ScienceLogic

ScienceLogic Global Security

Last updated April 2022

Contents

Executive Summary

As organizations become more digital in nature, securing the data becomes a top-of-mind priority given the cybersecurity challenges. ScienceLogic is committed to making the necessary investments in security and providing the transparency to gain the trust of our customer and partners.

This whitepaper is a part of that transparency and an overview of ScienceLogic's approach to security. In the pages that follow we outline the risks inherent in operating in today's hyper-connected world, and how ScienceLogic plays a role in helping organizations mitigate those risks. SL1 is not a security product; but it is a *secure* product. We want our customers and partners to know that we will never be the weak link in their security chain.

That is why we maintain a Trust Center of information and documentation to demonstrate our commitment to security. Transparency is vital to building and maintaining trust, and anyone who wants to see our security best practices, learn about our certifications, or understand how we architect our products can find the information they need there. That includes product security features, supported data security contexts, our role in the digital supply chain, and our corporate digital and physical security policies.

Disclaimer

ScienceLogic: Secure by Design

As hyperconnectivity becomes endemic to IT operations monitoring and management, and as technology and organizational siloes are dismantled, modern enterprises find that their IT ops and IT security domains are increasingly overlapped. The advent of AIOps, enabling real-time discovery of configuration items, has revealed the full scope of the environment that CTOs need to manage and that CISOs need to protect.

Threat actors are highly skilled and relentless in their desire to compromise digital enterprises. Whether motivated by monetary greed, ideology, a desire to acquire intellectual property, or simple maliciousness. If there is a weakness in a network, someone will attempt to exploit it. There are several common threat vectors that cybercriminals often use to gain illicit access to their victims' networks, including: Malware, Denial-of-Service, Social Engineering, Malicious Insiders among others.

Keeping your IT estate secure today requires an approach that starts with choosing components that are themselves architected to be secure, and then applying security tools to mitigate the gaps, risks, and threats that imperil operations. Unfortunately, most enterprises include a mix of legacy systems and configurations that were not designed, acquired, and deployed within the framework of a cybersecurity strategy. Nor is it realistic to expect that, in an era where on-demand services and self-service computing is the norm, that security will be a part of every decision to activate these assets.

Two philosophies have emerged to overcome the weaknesses inherent in every enterprise that hinder IT operations and IT security:

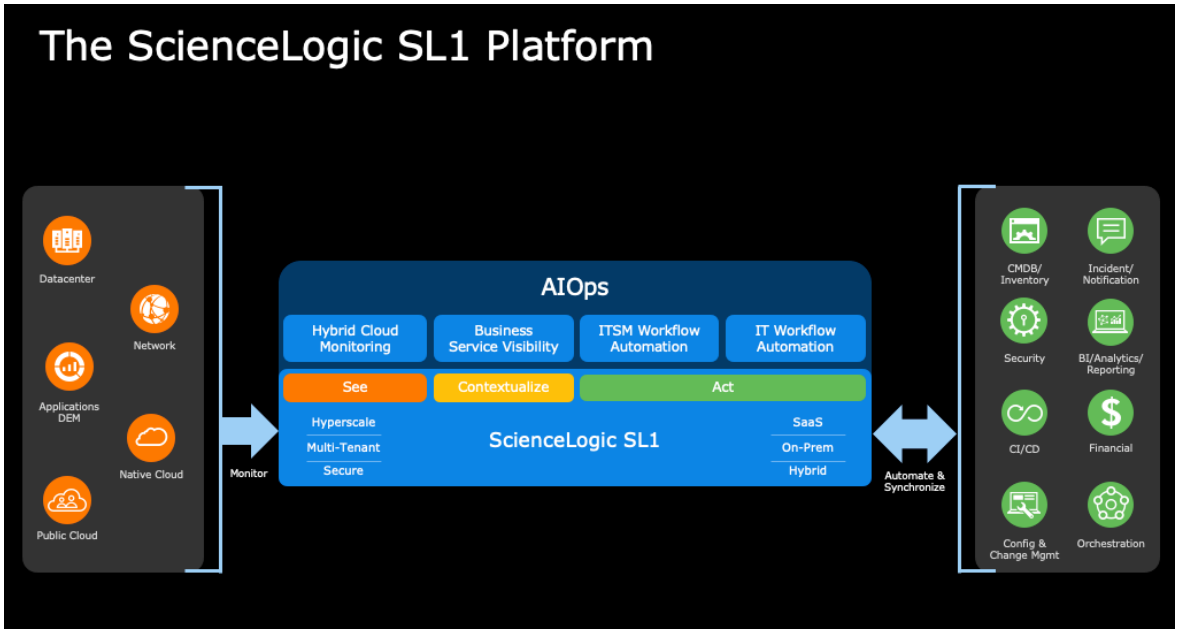
- **Secure-by-Design.** An approach to building technology products so that they are inherently secure in their construct and operation. This includes processes and elements like rigorous code testing during DevOps, use of strong passwords and authentication, seamless interoperability with complementary technologies, ongoing support, test and process automation, and compliance with security and privacy regulations.

- **Zero-Trust.** Defined by the National Institute of Standards and Technology (NIST) as "an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources." NIST defines **Zero Trust Architecture** as using "zero trust principles to plan industrial and enterprise infrastructure and workflows."

ScienceLogic's commitment to Secure-by-Design and Zero-Trust is embodied in the SL1 AIOps platform, ensuring that the deployment of our product will not introduce a vulnerability into your enterprise.

Solution Architecture

ScienceLogic delivers on the promise of AIOps by enabling analytics-driven automated operations through the SL1 platform.



Monitoring and Data Collection

The journey to AIOps begins with gathering a variety of data from a variety of data sources. SL1 uses a variety of agentless and agent-based mechanisms to collect data across your IT environment–whether it resides within a data center, cloud, hybrid, or multi-cloud environment.

Expandable Data Platform

SL1 can ingest a wide variety of data into the SL1 platform such as configuration, events, logs, performance, availability, etc. The SL1 data platform prepares and normalizes the data so that it can be shared across your IT ecosystem. All data is accessible through our UIs and APIs built to support scalable, microservice-based applications.

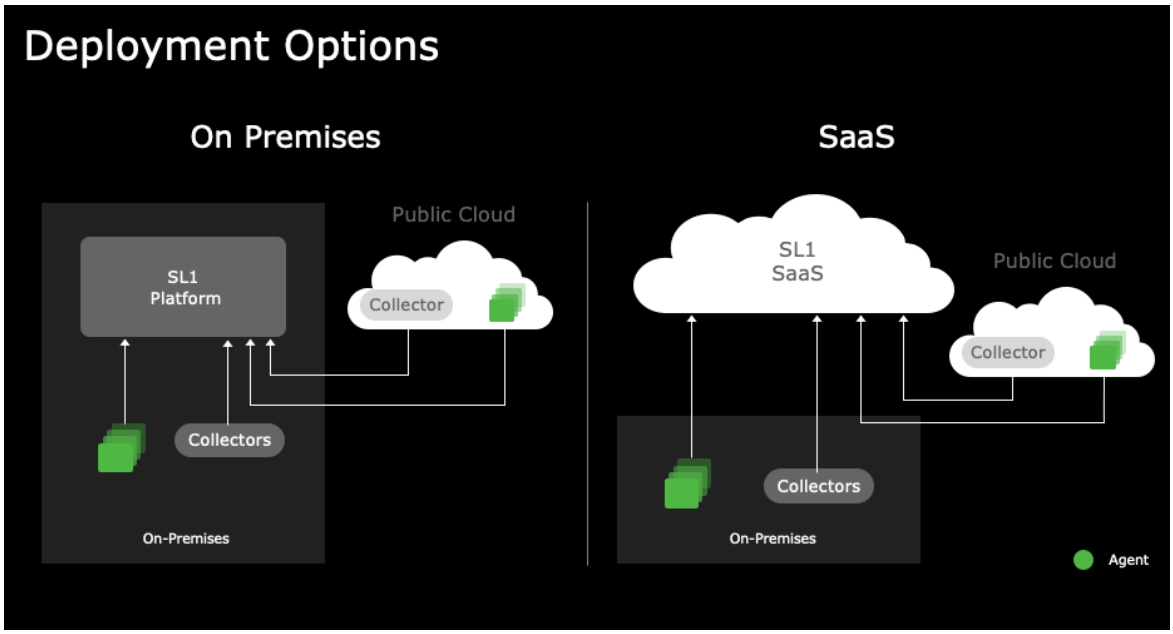
Business Services

Contextualization via full stack service topologies and AI/ML turn data into meaningful insights that align the business with IT. SL1's unique behavioral correlation of events, changes, and anomalies within a service context reveals the real-time health, availability, and risk of IT services on business outcomes.

IT Workflow Automation

SL1 automates data flows and workflows across multiple systems and tools including CMDB, Incident/Notification, Collaboration, Configuration & Change Management, DevOps, SecOps, BI/Analytics, Orchestration, and more.

The SL1 platform can be deployed on customer premises, customer-managed public clouds, or can be made available via a ScienceLogic-managed SaaS model. SaaS leverages Agents and Collectors, while on-prem deployments leverage Collectors only.



With SL1 SaaS, your SL1 instance is hosted, managed, and updated by ScienceLogic in public cloud – so your team can focus on unlocking the true value of SL1 to grow your core business. Customers can install SL1 Collectors and Agents to collect relevant and permitted data points around performance, configuration, availability, etc. from any combination of on-premises and cloud customer environments.

Resilient Architecture

Microservices-based SL1 SaaS application and its components (Compute, Storage and Database nodes) deployed in a highly redundant configuration across a cluster of data centers within the same geographic region ensuring high-availability.

Daily data backups to ensure swift failover and recovery.

Scale up or down to meet customer needs with no impact to SL1 performance.

Product Security Features

Deployment

Deployment Options

Choose your preferred deployment option: ScienceLogic-Managed SaaS, Customer-Managed On-Premises or Public Cloud. As your environment grows in scale, additional collectors can be deployed to cover additional infrastructure or geographic regions. Everything is centrally managed and accessed through a single web interface. Refer to Solution Architecture.

Government-specific Deployments

To meet U.S. Department of Defense (DoD) specifications, there is an option to install as a Military Unique Deployment (MUD) to comply with DoDIN APL (DoD Information Network Approved Products List) requirements. FedRAMP authorized solutions are available via our channel partners.

Authentication

Secure User Login

Customers can continue to adhere to their corporate policies via several authentication mechanisms such as configurable password requirements, SSO, Client Certificate & CAC Authentication. SL1 supports enterprise-grade single sign-on (SSO) integration options for SAML and Active Directory/LDAP, as well as local authentication using email address and a password. User logins can be secured by multi-factor authentication.

Authorization

Flexible Access and Permission Management

SL1 allows customers to manage granular, role-based access for users and groups locally or via Active Directory, LDAP, SAML, CAC, PIV, and multiple Identity Providers (IdPs) simultaneously.

Auditing

Audit Logs

View an audit trail of actions performed by users in the platform, including user logins and logouts.

Monitor for Illicit Behavior

Setup alerts and events for monitoring unwanted behavior such as illicit processes, changes in performance, domain records, open ports, etc.

Data Security

Data Segregation

Dedicated Instances

SL1 SaaS customers are deployed in their own dedicated instance of SL1 in ScienceLogic's public cloud environment, inherently ensuring data segregation between customers.

Multi-Tenancy

Data Access by "Organizations"

SL1's built-in multi-tenancy allows customers to organize data by 'Organizations' within the same instance of SL1. This adds another layer of logical separation of customer data and better role-based access control by department, region, line of business, etc.

Highly Secure Data Centers

Secure Data Handling

SL1 SaaS is deployed in AWS, which runs in ISO 27001 certified data centers. SL1 follows industry standards for encrypting data. Data collection and transmission from SL1 Agents, SL1 Collectors, or via platform integrations is secured with white-listing, SSH tunnels, PhoneHome methods (to limit firewall configuration changes), and 'Least Privileged' access to each customer environment. Stored data is protected with AES encryption. Data in transit is protected via Transport Layer Security (TLS). Customers who use Crowdstrike can install Crowdstrike Agents on ScienceLogic SL1 collectors for extended endpoint protection of SL1 devices on customer networks.

High-Availability Architecture

Resiliency and Redundancy

The microservices-based SL1 SaaS platform is designed to be highly redundant when deployed. The SL1 SaaS platform and its components (Compute, Storage, and Database nodes) are deployed in a highly redundant configuration across a cluster of data centers. The failure of one component automatically redirects traffic to a replica of the node instance within the redundant cluster, minimizing impact to the SL1 SaaS platform availability.

Incident Response Management

Continuous Vigilance

Performance, availability, and security events are constantly monitored, and alerts are sent to a dedicated incident response team. Security incidents can be reported online.

Software Supply Chain Security

Threat Modelling

Security Design Considerations

Security starts in the requirements and design phase. That's where our security architects help analyze potential attack vectors using threat modelling techniques before the actual implementation starts.

Secure Software Development Lifecycle Practices

Secure SDL

ScienceLogic enforces security best practices throughout the software development lifecycle such as OWASP 10 and peer code reviews. These best practices include:

- Automatically scanning for vulnerabilities and malware.
- Automatically running thousands of automated tests.
- Automatically signing assets and verify signatures during installation.
- Conducting manual penetration testing.
- Ensuring all artifacts are transferred and stored encrypted.
- Tracking changes via change management process.

Access to source code repositories is limited on both the network and the user level. Only authorized users can access code repositories and make changes to source code. Source code management systems are only accessible from within the ScienceLogic corporate network. Remote access to the ScienceLogic corporate network requires multi-factor authentication (MFA).

Software Upgrades

Secure Distribution

ScienceLogic implements several security controls and uses industry best practices to protect ScienceLogic software components like SL1, SL1 Agent and Collectors, and SL1 PowerPacks from malicious manipulation by attackers on the way to our customers' infrastructure.

All steps are fully automated, from source code being compiled to binaries, to the upload of the binaries to the AWS infrastructure where they are available for customers to download. No manual, error-prone steps are involved. Data in transit is encrypted using industry standards (TLS 1.2). Every storage location involving data at rest is encrypted as well.

All installation packages are scanned for malicious software and digitally signed before they're uploaded to AWS. The signatures are automatically verified during the update process on the customer infrastructure. If a verification fails (for example, due to installation package manipulation by an attacker), the update process is stopped. Learn more about our security features.

Internal and External Penetration Testing

Internal and Third-party Tests

On an ongoing basis, we test new and existing features. Our internal penetration tests are led by a certified penetration tester in our Security team. Our external penetration tests are performed bi-annually by independent security firms.

Vulnerability Scanning

On-going Scanning

Vulnerability scanning is performed regularly using static code analysis, dynamic runtime scans, network scans, and third-party component scans.

Corporate Security

Vendor Management

Onboarding and Ongoing Checks

- External vendor products that are leveraged within the SL1 platform, or leveraged for delivery of the platform are subjected to a detailed security assessment to guard against various attacks such as attempts to inject malicious code, hijack internal processes, etc.
- Vendors evaluated prior to onboarding and on a periodic bases or whenever there's a significant change in their cyber risk rating.
- All third-party libraries are evaluated for quality, performance, licensing, and vulnerabilities and require approval before being used.

Employee Awareness and Background Checks

Training & Awareness

ScienceLogic conducts annual employee and contractor security training with quarterly boosters and spot-training as needed. Training topics include Ransomware, Social Media, Credential Management, Impersonation Attack, Data Handling, Fraud, Phishing, Identity Theft, etc. Additionally, employees participate in role-specific security training.

Secure Access

Remote employees are required to log in using secure VPN with MFA.

Background Checks

New employees are put through rigorous background checks.

Privacy

Customer Data

Our privacy policy reflects our commitment to protecting personal data. To accommodate various privacy regulations such as General Data Protection Regulation (GDPR) or California Consumer Privacy Act (CCPA), SL1 collects a very limited amount of PII about users (full name, work email address, work phone number), and only what is required for authentication and user management. The specific requirements of the customer's organization regarding PII should be reviewed with the ScienceLogic delivery team to ensure the deployment meets the customer organization's security requirements. Read our Privacy Policy to learn more about the type of personal information we collect, how we store it, how we use it, and what rights individuals have and how they exercise them.

Compliance & Privacy

ScienceLogic understands that taking a holistic approach to securing every possible touchpoint for customers' data—from corporate and physical security, development best practices, securing the supply chain, to securing how data is transmitted to and stored within our environment—are key to earning your trust. As stewards of that data, we leverage industry-standard security, privacy, and compliance frameworks with supporting materials that attest to our capabilities. So, you can rest assured of a secure supply chain for your customers.

DoDIN APL

ScienceLogic is named on the U.S. Department of Defense Information Network Approved Products List (DoDIN APL). As the first complete end-to-end IT infrastructure monitoring solution ever to conform to the DoD's rigorous security and interoperability standards, government agencies can now purchase and implement ScienceLogic's IT infrastructure monitoring products on an expedited basis, and dramatically mitigate their network management challenges. As part of being listed on the APL, ScienceLogic complies with the requirement for timely patching of issues to maintain the operational availability, confidentiality, and integrity of customers' systems.

FIPS 140-2 Compliant Cryptography

Products that collect, store, transfer, share, and disseminate sensitive but unclassified (SBU) information must be certified for use in U.S. government departments (such as Department of Defense). A customer's SL1 configuration can be made FIPS 140-2 compliant. Specific requirements for FIPS 140-2 compliance should be reviewed between the customer and the ScienceLogic delivery team to ensure the deployment meets each customer organization's security requirement.

ISO 27001

SL1 SaaS is deployed in AWS which runs in ISO 27001 certified data centers.

SOC 2 Type II

ScienceLogic's On-Premises and SaaS deployment offerings are evaluated on an annual basis by a third party in a SOC 2 Type II examination. The product and service are evaluated against controls related to Security, Availability, Processing Integrity, and Confidentiality. A copy of this report may be shared with third parties once a non-disclosure agreement is in place.

Data Residency

We offer customers the ability to meet data residency requirements in multiple jurisdictions across the globe.

HIPAA

An SL1 Collector or SL1 Agent can be installed in environments where customers have certain security or regulatory restrictions, including with respect to Health Insurance Portability and Accountability Act (HIPAA). By default, SL1 does not collect regulated information such as protected patient information or data subject to export restrictions. Customers should review their security requirements with the ScienceLogic delivery team.

PCI/DSS

An SL1 Collector or SL1 Agent can be installed in environments where customers have certain security or regulatory restrictions, including with respect to Payment Card Industry Data Security Standards (PCI/DSS). By default, SL1 does not collect regulated information such as payment cardholder data or data subject to export restrictions. Customers should review their security requirements with the ScienceLogic delivery team.

Accessibility and WCAG / 508

ScienceLogic is committed to constantly improving the accessibility of our SL1 Platform and associated products to serve a wide variety of customers with varying accessibility needs. Our team of designers and developers implement best practices in accessible design and inclusive user experience. With each major release, we generate Accessibility Conformance Reports (completed VPATs) to document our products' conformance with accessibility standards outlined in the W3C's Web Content Accessibility Guidelines (WCAG), as well as Section 508 of the US Rehabilitation Act, an important amendment requiring Federal agencies' electronic and information technology to be accessible to people with disabilities.

For more details, you can review our Accessibility Conformance Reports:

- Section 508
- WCAG

CSA Star Level One

ScienceLogic is registered in the Cloud Security Alliance's (CSA) Security, Trust, and Assurance Registry. CSA provides a comprehensive framework for cloud provider trust and assurance, which is designed to recognize the varying assurance requirements and maturity levels of providers. ScienceLogic completed the security and privacy self-assessments based off the CSA's Cloud Controls Matrix required for CSA Star Level One.

Conclusion

ScienceLogic takes a holistic approach to securing our customer's trust. We engineer and deliver our products and services with a secure-by-design approach that prioritizes our customers' and partners' data security and privacy goals. And our entire organization operates with security best practices at every level of the operation–from employee recruiting to safe working practices, to securing how data is transmitted within our environment, as well as between ScienceLogic and customer environments.

ScienceLogic will continue to maintain the security and compliance certifications of our platform, with constant assessments, testing, and improvements to not only keep pace with the industry, but to lead by example.

To further understand how ScienceLogic addresses security and privacy, please feel free to visit our Trust Center or contact your ScienceLogic Account Executive.

About ScienceLogic

ScienceLogic enables companies to digitally transform themselves by removing the difficulty of managing complex, distributed IT services. Our IT infrastructure monitoring and AIOps platform (SL1) provides modern IT operations with actionable insights to predict and resolve problems faster in a digital, ephemeral world. The SL1 platform sees everything across cloud and distributed architectures, contextualizes data through relationship mapping, and acts on this insight through integration and automation. SL1 solves the challenges and complexities of today and provides the flexibility to face the IT monitoring and management needs of tomorrow. Trusted by thousands of organizations, ScienceLogic's technology was designed for the rigorous security requirements of United States Department of Defense, proven for scale by the world's largest service providers, and optimized for the needs of large enterprises.