

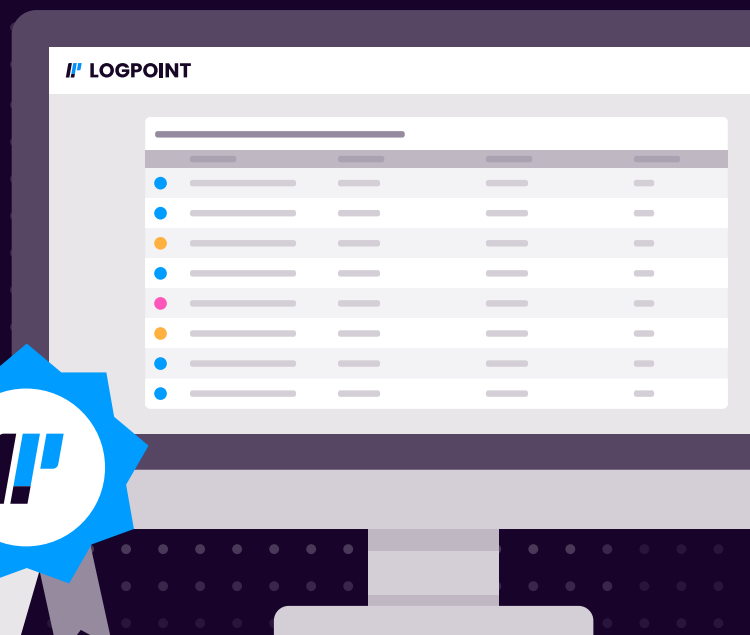


PRODUCT SECURITY

SOC 2 Type II and EAL 3+

Security of your information and data with Logpoint combines the rigor of SOC 2 Type II compliance with the advanced assurance of EAL 3+ certification, offering a dual-layered approach to cybersecurity. Our commitment to SOC 2 Type II standards guarantees the utmost confidentiality, integrity, and availability of your data, while EAL 3+ certification ensures our systems are robustly evaluated and prepared for emerging threats.

Our approach is not only about safeguarding your information and data but also about creating a resilient and adaptive security environment. This means you get a proactive, predictive security platform that keeps you one step ahead of potential threats. Let's redefine cybersecurity standards. Embrace a partnership where your data's security is our top priority, ensuring peace of mind in a world where digital safety is paramount.

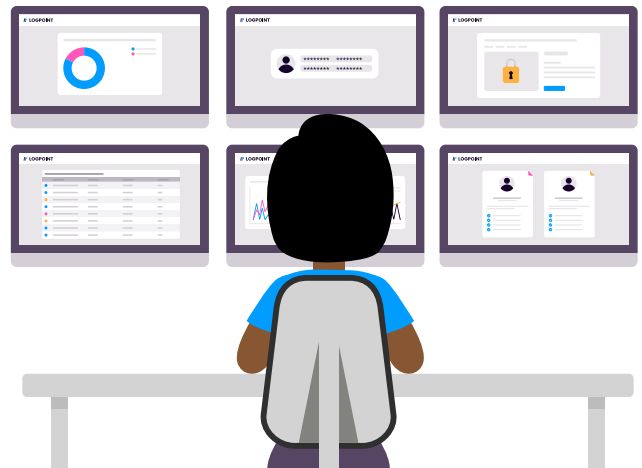


| We safeguard society in a digital world

EAL testing is rigorous

The Evaluation Assurance Level is a certification given to IT products or systems, providing assurance that the process of specification, implementation, and evaluation in the development has been conducted in a rigorous, standardized, and repeatable manner. The level of EAL certification depends on whether the product meets specific assurance requirements, which include:

- Design documentation
- Design analysis
- Functional testing
- Penetration testing



Common criteria

Common Criteria is the international standard (ISO/IEC 15408) for software assurance certification, recognized by 31 countries as the official third-party evaluation criteria for quality, security, and engineering practices.

Earning EAL 3+ certification is no easy task. It requires stringent testing, which ensures that you have maximum assurance of positive security engineering at the design and engineering stages. This is especially important in critical infrastructure, intelligence agencies, defense and other industries with exceptional requirements towards security.



Third-party testing eliminates bias

Independent testing organizations make the determination based on the completion of a Common Criteria security evaluation. Logpoint submitted its SIEM solution for certification to EAL assurance level 3+ to the Swedish Certification Body for IT Security (CSEC). Logpoint was EAL 3+ certified in 2015 and re-certified to EAL 3+ in 2021.

Trust is an invaluable piece to the network security puzzle. With its EAL 3+ certification, you can deploy Logpoint onto your network with the peace of mind that comes with using a solution that far exceeds security-testing standards of other SIEM solutions on the market.



A testament to trust at Logpoint

Building unwavering trust with advanced compliance

At Logpoint, our commitment to maintaining the highest standards of data security and privacy in our cloud services is demonstrated through our adherence to SOC 2 Type II criteria. This attestation reflects our dedication to building and sustaining trust with our customers and partners.

What SOC 2 Type II means for Logpoint customers

SOC 2 Type II is a rigorous, detailed audit that evaluates how cloud service providers safeguard data and how well those controls work over time. This means our cloud deployment of Converged SIEM provides maximum security with complete customer isolation, data encryption, customer data segregation, and role-based access. Rest assured, your information is safe with us.



Security

Protecting information and systems from unauthorized access, use, or modification to ensure their confidentiality, integrity, and availability. This includes network and application firewalls, two-factor authentication, and intrusion detection.



Availability

Ensuring the system, product, or service is available for operation and use as committed or agreed. This criterion focuses on performance monitoring, disaster recovery, and incident handling.



Processing integrity

Ensuring system processing is complete, valid, accurate, timely, and authorized. It may not be relevant for all service organizations, but it's crucial for those processing transactions or other data where processing integrity is vital.



Confidentiality

Protecting information designated as confidential from unauthorized disclosure. This criterion is crucial for companies that handle sensitive data like business plans, intellectual property, internal price lists, and other types of confidential information.



Privacy

Privacy is Paramount. We are committed to upholding your privacy rights. Our practices for handling personal data are in strict accordance with our privacy policies, assuring you of our unwavering commitment to confidentiality.

Beyond compliance

For us at Logpoint, SOC 2 compliance is just the beginning. We are continuously evolving our security practices to stay ahead of threats, ensuring that your data is protected with the most advanced cybersecurity solutions available. Partnering with us means choosing a cybersecurity ally dedicated to maintaining the highest standards of data security and privacy.