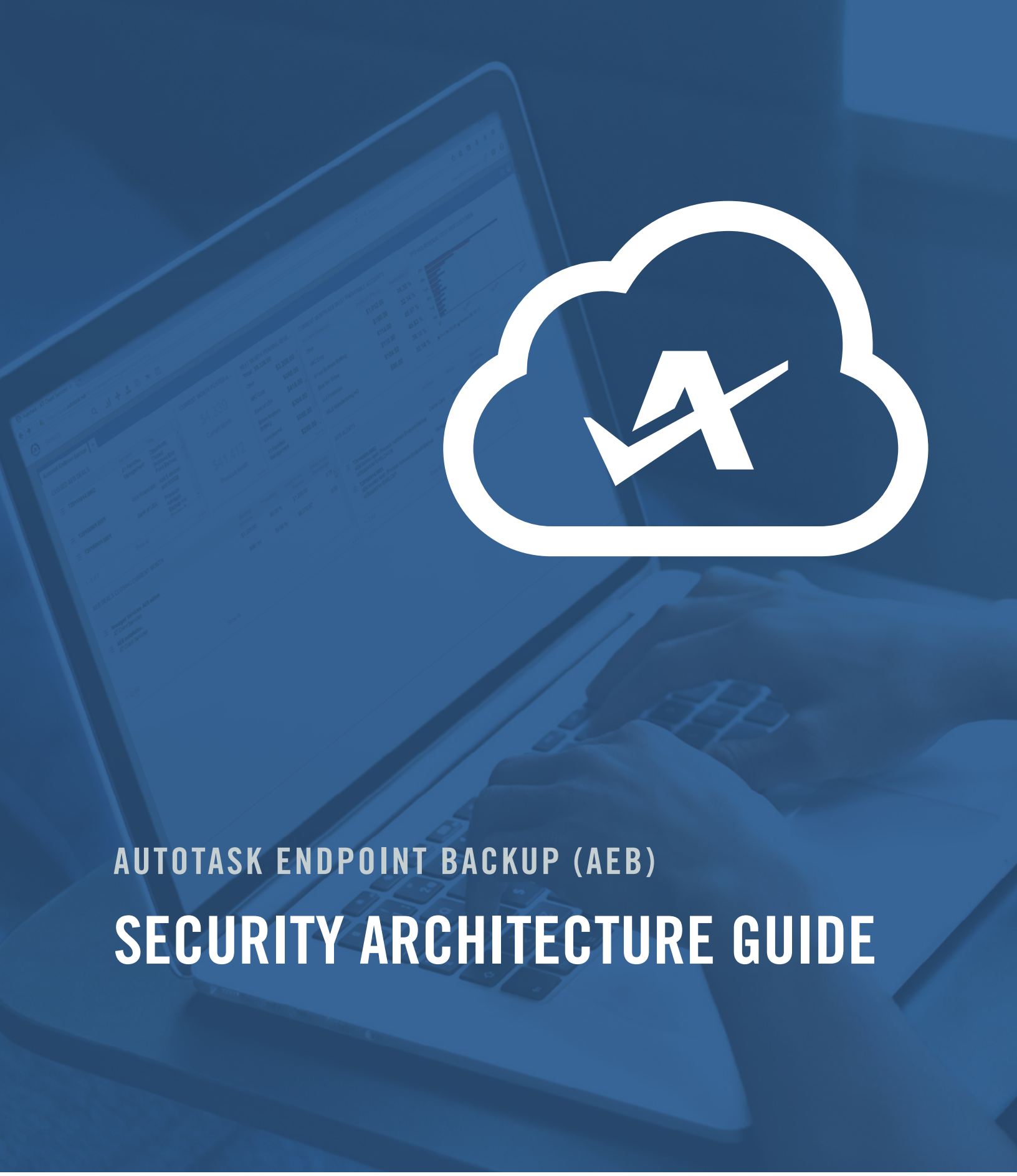

AUTOTASK ENDPOINT BACKUP (AEB)

SECURITY ARCHITECTURE GUIDE

PARTNER | Autotask Endpoint Backup

Table of Contents

Dedicated Geo-Redundant Data Center Infrastructure

As opposed to the common virtualized approach to cloud services, wherein cloud service providers lease processing and storage capacity from Internet infrastructure providers, **all Autotask hardware and software in each data center is 100% owned, operated, and managed by Autotask.** In typical virtualized cloud environments, service applications and customer data actually share processing and storage platforms in a virtual time-sliced manner, resulting in a minimum of separation between independent operating domains. With the dedicated data center approach that AEB has invested in, nothing operates on any Autotask hardware or software processing or storage platform except AEB services.

True 100% isolation of the AEB service eliminates the possibility of experiencing any service interruption, performance degradation, or malware infection that might otherwise be caused by adjacent applications. Combined with multi-level regional and data center redundancy, the AEB infrastructure represents one of the most secure, reliable, and available cloud service architectures available today.

AEB uses a co-location model for deployment of Autotask owned and operated equipment and software, utilizing the rack space, power, cooling, and physical security of major world-class SSAE 16 audited data centers. These facilities are a classified as Tier 3 or better with N+1 fault tolerant systems guaranteeing 99.982% availability. The AEB network architecture deployed to these facilities includes multiple levels of redundant application servers and storage arrays, thus ensuring High Availability, Failover support, and Load Balancing.

Autotask operates data centers in several different geographical regions, including the United States, Canada, Denmark and Australia, and is planning further expansion into other regions. Within each region, two levels of redundancy are provided. First, within each data center, redundant servers and file storage ensure that data center level failures can be isolated and resolved quickly. Second, within each region, at least two independent data centers are physically distanced and isolated from each other, thus providing protection from higher-level data center failures, regional disasters, or broader Internet related failures. This dual-level geo-redundancy ensures the greatest possible availability and protection against data loss.

The physical presence of data centers in separate regions also means that data does not leave the region; it stays in the United States for U.S.-based customers, in the European Union for EU-based customers, in Australia for AU-based customers, and in Canada for Canadian customers (in compliance with PIPEDA and local regulations).

In May 2018, a new European privacy law, the General Data Protection Regulation ("GDPR"), goes into effect. The GDPR fundamentally changes European privacy law and requires all companies that handle "personal data" of individuals in the EU to adopt more stringent privacy and security practices.

Autotask is making a substantial investment of time and resources to ensure its products and services are fully GDPR compliant by May 2018.

SUMMARY

- Co-location model with HW and SW 100% owned, operated and managed by Autotask
- Geo-redundant, Tier 3, SSAE16 Audited data centers (two per region)
- Complete, redundant, regional data set in each data center
- Complete regional server setups in each data center
- Data center redundancy using RAID6 mirrored backup with replication
- Modular clustered server farms for service load-balancing, scalability, and failover protection
- SLAs for availability (99.982%), response time, service restoral

SSAE 16 / SAS 70 and SOC2 Audits

In the rapidly changing landscape of cloud services, companies that handle sensitive information, such as in the legal, finance, and medical sector, find that they are under increasing scrutiny over their information processing controls. **AEB data centers are audited against both AICPA SSAE 16 / SAS 70 and ISAE 3402 criteria for system availability and security,** thus providing assurances regarding adequate oversight over the controls utilized in the processing of information. Similarly, AEB's own internal security controls are audited against SSAE 16 / ISAE 3402 criteria for employee policies, physical and logical access controls, intrusion detection and testing, service reporting, security incident procedures, training, change control, and configuration management.

AEB's SOC2 Type 2 examination report is issued in accordance with both the SSAE 16 attestation standards established by the American Institute of Certified Public Accountants and also the attestation standards established by the International Standard on Assurance Engagements (ISAE) 3402, known as "Assurance Reports on Controls at a Service Organization." Accordingly, AEB services can serve as a foundation upon which customers can build their SSAE 16 / SAS 70 / ISAE 3402 compliant data processing and storage policies and practices.

Logical Access Security

All AEB application servers are protected with OS security modules that apply Discretionary Access Control and Mandatory Access Control policies to all server processes, thus ensuring that no software process can be gainfully subverted.

All connection pathways within the AEB infrastructure are highly regulated as to the kinds of traffic that are allowed between various internal server endpoints. Any network traffic that does not meet the expected data flow patterns, in terms of source, destination, and traffic type, is immediately interrupted and reported to monitoring personnel through alerts. All known attack vectors are specifically prohibited.

Comprehensive Monitoring

All of the AEB regional data centers are monitored 24 hours a day, 365 days a year, by equipment service and operations staff, who also have immediate access to AEB engineering personnel in the event that it becomes necessary. Co-location with major world-class data center industry partners ensures that physical and environmental security is unsurpassed.

AEB utilizes dedicated software monitoring components that are designed to track and evaluate the operation of servers, networking equipment, applications and services within the AEB service infrastructure. This also includes monitoring of resources such as processor load, memory usage and disk space usage.

Alerts regarding performance or potential security issues are automatically distributed to several on-call staff via SMS and email.

Testing, Risk Assessment and Compliance

AEB makes use of independent 3rd-party testing, analysis and assessment services. AEB's multi-faceted approach to testing and risk assessment incorporates the following elements; ongoing 3rd party penetration testing of Web, Agent, and APIs, Periodic SAS/SSAE audits, and Daily Hacker Safe updates.

AEB is 100% compliant with all Security Rules specified in the Technical Safeguards, Administrative Safeguards, and Physical Safeguards from the Health Insurance Portability and Accountability Act (HIPAA) of 1996. AEB's Privacy Policy provides specific details regarding the policies implemented throughout AEB in order to comply with HIPAA. Furthermore, AEB engages health care provider customers as a HIPAA Business Associate through BAA agreements. AEB is also compliant with PCI DSS requirements, and therefore can be used as the foundation of a compliant infrastructure that end-customers might certify and deploy.

Data Encryption and Authentication

All files handled by the AEB service are secured, both in transit and in storage, using 256-bit AES-encryption. Furthermore, in order to maximize the separation between teams, users, and files, a different unique rotating encryption key is used for each individual file. None of the encryption keys are stored "in the clear" in any non-volatile storage, but rather are encrypted and stored under the protection of a master key. Authentication is ensured through the use of a certificate-based server authentication, which ensures that the user's agent will neither connect, nor cooperate, with any server other than those that comprise the AEB service. Even in the unlikely event of a successful attack on Internet DNS or routing infrastructure, which is quite outside the control of AEB or any other SaaS provider, AEB's certificate-based authentication will ensure that no malicious agent could successfully connect to the AEB service.

All of the Autotask Endpoint Backup regional data centers are monitored 24 hours a day, 365 days a year.

Reporting

AEB features a set of advanced reporting capabilities that are specifically designed to support auditing for compliance with company policies. These advanced reporting features, enable AEB partners to generate and export custom reports on behalf of their clients in order to establish audit trails and analytics on the following types of events:

- **Team Events** - Account management events for all users
- **User Access Events** - Device connections and portal access, with IP address filtering

Reports can be customized and altered to include or exclude a variety of events based upon various criteria, such as date range, user name, IP address, and more. Reports can be either viewed via the "Manage Team" function within Endpoint Backup Manager, and from there exported to XLS formats. When reporting on user accesses, any user access event can be mapped to specific source IP addresses, and can be viewed on a geographical map.