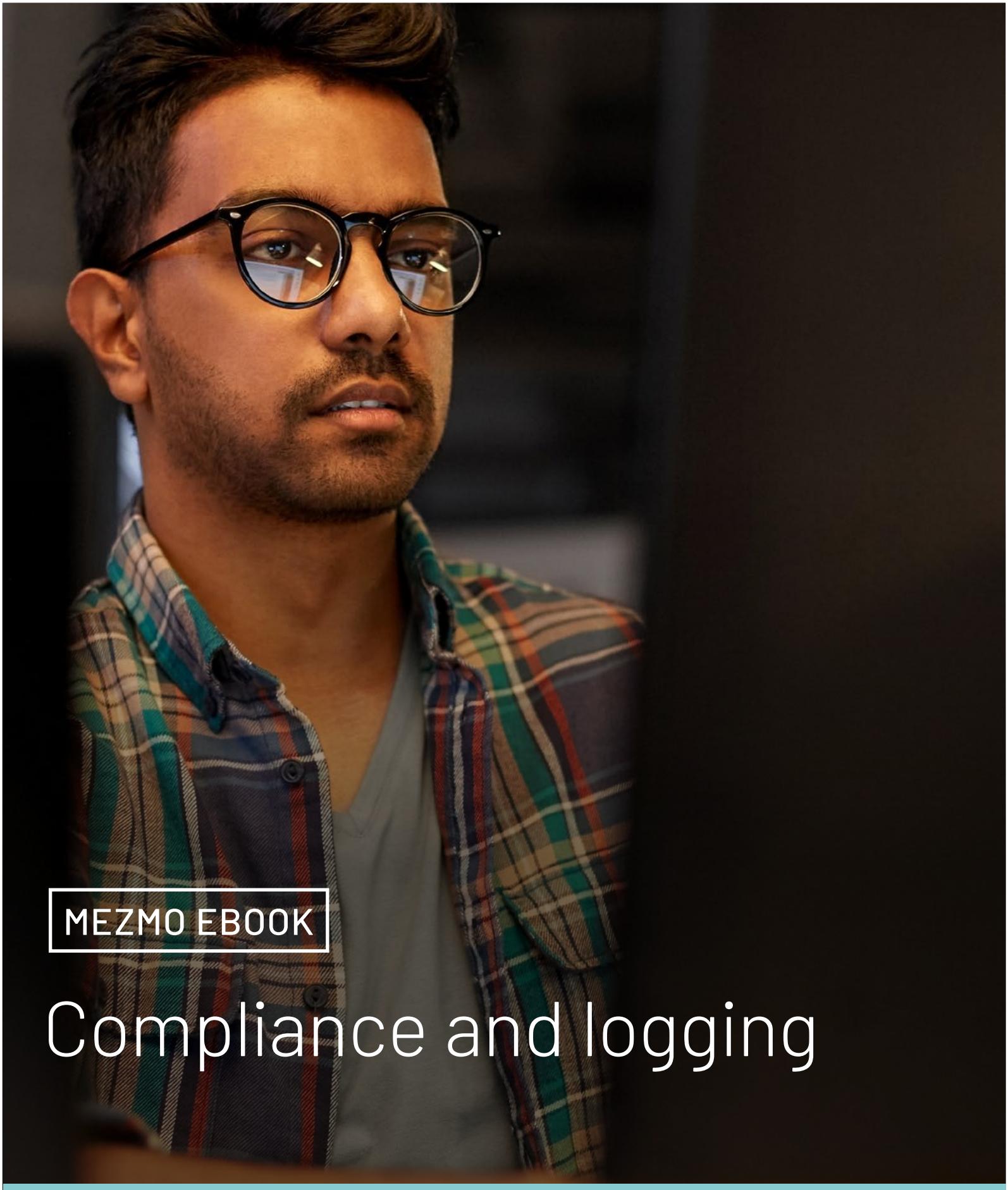


MEZMO EBOOK

Compliance and logging

This eBook will help IT professionals navigate today's complex compliance landscape. The following pages walk through common compliance challenges that organizations currently face and explain how to implement logging solutions that address those challenges.

mezmo

INTRODUCTION

Developers and IT teams have always relied on the data in log files to manage software performance and troubleshoot problems. Today, however, there's a critical new imperative behind logging: Compliance. Without effective logging measures in place for the applications and environments you deploy, it's nearly impossible to manage the compliance requirements to which your organization is subject.

This is not a new challenge, of course. Compliance frameworks have impacted the software ecosystem for decades. However, what's changing today is the number of compliance rules that developers and IT teams must adhere to, as well as the complexity of those rules. Today's organizations must contend with decades-old laws like HIPAA and new requirements like the GDPR, CCPA, and other novel compliance frameworks within various jurisdictions around the world.

Simultaneously, the widespread adoption of cloud-based, highly-distributed software architectures adds a new level of complexity to compliance. Gone are the days when most organizations could keep their data on-premises to simplify compliance policies. In an age when four-fifths of companies rely at least in part on cloud-based infrastructure, they must address compliance challenges related to third-party control over their workloads and the far-flung geographic dispersion of data and applications.

To make matters even more complicated, the abstraction of workloads via platforms like Kubernetes means there are more layers of software and infrastructure to manage to ensure compliance. It's no longer enough to only track operating system logs and application logs for signs of compliance risks; today's teams often juggle dozens of different types of logs and log formats generated by the many layers of their software stacks.

Logging alone won't guarantee full compliance; that also requires careful application design and software delivery processes that align with compliance rules. However, logging will go a long way toward empowering your team to stay ahead of the compliance requirements it needs to meet today, as well as whichever new rules may appear in the future.

TABLE OF CONTENTS

APPLICATION SECURITY AND COMPLIANCE THROUGH LOGGING

Every developer and IT professional can agree on the incredible value that log files provide when performing post-incident reviews; this holds true for identifying all types of application vulnerabilities, including those involving security and compliance shortfalls.

How Log Analysis Can Help Organizations Maintain Secure Applications

Data and context are absolute necessities to identify the source of any problem. In this case, the data are often log events. Log files usually consist of thousands of entries with each entry representing an individual event that has occurred within a system. Each event contains critical information about the action that was taken. A human being can only learn so much by simply scanning hundreds or thousands of log events in a text editor.

Through log analysis (often with the assistance of log analysis software), someone can contextualize log data to provide useful insights that can be leveraged to identify and resolve issues involving system security.

Log Analysis Reveals Patterns

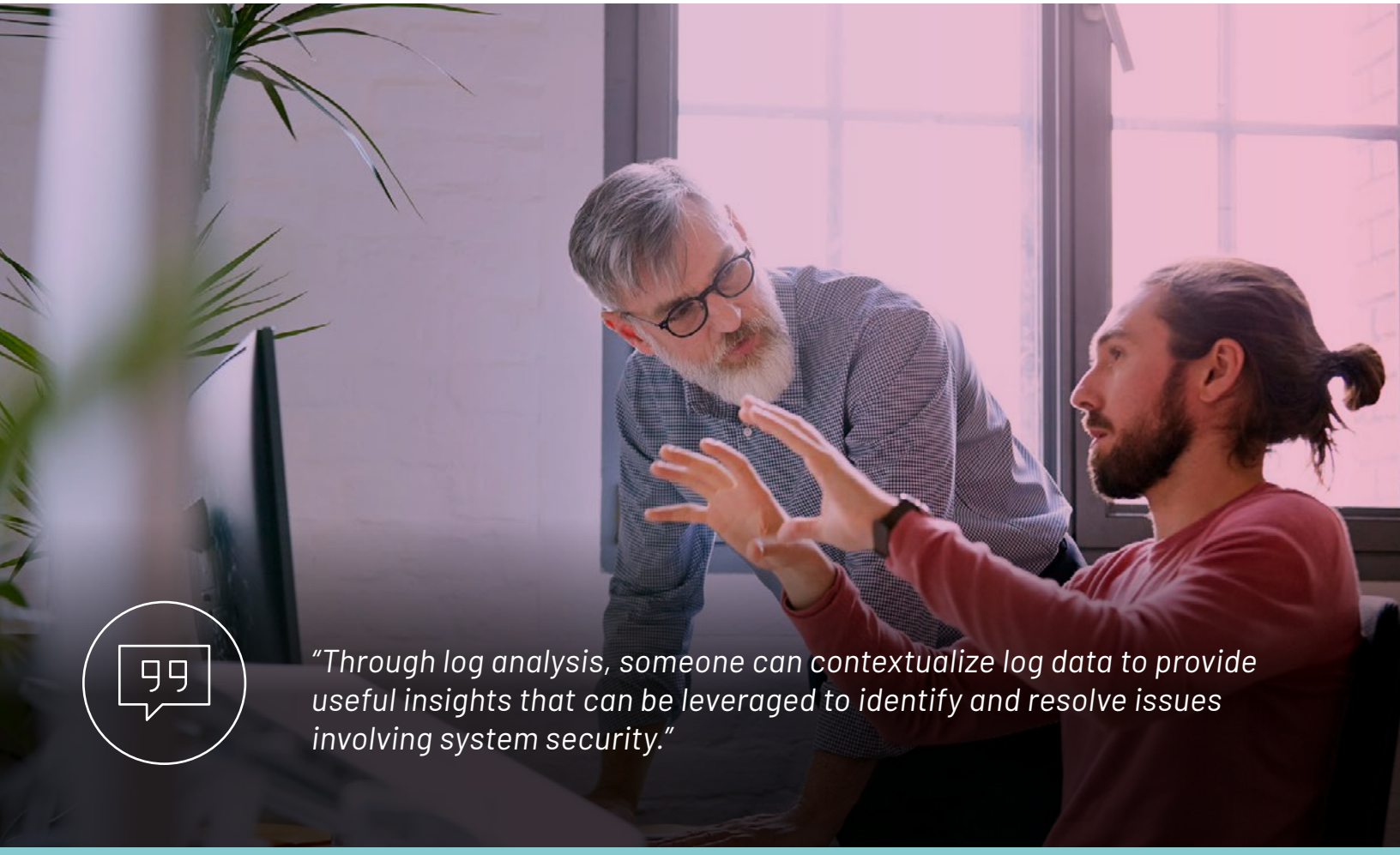
One way log analysis can prove useful for improving system security is its ability to help teams identify alarming patterns. For example, repeated failed login attempts, especially from geographic locations in which nobody should have access, would be a pattern that catches attention. A pattern of repeated requests, that are increasing in number, to a web application might indicate a pending DDoS attack. When a security incident occurs, the quick discovery of these trends can prove critical for closing the gap in system security before significant damage is done.

Modern Applications Require More Complex Tracing Functionality

Modern applications are often highly distributed, making it more difficult than ever to look at a log file and determine the path taken by a particular request. With modern log analysis tooling, organizations can enable their development teams to trace specific requests to identify a cause of an issue within their system quickly, including finding requests in which information was accessed in an unauthorized manner. Headers and full-functionality search systems help immensely in tracing events across one or more systems.

Centralized Logs and Enhanced Log Search Capabilities Help Identify Security Shortfalls

Log analysis tools like Mezmo allow organizations to centralize their logs from across their entire infrastructure. In addition, they provide more advanced search and query capabilities than you'll find in a simple text editor. Thus, it's easy to see how development teams can leverage this functionality to identify problematic entries in logs that account for all instances of their application. These issues include events that indicate severe security deficiencies such as successful cross-site scripting attempts or SQL injection attacks with the potential to lead to data breaches or malicious takeovers of user accounts.



"Through log analysis, someone can contextualize log data to provide useful insights that can be leveraged to identify and resolve issues involving system security."

The Role of Logging in Maintaining a Compliant Application

While system security is always important to maintain from a logical and moral standpoint, it is also critical that DevOps-oriented organizations maintain compliance with the standards set for the protection and usage of personal data. In some cases, this is impossible to do without logging.

Auditing User Activity in Applications that Utilize Sensitive Data

For example, let's consider the case of HIPAA compliance. Applications must be HIPAA compliant if they manage or utilize electronic protected health information (ePHI). For instance, let's say an organization has an application that requires the employees of a dental practice to access patient information. HIPAA dictates, in section § 164.312(b), that the organization must have audit controls in place to "record and examine activities in information systems that contain or use electronic protected health information", and it also requires that these logs must be "regularly reviewed" (section § 164.308(a)(1)(ii)(D)).

In other words, actions taken within these types of applications must be logged, and the logs should be regularly analyzed to help identify activity that is suspicious or simply out of the ordinary. Such activity may include multiple failed login attempts (indicating an effort to gain unauthorized access via another's user account), instances of an employee accessing their user account at peculiar times, and much more.

By securely logging application activity and efficiently analyzing these logs, an organization can ensure that its application remains in compliance with HIPAA requirements while putting itself in the best possible position to remediate any misuse of ePHI data in a time-efficient manner.

Staying in Compliance with a Log Retention Policy

Many standards not only require event and audit logging to be put in place but also that these logs be retained for a specified amount of time. HIPAA, for instance, states that documentation recording actions and activities be retained for six years (section § 164.316(b)(2)(i)). And audit logs serve to document actions taken by users and the systems themselves.

For applications that accept, process, store, or transmit credit card data, Payment Card Industry Data Security Standard (PCI DSS) dictate that an audit trail history must be available for one year (requirement 10.7).

Log entries provide an audit trail, and maintaining this audit trail for the time specified by applicable standards is critical to remaining prepared for a potential audit. These entries are also important when conducting reviews of security-related incidents that were not immediately identified by the organization. Log entries, like all other pieces of valuable incident data, help to remove the guesswork from the remediation process, ensuring that the fix thoroughly and permanently addresses the issue.

Mezmo offers plans for different data retention needs; including plans that retain 30 days of searchable log data. For longer retention, Mezmo provides an archiving service that automatically exports older logs to your preferred cloud storage service. In addition, Mezmo recommends to request a Business Associate Agreement (BAA) from your preferred cloud storage provider and secure your storage bucket before enabling archives.

The Effectiveness of Cloud-Based Log Management Solutions in Ensuring Compliance

Cloud-based log management solutions like Mezmo can drastically simplify the process of managing logs in a manner that is consistent with the various standards that are relevant to many of the applications being developed today.

Simplifying the Process for Log Review

As mentioned above, frameworks such as HIPAA and PCI DSS require regular analysis and review of various log data to ensure that the personal data being processed and stored by these applications is being adequately protected and appropriately utilized.

Cloud-based log management platforms improve this process through log centralization, alerting, and enhanced log search capabilities that provide DevOps-oriented organizations with all the tools they need to identify and remediate security-related issues in a time-efficient manner.

Maintaining Log Data Security

It's important to note that the log data itself should be stored and accessed in a secure manner. With Mezmo, logs are encrypted when they are stored, and granular access to these logs can be restricted using role-based access controls (RBAC).

For instance, when reviewing access or event logs for a specific application, it's likely that particular IT folks only require access to certain logs and that their access should be restricted to read-only. Mezmo helps restrict user access to only the appropriate levels by following the principle of least privilege.

Overall, a log management system can help you identify the gaps in your application's security and help you ensure compliance with various requirements out there. Whether you're looking to improve your security, get or maintain compliance, or otherwise

USING LOGS TO MEET SOC 2 & PCI DSS REQUIREMENTS FOR YOUR SAAS APPLICATION

If you offer a Software-as-a-Service (SaaS) application, meeting the American Institute of Certified Public Accountants (AICPA) SOC 2 auditing requirements and Payment Card Industry Data Security Standard (PCI DSS) compliance rules is critical for avoiding compliance or data privacy pitfalls. These requirements add another layer of complexity to your software management process, but they can be met if you have the right logging solution in place.

To explore how, let's look at how logging, SOC 2 auditing, and PCI DSS compliance go hand-in-hand for any company that offers a SaaS application.

SaaS, SOC 2, and PCI DSS

An application that is delivered using the Software-as-a-Service, or SaaS, model means that the application runs on the software provider's servers and that users access it remotely over the Internet. If the SaaS application collects any data point about users that is potentially personal or private in any way, that data ends up being stored on the software provider's servers due to the architectural structure of SaaS.

As a result, most companies that deploy SaaS applications are subject to certain reporting and compliance requirements involving personal data. Chief among those requirements is the SOC 2 audit report, an auditing process by which software providers must prove that they meet certain requirements when working with users' data.

A SOC 2 report addresses a service organization's controls that relate to operations and compliance, as outlined by the AICPA's Trust Services criteria in relation to availability, security, processing integrity, confidentiality, and privacy. A service organization may choose a SOC 2 report that focuses on any one or all five Trust Service principles and may choose either a Type I

or a Type II audit. SOC 2 is not a compliance regulation per se, but the ability to produce SOC 2 reports is a critical step for proving to regulators, customers, and other stakeholders that your company follows basic best practices when working with sensitive data.

Along similar lines, the Payment Card Industry Data Security Standard, or PCI DSS, is a standard that defines various rules that you must meet if you process payments in an application using any mainstream digital payment platform (such as a credit card). PCI DSS is designed to protect the security of payment data (like credit card numbers) and related personally identifiable information (PII).

In short, then, any SaaS application that collects data that may be considered personal, or that is associated with digital payments, must meet certain requirements defined by SOC2 and PCI DSS.

To be clear, those rules apply to various other types of applications, too; they're not focused just on SaaS applications. However, because SaaS applications by definition store user data on servers that are not controlled by users themselves, they present compliance challenges that would not necessarily occur in the context of applications that run locally and keep user data on users' personal devices.

How Logging Helps Meet SOC 2 and PCI DSS Requirements

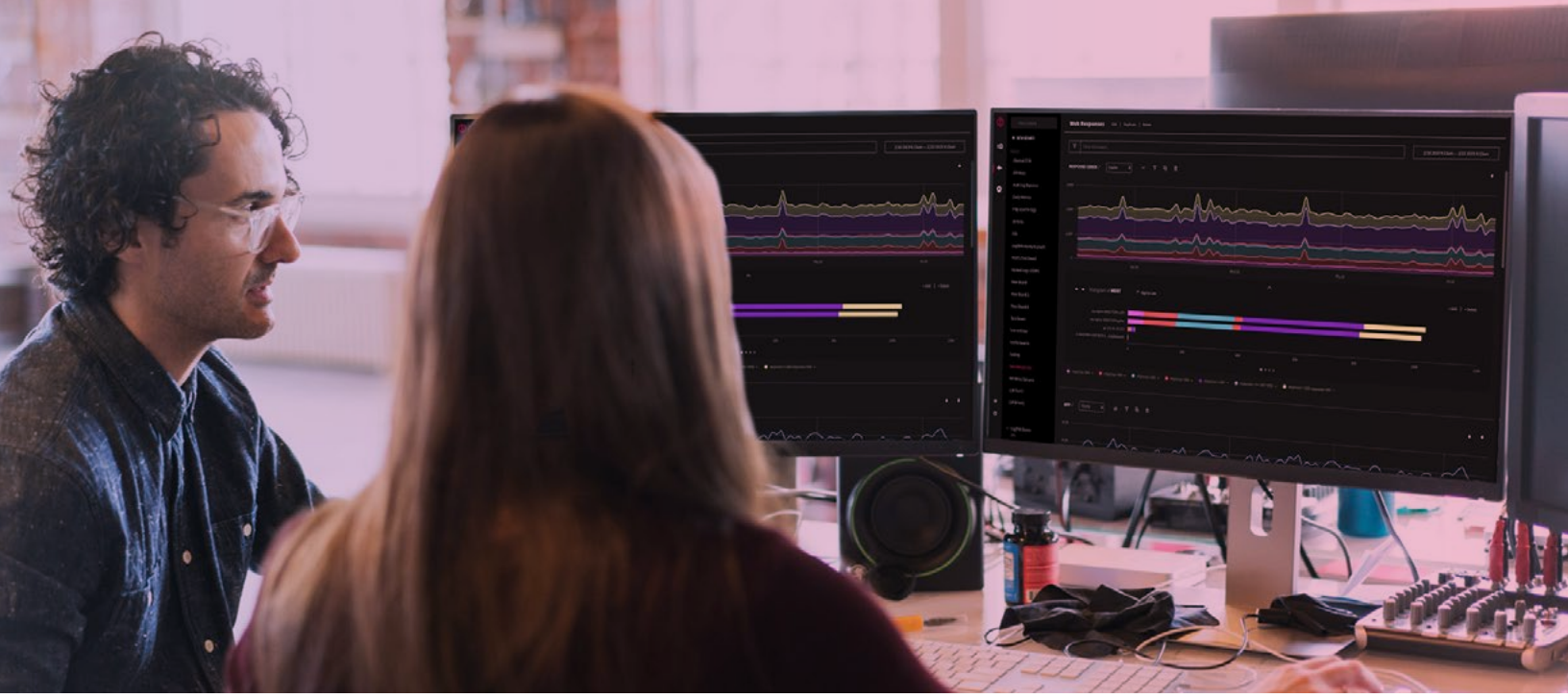
Having a logging solution in place is not a specific requirement of either SOC 2 or PCI DSS. However, it would be very hard to meet SOC 2 and PCI DSS rules without the visibility and management features that centralized logging provides.

Centralized log management solutions help meet SOC 2 and PCI DSS requirements in several ways. Although the two sets of rules are different in many ways, any team that wants to address them efficiently requires centralized logging.

Identifying and Alerting on Suspicious Activity

The security category of SOC 2, as well as PCI DSS requirements 10.6 and 10.8, mandate that organizations be able to identify and react to attempts to gain unauthorized access to protected data.

Logs alone may not guarantee that you can achieve these goals—SIEM platforms, firewalls, and various other security tools are also important resources;—but logs, especially authentication and access logs, do ensure that you have a way to gain comprehensive and systematic visibility into any abuse attempts on your SaaS application or the infrastructure that hosts it. The ability to centralize your logs and scan them for security-related events also enables you to generate reports that prove you handled security issues appropriately. Without logs, you would have no way to demonstrate your reaction to security intrusions.



Protecting Data Access

In addition to rules involving unauthorized access attempts, SOC 2 and especially PCI DSS include provisions regarding how legitimate stakeholders such as your employees or partners access and use sensitive data.

The main requirement here (spelled out in PCI DSS requirement 12, and more generally in the SOC 2 data availability and integrity rule) is that you need to have a policy in place to govern how legitimate access requests are handled. They don't dictate exactly what your policy entails, but they do require you to have reasonable controls in place.

Logging won't enable those controls, but it does provide the visibility you need to guarantee and to demonstrate to auditors that they are being followed. You don't want to wait for an external auditor to discover that your employees are not abiding by the rules you lay out regarding the management of payment processing information or customers' personal data. You want to be able to use logs to identify issues of non-compliance yourself before they turn into broader problems with external auditors or become known publicly and harm your reputation.

Securing Sensitive Data in Logs

Generally speaking, logs shouldn't contain user or payment data. However, there is always a chance that sensitive data like this may be stored inside a log accidentally. In that case, having the ability to scan all logs for strings that look like credit card numbers or personal names is a powerful way to remove sensitive information from logs. In addition, that ability helps you identify the source that placed the data in the logs in the first place so you can prevent sensitive information from being logged on a continual basis.

Alternatively, if for some reason you need to store sensitive data inside logs, the ability to aggregate all logs into a central location makes it easy to encrypt the logs and protect sensitive data inside them. You could also transform the logs to protect that sensitive data, which means, for example, replacing data like credit card numbers with an alternative string of data in order to "mask" the credit card number. Steps like these, which would be impossible to perform efficiently if your log data is spread across your infrastructure and cannot be easily centralized, are particularly important for meeting PCI DSS requirement 3.

Enabling Audits at Any Time

A key underlying principle of both SOC 2 and PCI DSS is that organizations should be able to demonstrate that they are following data protection best practices continuously, not just when it's time to do an audit.

Logs are the only way to demonstrate this kind of ongoing compliance. An audit report prepared at a single point in time demonstrates that you were compliant at that particular moment, but if you want to show that you were continuously compliant, you need the ability to gather and search through logging data stretching back into the past.

Likewise, the ability to rotate and securely archive logs is essential for ensuring that you have the historical log data that you need to demonstrate compliance at a certain point in the past. Without proper log management in place, you run the risk that older logs may be deleted or overwritten, depriving you of visibility into the past.

How to Build a Logging Compliance Solution

There are two basic ways to go about implementing a log management solution that empowers you to leverage logs effectively for meeting SaaS compliance requirements.

DIY Logging Using Open-Source Tools

The first is to build your own solution based on various tools that let you aggregate and analyze log data. The ELK stack, which is based on open-source tools, is a common approach.

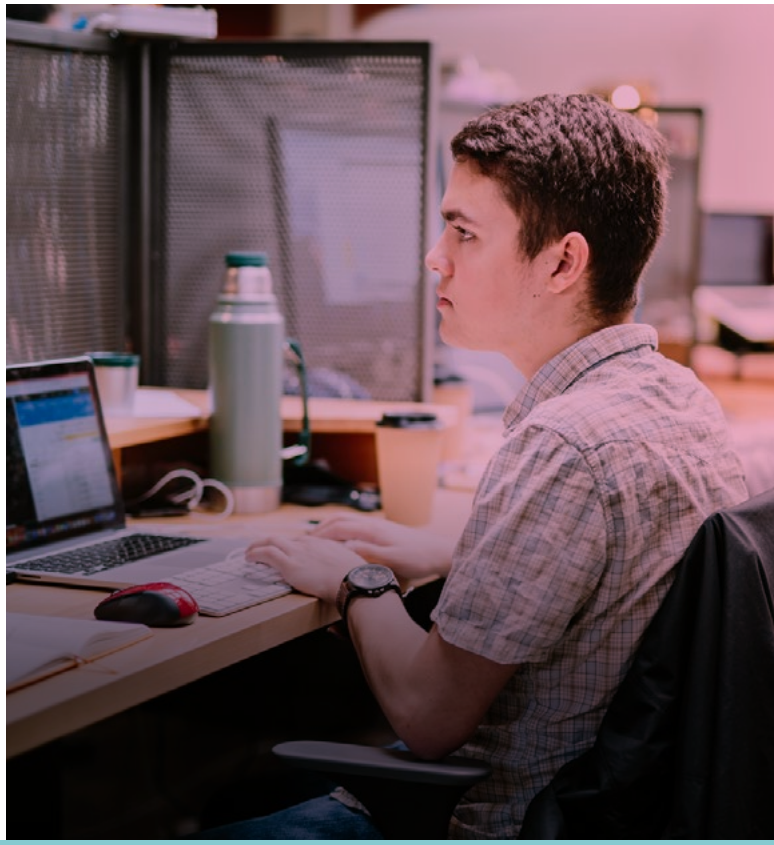
This strategy may work well enough if you have only a small amount of sensitive data to manage or if you have the extensive in-house development resources required to extend your open-source logging tools with compliance features that they don't include by default. However, for full-scale, streamlined compliance needs, solutions like the ELK stack come up short. Without custom changes, they usually don't guarantee the visibility you need to manage all compliance requirements for a SaaS application.

They also introduce the risk that the logging software itself is not compliant with whichever rules you need to meet—a common challenge when using open-source tools, which typically are not certified by external auditors to meet compliance requirements.

Turnkey, Compliant Logging

Alternatively, you can use a log management solution like Mezmo. Mezmo not only provides the features you need to gain holistic visibility into sensitive data within your applications without extensive configuration or customization, but it also provides a SaaS logging solution that is compliant with all major compliance frameworks.

That means that, when you use Mezmo to manage your logs, you can be confident that LogDNA's own software and servers store and process logs in ways that protect the privacy of your users and help you meet SOC 2 and PCI DSS rules.



THE IMPORTANCE OF RBAC AND SAML FOR SECURITY AND COMPLIANCE

Whenever the topic of compliance comes up in conversation, most people automatically think of regulations like PCI-DSS, HIPAA, SOC 2, and even GDPR. While compliance with these regulations is extremely important for your organization's security profile and reputation, your ability to comply with them hinges on your ability to control which users have access to specific systems and to monitor when they access them.

From Access Control Lists to Role-Based Access Control

As soon as computers became multiuser, there was an obvious need to be able to control and track who could log in to what. Access control lists (ACLs) were used to do just that—if you weren't on the list, then you couldn't get in. But while ACLs are very good at handling authentication, they don't limit what users can do once they are authenticated.

About thirty years ago, we solved this problem by introducing role-based access control (RBAC), which enables subsystems to control access based upon assigned roles.

To illustrate why these kinds of controls matter, let's imagine that we have three employees who work for a medical clinic: Vijay works in the billing department, Michelle is a nurse, and Noelle is a security auditor. All three of these users have access to the patient tracking system, but since they have access for different reasons, they have access to different information. For example, when Vijay logs in, he can see a list of every patient in the system, the date they were admitted, and a code for every procedure performed on them (such as X-rays), but he cannot see the results of these procedures or any notes that medical personnel put in the system. Michelle, on the other hand, has access to these notes and the results of the procedures, but she can only see this information for current patients, and

"Your ability to comply with regulations like PCI-DSS, HIPAA, SOC 2, and even GDPR, hinges on your ability to control which users have access to specific systems and to monitor when they access them."

she cannot access it after the patient is discharged. When Noelle logs in, she can see a list of every user in the system, when they were added, and when they accessed patient records, but she cannot see any details about the patients themselves.

Now, let's take a closer look at the role of our hypothetical security auditor, Noelle. While she can see information about who accessed what on demand (for example, she can see that Vijay accessed the code for a patient's X-ray procedure while Michelle looked at the results of the X-ray), this is not scalable or very reactive. But what if this information was compiled into a log and loaded into a centralized logging system? Not only would this allow for better scalability (for example, adding more clinics without adding additional security auditors), it would also allow for automated reporting on potential security issues such as a nurse attempting to access patient records after hours or attempting to access the records of a patient from another clinic. Both of these events could be signs that staff accounts have been hacked, and the earlier it's discovered, the better the chance of preventing a data leak that could ruin the reputation of the clinic and the wider organization.

For this and a host of other reasons, both RBAC and centralized logging are key for successful service delivery.

Your Service Providers Use Identities, Too

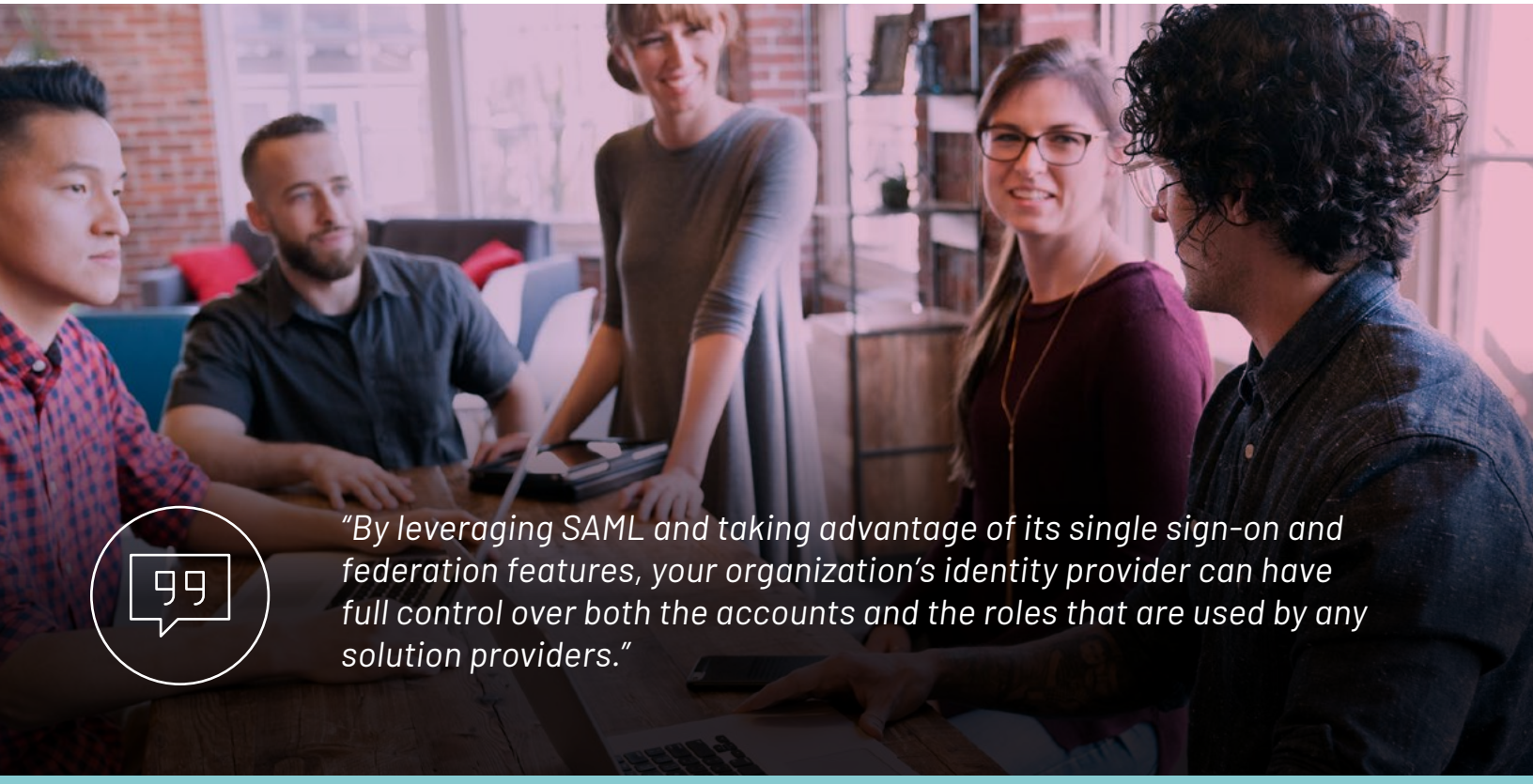
Almost every business uses external services as part of its day-to-day operations for everything from HR to CRM Salesforce. All of these third-party service providers have their own identity systems that rely on RBAC, too. The big, enterprise-class vendors have the ability to leverage Security Assertion Markup Language (SAML) as part of

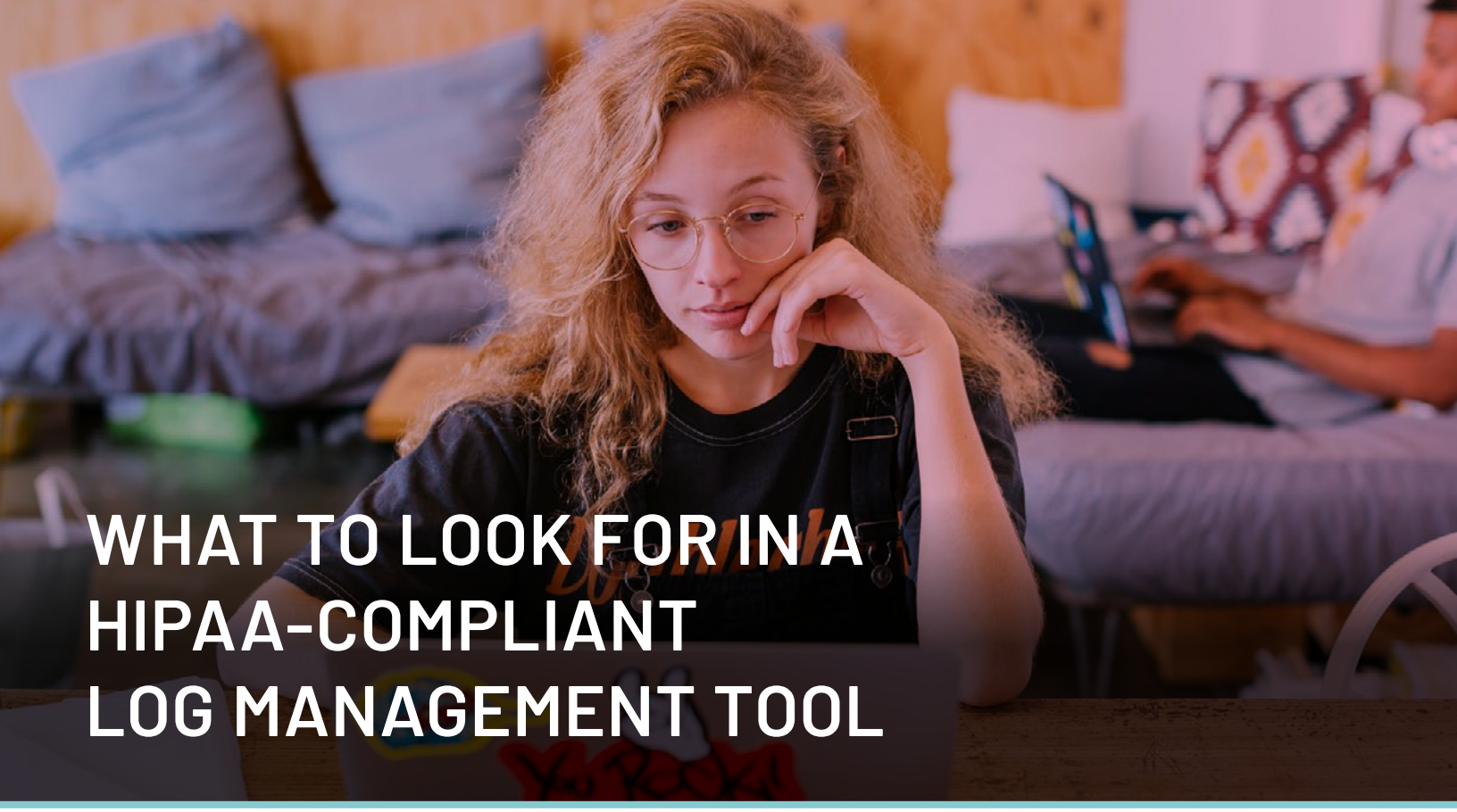
their authentication and authorization process. SAML allows them to leverage existing identities and roles within your organization to control access to your data that's stored in their systems.

The basic process is quick and fairly seamless:

1) A client connects to the service provider.
2) The service provider redirects to the client organization's identity provider with a basic SAML token (such as an Active Directory).
3) The identity provider recognizes the SAML token and asks the client for their login credentials.
4) After a successful login, the identity provider redirects the client back to the service provider with a fully populated SAML token, which can include client information and authorized roles.
5) The service provider receives the SAML token and processes its data; then, it grants the client access according to the roles that it has been assigned.
6) The client uses the service provider.

By leveraging SAML and taking advantage of its single sign-on and federation features, your organization's identity provider can have full control over both the accounts and the roles that are used by any solution providers. This use allows existing processes to handle account management, and any centralized logging that you have in place will gain immediate visibility into logins and access requests on those external systems. Many third-party services also allow events and other activities to be exported as logs, either in real-time or as a scheduled activity. These logs can then be incorporated securely into your centralized logging to improve visibility into all ongoing activities across your organization.





WHAT TO LOOK FOR IN A HIPAA-COMPLIANT LOG MANAGEMENT TOOL

Most modern log management solutions claim to be HIPAA-compliant, and indeed, most logging tools can be used in a HIPAA-compliant way—provided that you spend enough time configuring them to meet HIPAA rules.

That does not mean, however, that all logging solutions are created equal when it comes to HIPAA. The extent to which logging tools offer out-of-the-box support for HIPAA compliance varies widely depending on the specific logging features that the tools offer and how easy those features are to implement.

Here's a look at which log management features are most important for meeting HIPAA compliance rules.

HIPAA and Logging: A Brief Overview

Overall, HIPAA is a rather vague framework. When it comes to logging, however, HIPAA imposes several fairly specific requirements:

- Organizations must monitor events that involve access or updates to Protected Health Information, or ePHI.
- Organizations must have "audit controls" in place to "record and examine" activity on systems that store ePHI.
- Organizations must "regularly review" records of activity on systems that contain ePHI.

These rules are spelled out in HIPAA sections 164.308(a)(5)(ii)(C), 164.312(b), and 164.308(a)(1)(ii)(D), respectively.

HIPAA doesn't specify that logs in particular have to be used to record and track the information described above. However, it's hard to imagine how else you would systematically record and audit these events without logs. For most organizations that work with ePHI, then, the ability to maintain logs that record ePHI access events, as well as enable audits of access to ePHI data and the systems that store it, is essential.

Making the Most of HIPAA Logs

You can create the HIPAA logs described above in any way. HIPAA is not specific about how the data has to be structured. However, when it comes to managing HIPAA log data, there are several specific considerations to bear in mind.

HIPAA Log Retention

Chief among them is log retention and log rotation. HIPAA generally requires that event, access, and audit data remain available for six years after it is generated. For that reason, it's important to be able to configure log management tools so that historic log data can be maintained for the HIPAA retention period.

Mezmo offers plans for different needs, including plans that retain 30 days of searchable log data. For longer retention, Mezmo provides an archiving service that automatically exports older logs to your preferred cloud storage service. In addition, Mezmo recommends to request a Business Associate Agreement (BAA) from your preferred cloud storage provider and secure your storage bucket before enabling archives.

HIPAA-Compliant Log Storage

The rules surrounding the storage of data that is subject to HIPAA rules are complicated. When it comes to logs—which generally shouldn't contain ePHI, but could—the simplest way to meet those requirements is to use a SaaS log management solution that stores logs on infrastructure that is certified for HIPAA compliance. That way, you can outsource your HIPAA storage challenges to your log management provider.

Of course, you may prefer to store log data on your own infrastructure if you are confident in your ability to meet HIPAA requirements yourself. You should thus look for a log management solution that offers the flexibility to run on any cloud as well as to use a SaaS model.

Business Associate Agreement

Likewise, look for a log management provider that will sign a Business Associate Agreement, or BAA, with you. Under HIPAA, a BAA is required if you work with a third-party organization that manages ePHI on your behalf. Because logs may contain ePHI (and even if they don't,

they typically contain sensitive data related to systems that store ePHI, which in itself presents a potential security risk), having a BAA in place with your log management provider helps to reduce potential HIPAA compliance risks. It also formalizes the log management provider's guarantee to store and manage your log data in a HIPAA-compliant way.

Use Encryption

When sending logs to your log management provider, use HTTPS or TLS encryption techniques to encrypt your logs in transit, or else your logs will be sent in plain text, making them trivial to intercept by a malicious third party.

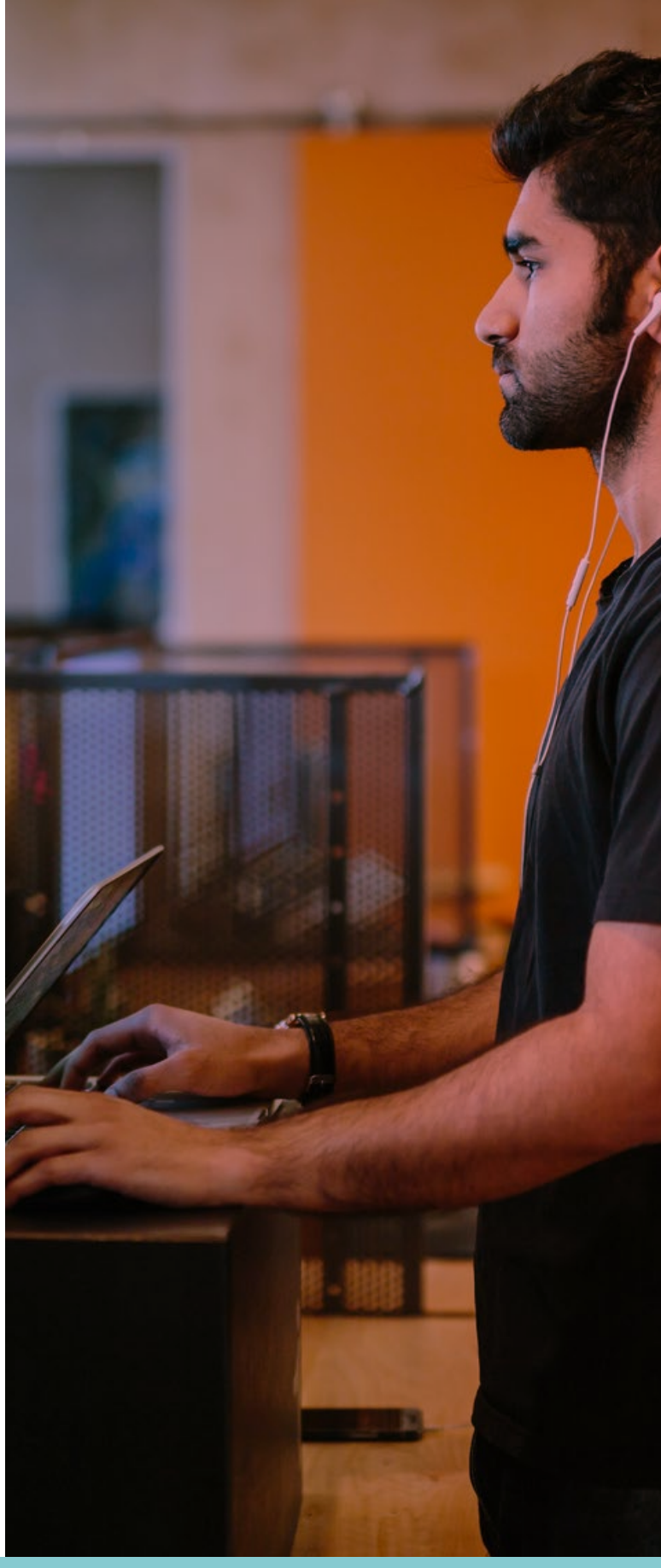
Encryption is enabled by default in the Mezmo agent and within official code libraries. Mezmo also encrypts your logs when storing them and only allows access to the web application over secure HTTPS. If you are archiving your logs, encrypt your storage bucket before enabling the archiving process.

Control Access to Log Data

Whether or not your logs contain ePHI, the data they store about your infrastructure could give attackers the information they need to gain unauthorized access to your systems and therefore to ePHI.

To mitigate this risk, your log management solution should allow you to control, in a granular way, who in your organization has access to logs. You shouldn't need to give all of your engineers unfettered access to all logs; instead, each engineer should be able to access logs only for the specific systems they maintain.

Mezmo lets you set granular permissions using role-based access control (RBAC). You can restrict each user's ability to view, create, or modify Mezmo resources, as well as restrict their access to logs based on source or content.



Identify Logging Failures

Logs only help you meet HIPAA auditing requirements if the logs actually exist and are accurate. To guard against the risk that some HIPAA-relevant data is not logged properly due to an issue like a log agent failure or the exhaustion of log storage space, choose a log management tool that allows you to configure alerts that will notify you when something goes wrong in your logging routine. You don't want to wait for an audit to learn that you haven't actually logged all the data you need to meet HIPAA requirements due to a technical failure.

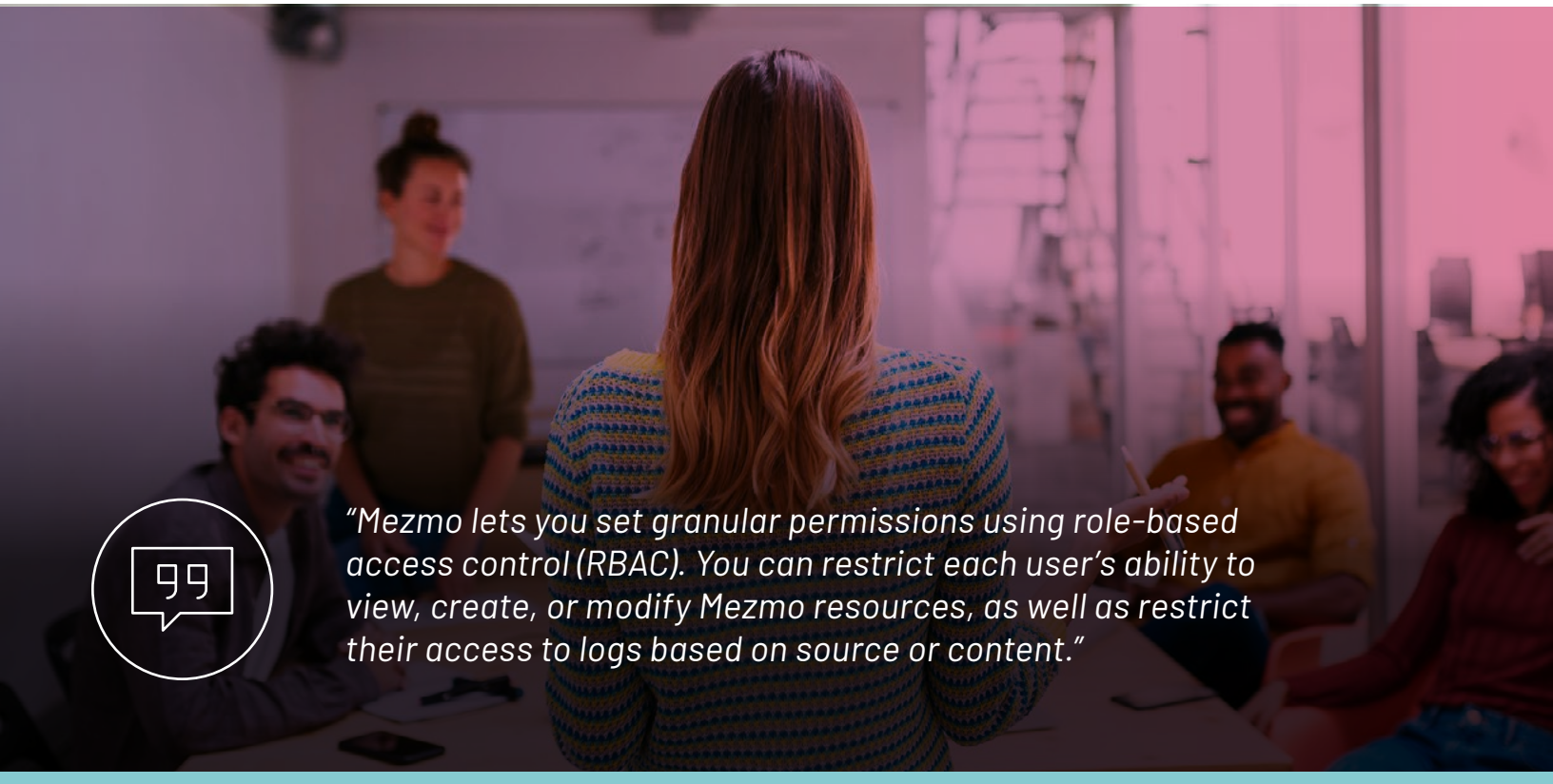
Chapter Summary

In short, there are lots of logging solutions available, and all of them can manage logs that store HIPAA-related data. But not all of them offer the rich set of features that you need for meeting HIPAA compliance requirements easily.

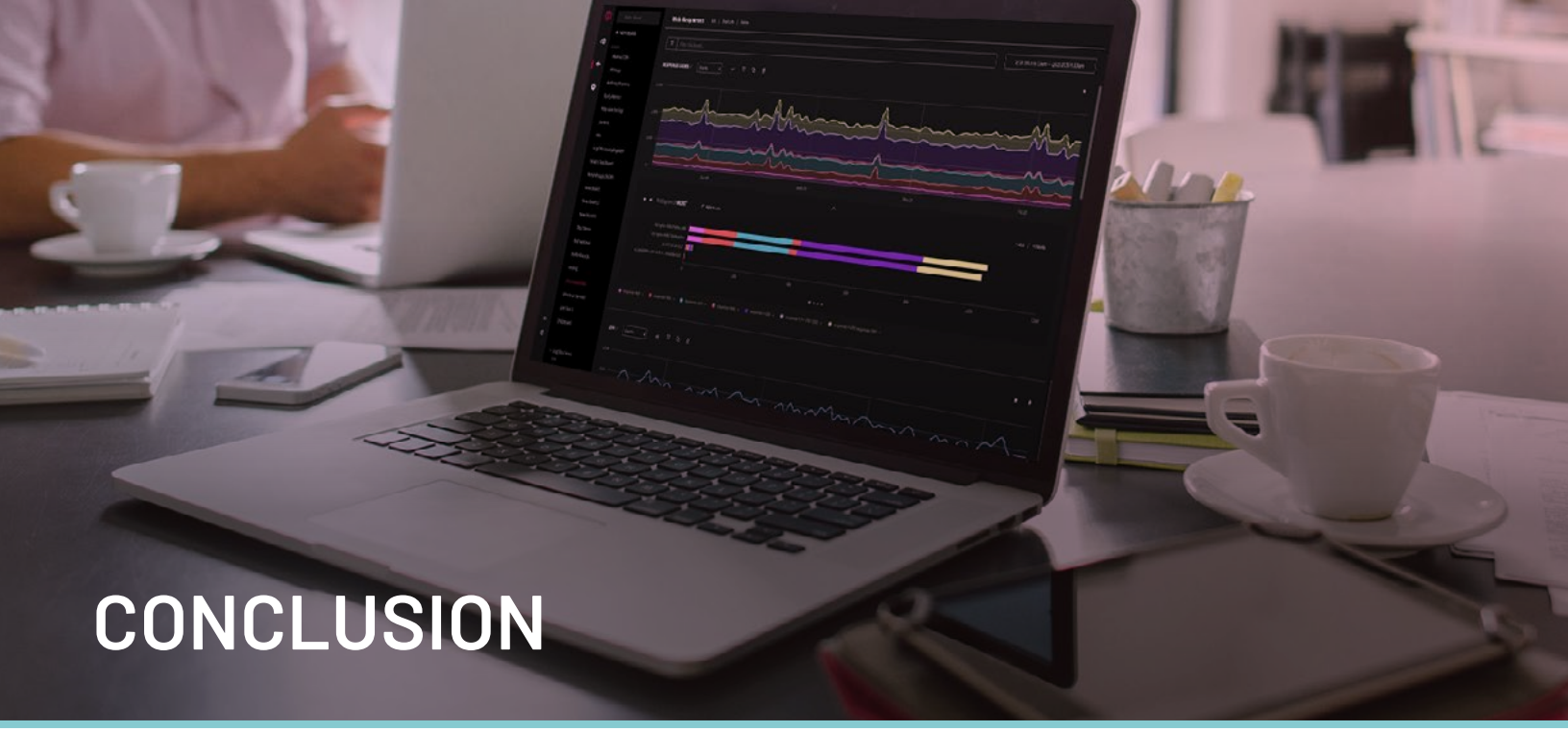
Log management tools that natively lack features for restricting access to log data, alerting you to logging failures, or storing logs in a HIPAA-compliant way will require you to implement workarounds or custom extensions to meet HIPAA rules. Likewise, if your log management provider can't sign a BAA or guarantee compliance of its own systems with HIPAA requirements, you face an uphill battle in using logs to reinforce your HIPAA compliance.

With Mezmo, you can avoid these pitfalls and stay HIPAA-compliant. Mezmo offers sophisticated features for securing access to logs and monitoring logging failures. In addition, Mezmo itself is certified by an external assessor to meet HIPAA requirements, and Mezmo will sign BAAs with customers.

To learn more about how Mezmo can simplify HIPAA compliance for your organization, contact the Mezmo team.



"Mezmo lets you set granular permissions using role-based access control (RBAC). You can restrict each user's ability to view, create, or modify Mezmo resources, as well as restrict their access to logs based on source or content."



CONCLUSION

From HIPAA to PCI DSS to GDPR and beyond, today's developers and IT engineers face a dizzying set of compliance requirements that they must meet. Fortunately, with the help of a comprehensive, compliance-oriented logging solution like Mezmo, teams can efficiently collect and analyze the data they need to identify and address compliance risks, no matter how complex their infrastructure and applications may be.

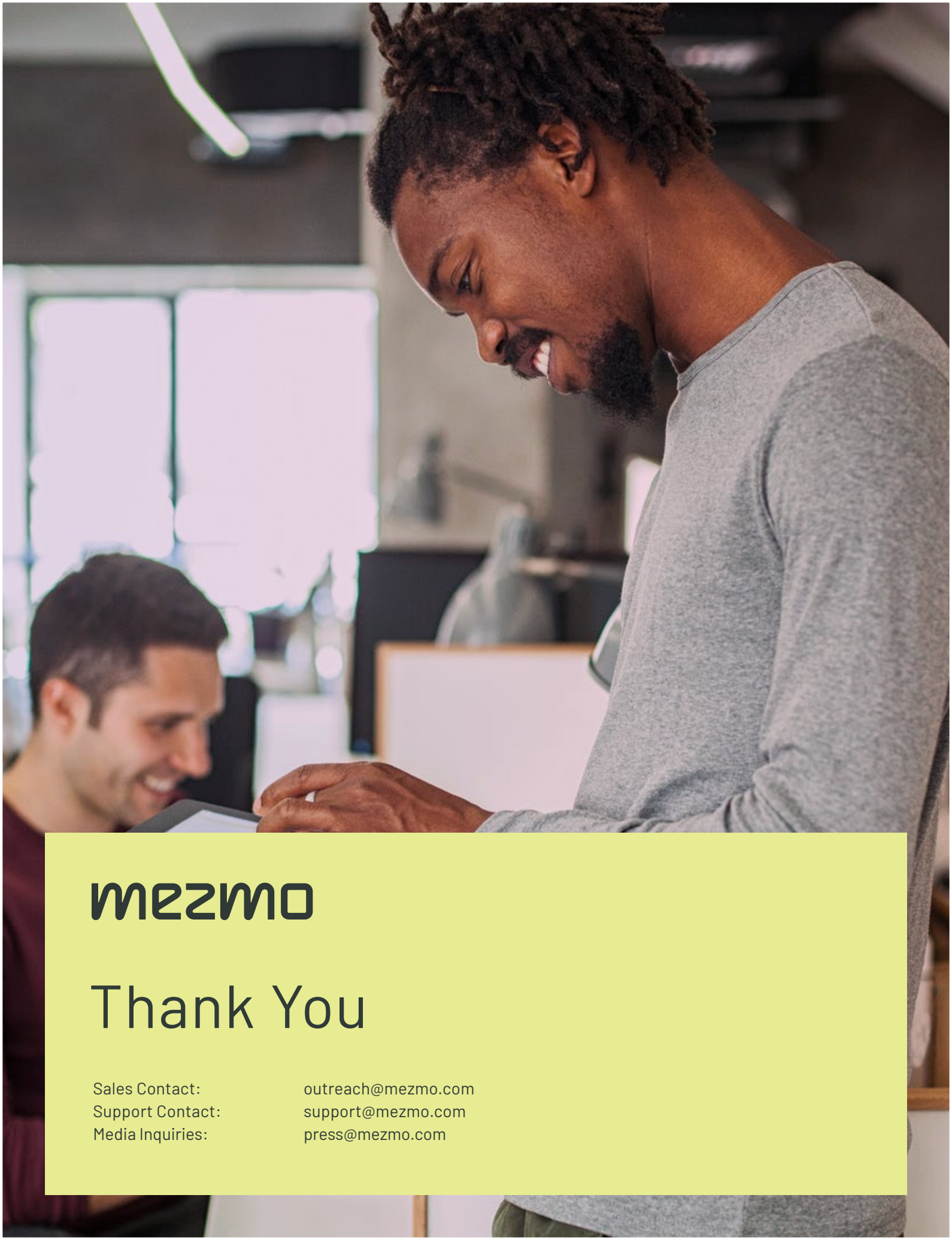
To learn more about how Mezmo can simplify your organization's compliance operations in a landscape that is becoming ever-more complicated, schedule a live demo with the Mezmo team.

Next Steps

Mezmo takes compliance very seriously. It can be used to process your log files regardless of which language your application is written in, and it has a series of connectors for services like AWS CloudWatch and Slack. In addition, it can handle logs as they grow from megabytes to terabytes, and it also allows you to search live feeds in order to pinpoint ongoing issues. To see how quickly it will boost your operations, you can sign up for a free trial here.

About Mezmo

Mezmo is a centralized log management solution that helps modern engineering teams be more productive in a DevOps-oriented world. It enables frictionless consumption and actionability of log data so developers can monitor, debug, and troubleshoot their systems with ease.



mezmo

Thank You

Sales Contact:	outreach@mezmo.com
Support Contact:	support@mezmo.com
Media Inquiries:	press@mezmo.com