ScalePad

WHITEPAPER

ScalePad Product Security

April, 2024

ScalePad

SUMMARY

ScalePad Partners

ScalePad considers its customers to be partners. They are a crucial part of ScalePad's success and are involved in our process to keep their data secure. For that reason, we will refer to our customers as partners in this document.

Security at ScalePad

ScalePad commits to vigorously securing data entrusted to us. The company was founded in 2015 with the pillars of security woven into its DNA. ScalePad was founded by a security expert who contributed to improving the security of products used by many companies, as well as the API security of many established Managed Services Providers.

Software security is an area of our business that requires continuous attention and innovation to ensure our practices are always up-to-date. If you have any concerns or questions about our security practices or a potential vulnerability, feel free to contact our support team so we can address them appropriately.

The following document provides information about how we secure our partners' data and how we can work together to improve the security of the ScalePad product suite.

For several years, we have worked to implement and improve many controls we consider crucial for the security lifecycle of the product and the company. They include:

- Business Continuity and Disaster Recovery Plan
- Incident Response and Management
- Internal and External Access Controls
- Secure Infrastructure
- Security Coding Practices
- Security Assessment by Third Party
- Patch Management, for both the product, infrastructure and third-party tools

Certified Security Practices

At ScalePad we believe that when we stop being better we stop being good. That's why we have obtained the SOC 2 Type II attestation and ISO 27001 certificate for our company and many of the apps in our SaaS ecosystem. Having both in place we are able to prove and share our efforts to offer secure services.

SOC 2

We chose SOC 2 because it demonstrates the commitment to data security and privacy. It is a widely recognized auditing standard that focuses on the controls and processes related to security, availability, processing integrity, confidentiality, and privacy of customer data. SOC 2 attestation showcases a company's adherence to rigorous standards. This provides assurance to clients and stakeholders regarding the company's data protection practices and security posture.

ISO 27001

We became ISO 27001 certified because it provides a comprehensive framework, promotes a security-conscious culture, supports incident management, facilitates continual improvement, and offers independent certification for demonstrating commitment to information security.

App Robustness and Usability

At ScalePad we understand that the usability of our products is as important as the privacy and security of your data. This is why we commit to offering you a quality product with great performance, user experience, and access.

We strive to provide 100% uptime of our suite of products to make sure users can access ScalePad services at any time. In fact, according to our most recent report, we provided 99.9% uptime in all regions of the world over the last year.

We have developed many infrastructure strategies to provide high uptime and scalability of our services to our partners. We have enabled a strong incident management process, allowing us to identify incidents and take action within minutes of their occurrence. Furthermore, we log, audit, communicate to internal teams and take corrective action to ensure we are aware of the scope of the incident and remediate it. Moreover, we also ensure that we understand the root cause of the incident to ensure that a similar incident does not happen again in the future.

PRODUCT DESCRIPTION

The ScalePad product suite allows partners to collect data from different sources, including third-party tools they use and publicly external web sources.

Lifecycle Manager

Lifecycle Manager applies quality checks, curation, aggregation, and deduplication of data through different algorithms providing partners with enriched analytic insights. Partners can develop business strategies based on that data for their clients directly in the app. At the same time they can provide them with protection or disposal services offered by ScalePad Marketplace (availability varies by region).

Lifecycle Insights

Lifecycle Insights makes it easy for vCIOs to deliver a best-in-class experience to their clients. Its templated assessments and budgeting tools help MSPs evaluate their clients' technology risk and manage action plans.

Backup Radar

Backup Radar is a backup monitoring platform delivering automated oversight of virtually any backup environment.
It surfaces gaps in any backup process by highlighting unreported backups, with intelligent ticketing automation that integrates seamlessly into an MSP's existing workflow.

ControlMap

Enabling MSPs to build and manage a multi-tenant compliance program, ControlMap simplifies the compliance journey. With turnkey tools, automation, and templates, MSPs and their clients can achieve compliance in weeks instead of months. ScalePad used ControlMap as an internal tool for our own SOC 2 and ISO 27001 compliance journey.

PRODUCT SUITE MANAGEMENT

In 2023, ScalePad extended the product suite with several more apps.

Managing a product suite developed and maintained by different product teams is not an easy task. The security practices and culture need to be consistent across all areas which is why we put a considerable effort into maintaining a secure product lifecycle.

It is our goal to provide a seamless user experience and to increase the security by reducing potential attack surface, we committed to developing a centralized login and billing experience for all our products.

AUTHENTICATION, AUTHORIZATION AND ACCOUNTING

ScalePad products allow partners to manage users with permissions to restrict and scope access to our products. Account administrators can at any time extend or revoke permissions through adding, removing and disabling users from the system. Administrative actions are recorded and visible to the account holders in an activity log.

ScalePad products allow the usage of multi-factor authentication (MFA) and we recommend to all our partners to activate and make use of that feature. Administrators can also enforce MFA, requiring all users to set up an MFA login the next time they log in.

We store all sensitive user credentials to our database using a secure salted hash with multiple iterations. Our MFA secrets are stored using the best storage practices described in the Data Storage section of this document.

INTERNAL IT SECURITY

Summary

At ScalePad we believe that, even if a product applies all best security practices, the data of our partners is only as secure as the internal operations of the company are. This is why we take our internal operations' security policies and controls very seriously

Controls

Different controls are implemented to ensure we have reasonable internal security measures to protect the data of partners.

- Employee Security Training and Certification
- Security, Identity and Access measures
- Security of premises
- Server room / data center / workplace security
- Hardware & Endpoint security
- Identification and authentication
- Data access and role based access control (RBAC)
- Access from outside the organization
- Regular testing, assessment and evaluation
- Measures for application suite data
- Data input & output validation
- Logging and Monitoring
- Pseudonymization and anonymization
- Encryption & Integrity
- Security of storage media
- Backup, BCM, DR and Availability
- Data destruction
- Outsourcing of tasks (processing by third parties)
- Security and protection
- Measures for data exchange
- Network security
- Message encryption
- Data protection measures
- Data subjects' rights
- Incident response and notification

INFRASTRUCTURE SECURITY

Endpoint Protection

All employees' hardware and software are monitored and protected by next-generation endpoint protection, offering rich software management and anti-malware functionality.

To further minimize the attack surface, we standardize the IT stack the ScalePad employees use. We also keep a close eye on the presence of shadow IT assets.

Hardware usage

Standardization

We believe that hardware standardization contributes to ease the maintenance and diminishes the exposure. We work exclusively with 3 OEMs to provide workstations to the entire organization.

Furthermore, the operating system (OS) and the OS version landscape is tightly controlled and allows us to efficiently manage patches and their overall lifecycle. This approach allows us to reduce the risk associated with modern OS ecosystems.

Network Devices

As defined in our RBAC controls, a very small and defined group of resources have access to network equipment such as routers, switches and firewalls. The same applies to any virtual equipment part of cloud provider VPCs.

Hardware MFA

Multiple Factor Authentication is crucial for the security access or ScalePad employees work environment. ScalePad has strict controls to ensure that every employee has a second factor enabled to authenticate to any service used in relation with ScalePad

Since there is nothing better to protect against online attack than to be offline, we have adopted hardware security devices (i.e. YubiKey) as the default second factor for all work environment resources at ScalePad.

Network and Cloud Provider

ScalePad has strict policies and controls to allow specific ScalePad resources to access our Cloud Service Provider and VPC. All direct access to the VPC is IP restricted and requires multi-factor authentication. Network rules then restrict access to and between specific resources.

All product infrastructure is located on Amazon Web Services (AWS) and/or Azure's cloud platform.

AWS supports more security standards and compliance certifications than any other offering, including PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171.

Along with AWS, Azure's hosting platform is one of the most secure and highly tested systems in existence. Their entire infrastructure is PCI-DSS certified. Azure services also maintain SOC 1, SOC 2 and SOC 3, ISO 27001, and 27017.

Secure Coding

Injection vulnerabilities, brute force exposure, weak encryption, unsecure storage and transmission are some of the most common vulnerabilities cyber criminals like to test and exploit. Most of those vulnerabilities can be prevented by having a properly trained team of developers following established coding practices focused on security.

At ScalePad we ensure all developers refresh their secure coding training on a regular basis. We also automate as much as we can of our security code by abstracting it at framework level and by integrating security testing components to our CI/CD pipelines.

All libraries and frameworks we use are permanently monitored, updates and patches are applied through an automated process with manual approval which ensures that we use the latest stable and tested versions.

THE TEAM

The ScalePad security team is composed of professionals with diverse backgrounds and areas of expertise. This strategy ensures the company provides a maximum of coverage based on different perspectives and specializations.

We are proud to have vast experience in the areas of SOC2, MSP industry, PCI-DSS, SaaS, security research, ISO27000, cloud security, privacy & data protection and many more.

The Security Committee

A lot of security issues can result from a chain reaction of several isolated department processes and without a proper cross-functional workflow it is very difficult to have a full 360 view of a company's security posture. At ScalePad we have a group of individuals from different departments committed to security who meet on a regular basis to share updates and discuss topics of interest.

DATA PROTECTION

Data Workflow

ScalePad products are designed to allow partners to integrate with third party tools. We communicate with the third parties to gather data that our algorithm analyzes, curates and aggregates to provide a set of rich insights to the partner. In some cases, we even enrich the data either by using AI techniques or by collecting publicly available data.

Partners can then decide to update some of the data in the third party tools with the new, cleaned data provided by ScalePad.

We do not share any of the partner data to any third party with the exception of service providers, such as warranties service providers. This happens exclusively upon a partner's request and consent to get the service

Partner information shared with ScalePad to synchronize data is secured as described in the Data Storage section. The transmission of data is secured as described in the Data Transmission section. The partner also controls any data synced and can decide to delete that data in the ScalePad product as described in the Data Controls section.

Data Backup and Disaster Recovery

All ScalePad databases and volumes are backed up on small incremental intervals varying from 5 minutes to 1 day. This allows us to have a RPO of 1 day and RTO of 1 hour on mostly all our services. Encrypted Backup Snapshots are taken on a daily basis and sent off site for maximum redundancy. We keep those backups for a period of 30 days.

ScalePad is configured for geographic redundancy and we test our disaster recovery plans on a regular basis

Data Storage

All sensitive data at rest is encrypted to ensure protection of the data. Some types of data are always encrypted such as (but not limited to): user credentials, third party integration credentials, authentication secrets and logs. We use Key Management Service to provide unique encryption keys for each partner and to ensure that their data can not be technically decrypted outside of the app VPC. We also use a Secret Provider to manage app access to the data. All data encryption operations are based on AES-256.

Data Controls

We believe that hosting our partners' data in our system is a privilege and we have a duty regarding security of that data. All unused data synchronized from third party integrations is automatically deleted from our system when a partner removes an integration from our system. We also commit to delete all other remaining data related to the account of partners upon request. Please note that certain data (i.e. data used for active warranties or accounting purposes) can not be removed as we are obligated by law to preserve it.

Data Transmission

All data transmission within services, clients and servers is done using a secure protocol. All services offered by ScalePad support and use TLS 1.3 (and also offer TLS 1.2 for compatibility). In certain cases (i.e. when a message is relayed through a system) we apply extra encryption on the payload.

DISCLAIMER

The information contained in this Product Security Whitepaper is for reference purposes only. Nothing contained in this document or relayed verbally to any customer or partner will be deemed to amend, modify or supersede the terms and conditions of any written agreement between such a customer or partner and ScalePad or the Partner.

ScalePad

www.scalepad.com | **Equipping Your MSP Adventure™**