KernelCare

How KernelCare's Live Patching Software Can Promote SOC 2 Compliance & Certification

www.kernelcare.com

How KernelCare's Live Patching Software Can Promote SOC 2 Compliance & Certification

Increasingly, cloud computing companies that want to attract business need to demonstrate SOC 2 certification. This is your brief guide to what SOC 2 is, why it matters, and how KernelCare can help you with vulnerability management – a crucial component of SOC 2 compliance.

What is SOC 2?

SOC 2 has a long history that dates back to earlier incarnations from the seventies. But for the present, what matters is that SOC 2 is a set of reports developed by the American Institute of Certified Public Accountants (AICPA) that pertain to standards of security controls.

SOC2 is an audit framework that helps service organizations prove their capacity to secure customer data stored in the cloud. It is not a government-regulated certification, but something that organisations proactively seek out and acquire, largely for use as a sales tool. (Sometimes, certification might be performed at the request of a client.) SOC 2 gives companies a trusted way to verify their controls for protecting, securing and utilizing data.

During the SOC 2 certification process, a third-party CPA firm conducts a thorough audit of a company to assess their security posture as it pertains to five Trust Services Criteria. There are two types of SOC 2 audit: Type 1 focuses on a single point in time, and the more in-depth Type 2 focuses on a longer period, to assess the organisation's real-time (rather than static) functioning. Getting SOC 2 Type 2 certification, which is the gold standard, usually takes from six to 12 months. You can only complete a SOC 2 Type 2 audit after first completing a Type 1 audit.

Why should I care about SOC 2?

SOC 2 matters because many of the best and brightest companies will only partner with software vendors who are SOC 2 compliant. Getting your SOC 2 certification is fast becoming a necessary cost of doing business with top IT outfits. SOC 2 proves, via a trusted third party, that you adhere to strict policies to secure and protect the privacy of customer data. SOC 2 is a shorthand for showing that you are operating in a secure manner; thus it is a way to win business.

If you sell software to businesses, you're going to find more and more clients asking if you're SOC 2 compliant. When they outsource functions to cloud computing providers, the liability stays with them, so they want to know they can trust their partners. This is why SOC 2 is already a de facto requirement for any organization that wants to store any customer data in the cloud, ie. almost all SaaS or cloud service providers.

Additionally, despite being laborious and far from cheap, SOC 2 can be a great way to conduct a thorough internal review of your systems and processes, and learn where you are achieving high standards, and where you have room for improvement. A SOC 2 certification also means far fewer security RFIs during the sales process.

What does a SOC 2 audit/certification consist of?

The parameters of a SOC 2 audit are designed and defined by the organisation being audited. That might sound a little odd, but SOC 2 is aimed at an industry that is incredibly varied in terms of product design, tech stack, and so on. Audits have to be tailored to fit the organisation under scrutiny in order to do their job.

Because of this tailoring, SOC 2 criteria describe in broad terms what standards have to be met, but leave the how up to individual organizations to develop the appropriate controls. At the start of the process, the organisation and the auditor agree upon the criteria, ensuring that the targets to be met are challenging but achievable.

Then, over the course of the audit, the auditor looks at these self-determined controls to decide whether their design and operation is of a high enough standard to achieve SOC 2 certification in some or all of the five Trust Services Criteria. The auditor's work largely takes the form of various sorts of observation (of a system back up, for example) and inspection (of an organizational chart, for example).

Upon the completion of a SOC 2 audit, the registered public accounting firm issues a report stating whether the appropriate controls are in place to address each of the organization's selected Trust Services Criteria. There are no penalties or fines for failing to achieve certification(s) during an audit. An auditor will simply point out shortcomings, and help you resolve them for next time.

The 5 Trust Services Criteria of SOC 2

"SOC" stands for System and Organization Controls, and the SOC2 reports relate to five key areas of organisational health, dubbed Trust Services Criteria: Security, Availability, Processing Integrity, Confidentiality and Privacy.

A SOC 2 report can cover any or all of these five criteria. Which of the criteria an organization is attempting to be certified for is decided at the very beginning of the process, and agreed upon with the auditor. The full details of each Trust Services Criteria run to multiple paragraphs, but here are the short versions of how each criterion is fulfilled:

Security

The organisation must demonstrate that information and systems are protected against unauthorized access, and that all data is protected and kept private at all times. There must also be strong systems for detecting and dealing with threats and breaches.

Confidentiality

Any information designated as confidential must be kept private (if its access is limited in any way) throughout its life cycle at the organization. The information covered here especially pertains to non-personal information, like contracts and intellectual property.

Privacy

The organisation must protect all personal information (names, addresses, phone numbers) and handle this data in a way that accords with their stated privacy objectives, and which follows the AICPA's Generally Accepted Privacy Principles.

Availability

The organisation must show that information and systems are available for operation by everyone who needs it (including customers) when required.

Processing Integrity

System processing at the organisation must be complete, accurate and timely, and devoid of any errors or issues that could allow for unauthorized manipulation.

Remember: A SOC 2 report can cover one or three or five of these criteria. That's up to the organisation to decide.

How should I prepare for a SOC 2 certification?

- Budget accurately. Hiring an accredited auditor for up to a year isn't cheap. You'll also need significant staff time, perhaps consultants, and you'll need to cover the costs of remediating anything found by the auditor to be not up to scratch. All in all, you're looking at well into six figures.
- Form a good team. The people owning and leading the project should be skilled at moving and communicating within the whole office, and working to extended and evolving timelines. They should have good technical knowledge. For at least one person, the SOC 2 audit will be essentially a full-time position.
- Define your scope – that is, which Trust Services Criteria you are aiming for – carefully, and don't overshoot.
- Establish a good line of communication with your auditor, and don't be afraid to ask as many questions as you need to.

How KernelCare can help you pass your SOC 2 audit

The SOC 2 Trust Services Criteria are deeply concerned with systems. A good chunk of all web servers run on Linux, and Linux systems have high maintenance overhead because of regularly discovered vulnerabilities.

Linux is constantly providing patch updates to combat such vulnerabilities. 95% of software companies apply patch updates for the kernel – the core of the OS – by rebooting their servers. This commitment to regular rebooting is a flawed approach. Because rebooting is a hassle, off-lining websites, kernel patching is always delayed, for weeks or even months. This gap between patch issue and patch application means :

1. A security risk: Every day that a vulnerability is discovered but not patched is another day when you are at risk.
2. Noncompliance with insurance policies, most of which stipulate a maximum of around 30 days for kernel patching.

Delays in kernel patching might sound like a minor issue – but it is precisely the kind of systems-level flaw that a SOC 2 auditor will take a dim view of.

Because the kernel is at the very heart of the OS, rapid patching improves every element of your security posture. Here are just a few examples of how live patching can help you meet your SOC 2 TSC (Trust Services Criteria) requirements:

Security

TSC contains the requirement that "information and systems are protected against unauthorized access" and "unauthorized disclosure of information." Kernel vulnerabilities – such as the recent high-profile Zombieload – represent problems at the very heart of a computing system. Once an unauthorized attacker has exploited the kernel, they can get anywhere, and access everything, including the most sensitive customer data, for months or years. If you're avoiding or delaying patching because of reboots, then you're simply not as protected as you could be.

Availability

TSC requires that "information and systems are available for operation" and that "systems include controls to support accessibility for operation, monitoring, and maintenance." If you are performing any sort of web hosting, but you are regularly having to reboot, then your information and systems are regularly unavailable. There are frequent stretches of time where operation, monitoring and maintenance all go completely offline. With live patching, you can eliminate the downtime due to critical security patching, helping you achieve levels of uptime commonly measured in years.

Processing Integrity

TSC requires that "systems achieve the aim or purpose for which they exist and whether they perform their intended functions in an unimpaired manner, free from error, delay, omission, and unauthorized or inadvertent manipulation." If you are regularly rebooting in order to patch, then your systems are impaired in essentially all of these ways. Even if it's only brief, the systems are frequently delayed or vulnerable to errors. And because you are undoubtedly delaying your patches, they are open to exploitation by attackers wise to vulnerabilities.

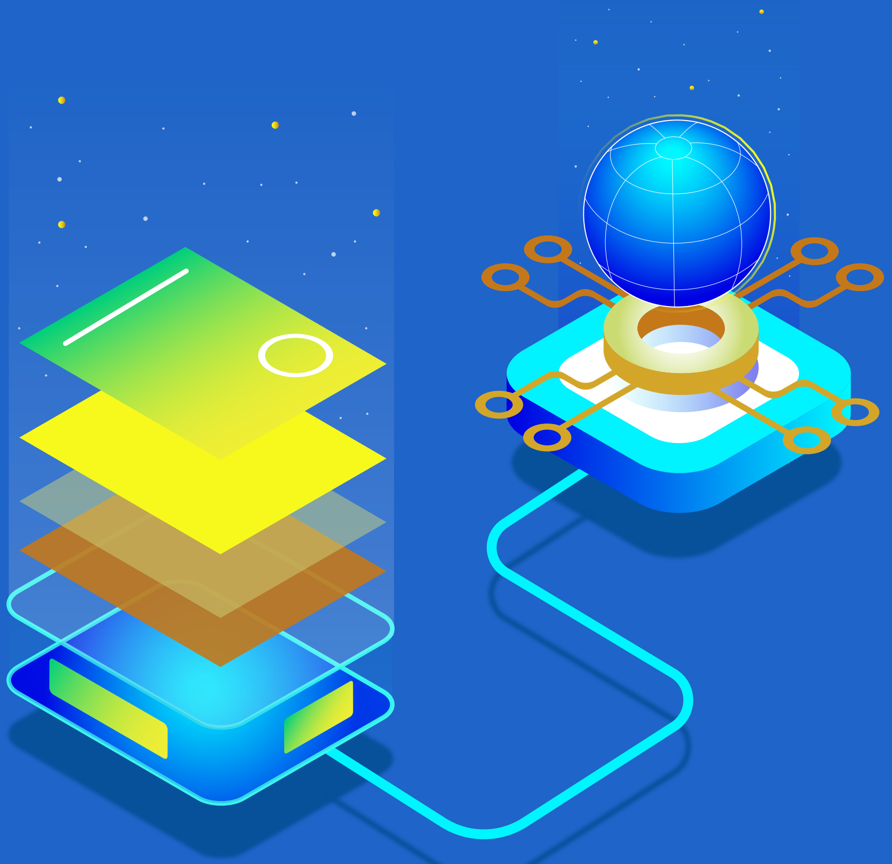
Confidentiality

TSC includes the straightforward requirement that "information designated as confidential is protected." This dovetails with the broader Security TSC: if you aren't applying kernel patches as soon as possible, then you are leaving yourself exposed to attackers who know all about new vulnerabilities, and are eager to steal confidential information.

Privacy

As with company data, personal data is exposed if your kernel isn't patched and up to date. What's more, point xiii of this TSC requires that "the entity monitors compliance to meet its objectives related to privacy." All companies will, of course, have an objective of honoring the terms of their insurance policies. In most cases, these require that patches are applied in around 30 days – which, if you're rebooting, almost definitely isn't happening. So, by keeping you insurance-compliant, live patching inherently fulfils the Privacy TSC for the system in focus.

Across every one of the five SOC 2 Trust Services Criteria, live kernel patching makes it easier to become compliant, and makes you more likely to sail through an audit. And over the coming years, SOC 2 compliance will be a must for any software provider that wants to keep attracting business.



To read the full SOC 2 documentationfrom which this information is sourced, head here. In terms of where KernelCare can help, pay particular attention to COSO Principle 7, COSO Principle 11, CC7.1, CC7.2, and CC7.4.

TO START USING KERNELCARE, AND GIVE YOURSELF A BETTER CHANCE OF SECURING SOC 2 CERTIFICATION, GO TO **KERNELCARE.COM**