CIMCOR

CASE STUDY

How Zoom Implemented CimTrak for FedRAMP Compliance and Increased Security Posture

zoom

INDUSTRY: Software
LOCATION: Headquartered in San Jose, CA with global locations
EMPLOYEES WORLDWIDE: 2,200+
SOLUTION: CimTrak File Integrity Monitoring for Servers and Network Devices
CUSTOMER SINCE: 2019
WEBSITE: zoom.com

»TRY CIMTRAK NOW

ABOUT ZOOM

Zoom Video Communications, Inc. brings teams together to get more done in a frictionless video environment. Zoom's easy, reliable, and innovative video-first unified communications platform provides video meetings, voice, webinars, and chat across desktops, phones, mobile devices, and conference room systems. Zoom helps enterprises create elevated experiences with leading business app integrations and developer tools to create customized workflows. Founded in 2011, Zoom is headquartered in San Jose, California, with offices around the world.

THE PROBLEM

With thousands of systems deployed across the globe, it was critical that Zoom achieve compliance for Service Organization Controls (SOC) 2 framework as well as meet FedRAMP Compliance requirements. This had to be done while continuously expanding to meet customer demand and doing so while going through an initial public offering (IPO).

Developed by the American Institute of Certified Public Accountants (AICPA), SOC 2 reports are specifically designed for service providers that store customer data in the cloud for commercial entities. This means SOC 2 applies to almost every Software as a Service (SaaS) company or any company that uses the cloud to store its customers' information.

What is required of SOC 2? It is a technical audit requiring companies to establish and follow strict information security policies and procedures that incorporate the security, availability, processing, integrity, and confidentiality of customer data. SOC 2 ensures a company's information security policies and guidelines reflect that of their cloud usage and requirements.

"It was really from a security standpoint, and for that case, FIM was chosen to be deployed as we could be successful in SOC 2, and FedRAMP accreditations."

–John Keese
Zoom Video Communications,
Head of Compliance

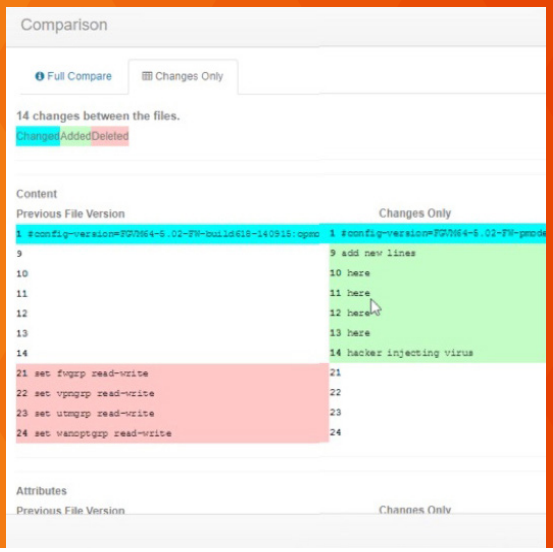
BENEFITS TO BUSINESS

- ☑ Real-time protection against unauthorized change to the Zoom network infrastructure.
- ☑ Ability to detect and classify changes to vital server elements, including OS files, directories, data files, file attributes and more.
- ☑ Reduction in system outages and bottlenecks increasing productivity and business continuity.
- ☑ Compliance with FedRAMP and SOC 2 compliance requirements, ensuring security and integrity across the infrastructure.

cimtrak
Detecting change thoughout the enterprise

"In the case of FedRAMP we needed discovery within 5 minutes, so the fact that we can be notified in real-time about events that require investigation or notification, those [notifications] would otherwise not occur. Without CimTrak in place we would have a compromise that we would not know about until it's too late."

–John Keese
Zoom Video Communications
Head of Compliance



Within their enterprise, the Zoom team essentially had to solve the compliance issue while also aligning with a number of other security initiatives with a single solution. CimTrak's file integrity monitoring (FIM) and compliance offerings were a perfect fit to meet their current and future objectives.

THE SOLUTION

The solution to help with Zoom's goal of compliance for the Federal Risk and Authorization Management Program (FedRAMP) was to implement CimTrak's file and system integrity monitoring software. Additionally, the focus of monitoring servers was of high importance, as CimTrak for Servers allows users to detect and classify changes to vital computer server elements, including operating system files, directories, data files, file attributes, Windows Registry, and more.

Deployed on thousands of servers worldwide in both the government and commercial environments, CimTrak's file integrity monitoring software was deemed the best choice for aiding in compliance requirements and security posture. Monitoring critical network devices, switches, and routers including Palo Alto and Juniper, was also a concern as it was a critical part of their data center network. Zoom datacenters are worldwide, as well as in the cloud, of which the number of servers and devices being monitored varies.

Automated deployments and configuration were not a problem, as CimTrak's capabilities worked for the Linux-based environment, and due to the highly regarded technical support offered by Cimcor, the choice was made to monitor network devices as well.

"Being able to remediate timely is significant, with CimTrak–it is already baked into image builds–and allows us assurance that this competency is under continuous management."

–John Keese
Zoom Video Communications
Head of Compliance

Zoom For Government

The original intent and usage of CimTrak was two-fold. With Zoom for Government, file integrity monitoring is a requirement for authorization. This can be accomplished in more than one way. John Keese, Head of Compliance at Zoom, has been in the FedRAMP space since 2012 and noted the lack of being able to execute with other solutions, specifically from an operational standpoint.

Zoom Commercial

The parameters for commercial usage of Zoom did not have the same set of requirements as FedRAMP, however the choice to utilize file integrity monitoring (FIM) was not only for security, but also as part of best practices. There was difficulty with operational execution for previous solutions, and the need to have success with SOC 2 was great.

OUTCOME

With CimTrak's file and system integrity monitoring for servers, Zoom's security posture has been improved, and compliance with FedRAMP and SOC 2 is no longer a concern.

From a feature standpoint, utilizing the ability to integrate with file reputation services Checkpoint, helped Zoom leverage the investment in CimTrak, as it allows planning for implementation, and easy integration with change management.

From a security posture standpoint, utilizing CimTrak's File Integrity Monitoring Software provides Zoom with assurance that systems are operating in the state they are supposed to be in.

> *"CimTrak does what it says it does–without a lot of heaviness and problems. Technical support understands the product and understands the implementation. It gives us assurance against things we cannot see or things that are hard to identify, like malware. All forensic post-event investigation and damage is prevented by the use of CimTrak."*
>
> *–John Keese*
> *Zoom Video Communications*
> *Head of Compliance*