1E security overview

April 2023

1E security overview

Document purpose and use

This document provides an overview of 1E's Information Security policies, practices, and procedures. This document may only be shared with customers that have signed a non-disclosure agreement (NDA) with 1E.

Company overview

At 1E, we reimagine how technology serves people and create new ways for IT to shape the future of work.

The 1E platform helps IT teams improve end user experience, tighten security, reduce costs, and evolve IT Operations from cost center to strategic enabler.

Third-party hosting providers

The 1E platform has been built to be accessed over public networks, and provides unprecedented access to an organization's endpoints, so the security and infrastructure of the platform has been given great care and attention.

All customer data is hosted by Microsoft Azure. Microsoft Azure data centers comply with leading security practices and frameworks, more details can be found here https://www.microsoft.com/en-us/trust-center/product-overview.

Information security and compliance program

1E has a formal Information Security Program and a dedicated team of security engineers and compliance specialists. Our Security and Compliance teams are headed by the Senior Director of Security Operations.

Accreditations

SOC2

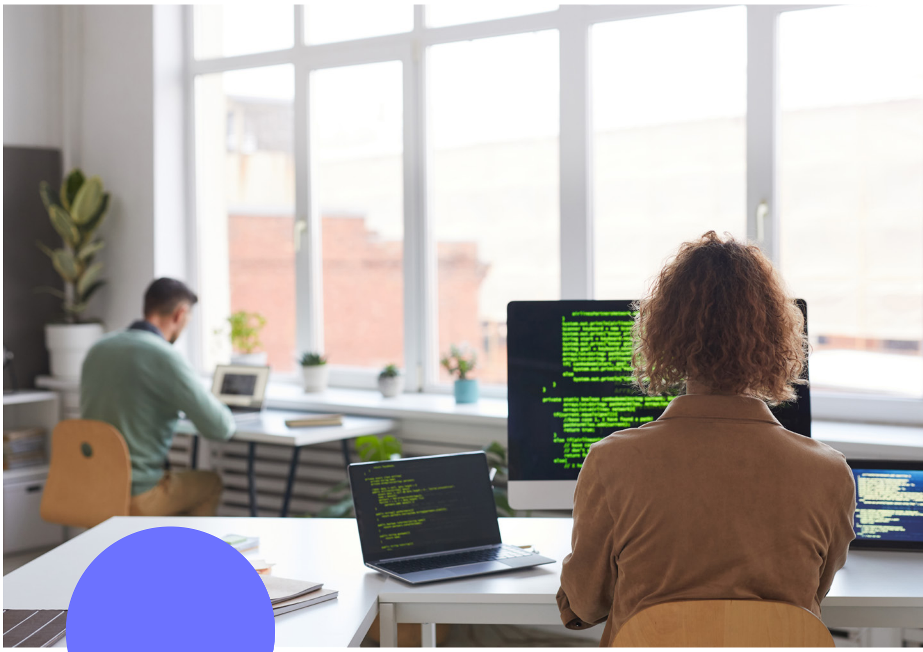
The American Institute of Certified Public Accountants (AICPA) System and Organization Controls (SOC) for Service Organizations (SOC2) is the gold standard of security certifications for services delivered from the cloud.

1E has a SOC2 type 2 report which provides a description of the 1E platform and the suitability of the design and operating effectiveness of controls covering the trust services criteria of security, confidentiality, and availability.

The report ensures:

- Oversight of the organization
- Vendor management programs
- Internal corporate governance and risk management processes
- Regulatory oversight

This report is available upon request under a Non-Disclosure Agreement (NDA).



ISO/IEC 27001:2013

Citation ISO Certification
Information security management
ISO 27001: 2013
REGISTERED

Certificate No:368632021

ISO/IEC 27001:2013 is a security management standard that specifies security management best practices and comprehensive security controls. The basis of this certification is the development and implementation of a suitable Information Security Management System (ISMS), which defines how 1E manages security and data protection.

The certification process verifies that 1E does the following:

- Evaluates the information security risks of the cloud services, considering the impact of - threats and vulnerabilities.
- Implements a comprehensive set of information security controls and other forms of risk management to address customer and architecture security risks.
- Performs periodic checks that the information security controls meet the requirements.
- 1E has been found in compliance with the standards outlined by the ISO and IEC, as stated in the audit plan.

A copy of 1E's current ISO27001:2013 certificate can be downloaded from https://www.1e.com/ISOCert.pdf

VPAT 508

A Voluntary Product Accessibility Template (VPAT) is a document that explains how information and communication technology (ICT) products such as software, hardware, electronic content, and support documentation meet (conform to) the Revised 508 Standards for IT accessibility.

1E can provide upon request the latest VPAT report for the 1E platform.

Data protection

As part of its service offering, 1E processes personal data contained in customer data, as defined in our End User Licensing Agreement (EULA) and privacy policy. During a customer's tenancy on the 1E platform, 1E acts as the 'processor' - acting on controller instructions - while the customer is the 'controller' who determines the purposes of the processing.

General use of personally identifiable information

1E uses customer Personally Identifiable Information (PII) to respond to requests and to provide, enhance and secure the platform. Generally, PII includes first name, last name, phone numbers, email addresses, and data provided by customers to use the platform.

PII collected by the 1E platform.

PII collected by the platform for use by customers within the platform is as follows:

- Process executions: Whenever a process starts on the device, the name of the process.
    - Username: The name of the user in whose session the process was launched (or blank if it is a system-launched process)

- DNS queries: Whenever a DNS address is resolved.
    - FQDN: The Fully Qualified Domain Name (FQDN) that is being resolved.

- Process stabilization: The time taken for a process to be considered stable. This is captured when a process starts on a device, but only if that process is in a list of processes selected for monitoring.
    - Username: The name of the user in whose session the process was launched (or blank if it is a system-launched process)

- ARP cache entries: Translations between IP addresses and MAC (physical) addresses, known as ARP (Address Resolution Protocol).
    - IP Address: The IP (v4) address
    - MAC address: Hardware Media Access Control (MAC) address

- User usage: Details about user sessions from login to logout.
    - Username: Domain-unique readable username. Note this value may be unique to an individual device.
    - SID: Windows Security Identifier (SID) of the user. Note this value may be unique to an individual device.
    - Email: Soon to be implemented. The email address that is cached in the system for this user. This may not necessarily be the email address to use to contact the user via corporate email.
    - First name: Forename that the system has cached for the user.
    - Last name: Surname that the system has cached for the user.

- Device inventory: Inventory data for each device.
    - SMBOID GUID: Allows system administrators to remotely identify and manage these systems.
    - 1E client GUID: Unique key used by 1E platform to identify the device.
    - Time zone: Can be used to identify the location of the device.
    - OS-locale: Can be used to identify the location of the device.
    - IP addresses: IP addresses appear in log files that may be sent back to our SaaS support team for diagnostics.
    - Log files capture device names and IP addresses for troubleshooting purposes. These files are stored in an encrypted disk volume and can only be accessed by 1E support engineers.
    - Except for log files used by 1E support, no other customer data stored within the platform can be accessed by 1E employees.

Data residency

Customers should be aware that data is never stored outside of the region that they select when signing up for the platform.

- For customers in the UK, this means all data is stored in London.
- For customers in the EU, this means all data is stored in Amsterdam.
- For customers in the US, this means all data is stored in Virginia.
- For customers in Canda, this means all data is stored in Toronto.

Where new regions are added in the future, the location of the corresponding data center will be announced to allow customers to make appropriate decisions when reviewing concerns such as the Data Protection Directive.

Risk management

1E's approach to Enterprise Risk Management has multiple layers, designed to focus on how we address risk as part of ongoing business operations throughout the year, not just as a point-in-time exercise on an annual basis. 1E maintains enterprise and cyber-security risk assessment procedures, including annual risk assessments.

People security

Background screening

All 1E employees and contractors must undergo background screening prior to employment where local legislation allows.

Employee handbook

All 1E employees must read and agree to the 1E employee handbook covering company policies, code of business conduct and ethics, and acceptable use policies. Our acceptable use policy outlines requirements around,

- Hardware, software, mobile device, e-mail, and network use
- Social media
- Data classification, handling and ownership

Non-Disclosure Agreements

All employees and contractors must sign a Non-Disclosure Agreement (NDA) prior to employment. Third-party services must sign an NDA before use.

Security training

All 1E employees and contractors attend mandatory information security training during the on-boarding process, as well as annual training thereafter. Training is tracked and monitored to ensure compliance.

Software development security

1E's Secure Software Development Lifecycle (SDLC) standard defines the process by which we create secure products and the activities that must be performed at each stage of development.

Change and release management

All changes to 1E production software follow 1E's change management process. 1E performs code reviews for internally developed software and services. Code changes must be approved via pull requests before they are merged into master branches, automated unit testing, automated functional testing, automated integration testing, and automated security testing.

Developer training

All developers are trained on software vulnerabilities, including the Open Web Application Security Project (OWASP) Top 10. These are taken into consideration during the development of features. All code is housed in source control where engineers are granted access based upon least-privilege. Training in handling sensitive data is included in the required annual security training.

Continuous monitoring and vulnerability

1E's monitoring processes and procedures provide continuous proactive and detective capabilities. 1E uses several sources and tools for identifying, tracking, responding to, and remediating vulnerabilities. We subscribe to security mailing lists for our OS, Datastores, Web Frameworks, Languages as well as to industry and government mailing lists.

Vulnerability management and penetration testing

1E performs regular and continuous scans of our systems to identify vulnerabilities. When a vulnerability is discovered, corresponding tickets are filed in our internal ticketing system and prioritized according to 1E's support SLA. In addition, 1E performs annual penetration testing of our networks and services, as well as regular application penetration testing. All penetration testing is performed by independent third parties.

Patch management

Patches and upgrades are applied based upon the severity level of vulnerability according to our patch management policy. Critical severity patches are applied within 7 days of patch release, High severity patches within 2 weeks.

Cloud and network infrastructure

Platform infrastructure

1E platform operates on resources hosted within Microsoft Azure. These resources exist and span several different Azure regions to provide increased performance for customers around the globe.

The 1E platform functionality is separated into several customer-facing services as follows:

- Web portal: For customer users of the platform.
- Switch: A permanent connection established with all connected devices to facilitate low latency event and command communication.
- Background channel: Used for downloading large data out-of-band of normal switch communication.
- API: A REST API for programmatic interaction with the platform.

Server instances

1E platform uses Windows Server 2022 Core Long Term Servicing branch and Ubuntu for the base operating systems of the server instances, hosted within Azure IaaS. These operating system images have been specially prepared and hardened for use in Azure by 1E. Server instances are launched from prebuilt and tested machine images to ensure 100% consistency. These virtual machines are backed up by Azure recovery services vaults.

Database

All data sent to the 1E platform is uploaded to SQL databases. The SQL instance is separate from the rest of the 1E platform components and is held entirely separate from any other customer data.

Firewalls

The 1E platform is only accessible through an Azure firewall instance that provides network Intrusion Detection and Prevention Services (IDPS).

All Azure resources for each customer are also secured by a dedicated Azure Network Security Group.

All access to the 1E platform is via encrypted TLS over port 443.

Information classification

1E has a formal information classification policy. Each information classification has specific requirements regarding the handling (i.e., access, storage, use, identification) of that data.

Data deletion and destruction 1E customer data resides in the Microsoft Azure cloud. Ninety days after service termination (or earlier upon request) 1E deletes all customer data using the API's provided by Microsoft.

Data encryption

Encryption in transit

All data transmitted to and from 1E over public networks is secured via HTTPS Transport Layer Security using TLS 1.2 or above.

Encryption at rest

All data at rest is encrypted using AES-256

Platform monitoring

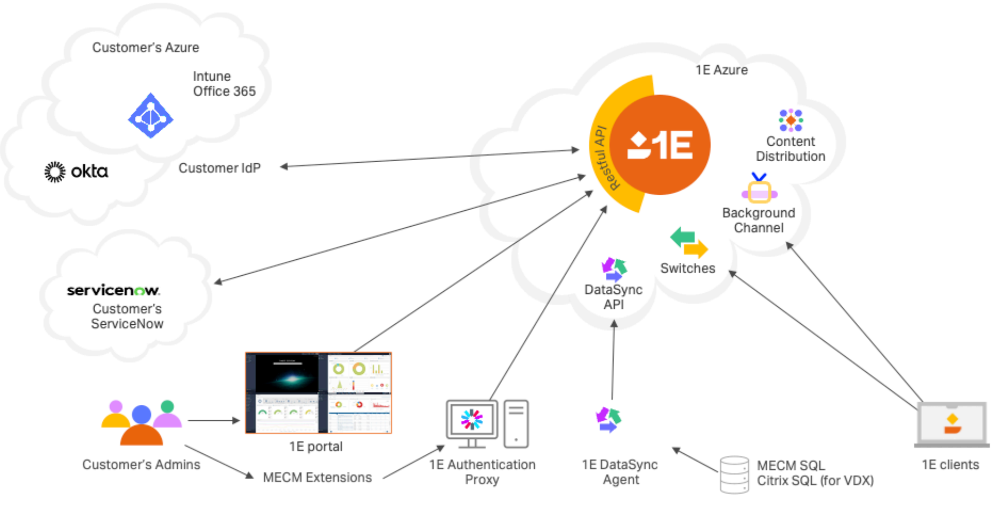
In addition to the instance monitoring services provided by Azure Data Explorer, the 1E platform uses several services to provide effective monitoring of platform health and metrics. For example, core platform services are monitored for health and throughput using custom metrics that are then pushed to Azure Data Explorer and DataDog. Custom metric and log gathering code is deployed to each server.

Azure Data Explorer and DataDog provide near real-time feedback on platform load and other potential issues that may occur, alerting regarding problems or service outages. 24/7 response is ensured through PagerDuty and a robust and well-practiced escalation procedure within 1E support.

By monitoring the platforms in this fashion, 1E can identify, pinpoint, and resolve potential customer issues before they become apparent to the end user.

1E platform architecture

1E SaaS architecture



All Internet connections use port 443 and certificate authentication

Product security

Web portal security

All access to the 1E platform web portal occurs over TLS v1.2 encrypted HTTPS using standard RSA 2048-bit certificates.

Access control is provided by the customer's own OAuth based Identity provider (IdP) via Single Sign-On (SSO). 1E currently supports Azure Active Directory and Okta directly, but other IdP's may be accommodated providing they follow OAuth 2.0 standards.

1E recommends that customers configure their IdP to enforce multi-factor authentication.

API security

The platform is entirely API driven, and the web portal is simply an extension of the API, the API is therefore secured in the same way as the Web Portal. Non-interactive API access can be configured through the customer's own IdP by using certificates as outlined in the online documentation.

1E client and switch security

The 1EClient.exe executable code is digitally signed with a certificate from 1E. All communication from the 1E client to the switch is encrypted using mutual TLS 1.2 RSA encryption over WebSockets on TCP port 443. Customers must provide a valid PKI root certificate upon service creation, and only clients with a valid client certificate from that PKI instance will be allowed to communicate with the customer's switch instance.

This ensures that there can be no accidental data contamination between customers of the platform and ensures no data leakage can occur through an unauthenticated client gaining access to a customer's switch.

There is also communication between the client and the 'background channel' which is encrypted using mutual TLS over HTTPS on TCP port 443.

Internet protocol

The 1E platform uses the IPv4 protocol. IPv6 is not currently supported.

Stateful packet inspection

Communications between clients and the switch and clients and the background channel cannot use stateful packet inspection as this would break mutual TLS and platform components would deny connectivity.

Supported TLS cipher suites

The 1E platform demands one of the following TLS cipher suites

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Infrastructure

The 1E platform runs on hardened Windows Server and Ubuntu Linux operating systems, with all instances launched from a patched and maintained Microsoft provided image. This image is then further hardened by using Packer and PowerShell scripts. This ensures consistency across all servers in the 1E platform and provides a base level of security. All server instances are then patched on a regular basis. All critical and security patches are applied weekly. All other patches are applied monthly. This includes all operating system and SQL patches.

Identity and access management

Each 1E platform instance is hosted within a separate Azure resource group and virtual network, with no shared access. Administration of the service is performed using both the Azure console and Azure API services for programmatic access.

Only essential staff within 1E have access to these services, with access configured using Azure Identity and Access Management (IAM). All logins to the console are required to have a secure pass phrase of at least twenty characters in addition to the use of multi factor authentication using Azure Active Directory and Microsoft Authenticator. Programmatic access to the Azure API is controlled through security principles stored within the 1E Azure Active Directory.

Each user has no direct access to any customer servers or data, and any such access must be requested through Microsoft Privileged Identity Management (PIM), is time limited, and must reference an open support ticket or authorized change control. All requests must be approved before being granted, and all approvals and subsequent elevation of privileges are audited. Privileges are automatically removed once the time limit is reached.

Passwords

1E requires National Institute of Standards and Technology (NIST) best practices for passwords and mandates the use of Single Sign-On (SSO) with multi-factor authentication.

Instance access

All access to server instances is performed using Microsoft Azure Bastion, which can only be used through the Azure portal, following a log on via Azure AD and MFA. User login credentials must be retrieved from Azure Key Vault storage for a particular instance. Access to the key vault can only be provided by Privileged Identity Management approval and is audited.

Security testing

The 1E platform undergoes periodic penetration testing, both application and infrastructure, via external approved companies at least annually.

The platform is continually tested for vulnerabilities via the use of automated tooling in the Microsoft Defender suite.

The web interface and APIs are also tested daily using Microsoft Azure External Attack Surface Monitoring (EASM).

Instance monitoring

1E’s cloud engineering team constantly monitors the availability and performance of each customer instance through Azure data explorer and DataDog, and any alerts are raised through PagerDuty.

All security events and metric data across all 1E resources are streamed in real time to 1E’s Security Information and Event Monitoring (SIEM) system which is an instance of Microsoft Sentinel. This is monitored 24/7/365 by 1E’s Security Operations Center(SOC), and incidents are raised directly with 1E’s security engineers.

Incident management

1E maintains multiple monitoring systems to detect and alert incidents. Incident severity is classified based upon customer impact and duration of incidents. 1E will notify affected customers of any security incident in line with our incident management plan.

Business continuity and disaster recovery

1E performs regular testing of our business continuity plans, and disaster recovery tests at least annually.

Recovery Time Objective (RTO) / Recovery Point Objective (RPO)

RTO = In the event of the VM being lost we will restore service by recovering the VM from backup within 4 hours.

RPO = The service is backed up every 24 hours at midnight local time.

Data backups

All backup data is encrypted in transit and at rest and written to geographically replicated data stores.

Third-party security

1E has a formal Third-party security review process for assessing third-party vendors at the point of engagement and annually thereafter. During this process we compare the classification of data stored and accessed by the third party with the data handling procedures outlined in our Information Classification policy. 1E's security team performs a technical assessment to determine if the vendor meets these requirements.

All third-party libraries used by our platform are scanned for vulnerabilities daily and updated appropriately.

Physical security

Office security

All 1E employees are required to use key cards to access our physical offices. Physical access is logged. Key cards are centrally managed by our business support team. All business technology infrastructure is secured in a separate climate-controlled room with fire suppression systems and limited access rights.

Clean desk policy

Employees are required to ensure that all restricted / confidential information (customer, vendor, employee, or intellectual property) is secure and stored in locked areas and out of sight when they are not in use or when the workspace is vacant. All such printed documentation must be stored and locked within secured containers. All computers must be (logically) locked when the workspace is unoccupied.

Data center security

Data center physical security for our hosting provider (Microsoft Azure) can be found here: https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security