

CUSTOMER STORY

Securing a Rapidly Expanding Attack Surface with Cosmos

As businesses and users have shifted to remote work environments, Zoom has experienced unprecedented growth in their user base – from 10M daily meeting participants in December 2019 to 300M in April 2020. To protect these new users, Zoom sought out continuous security testing to add to their robust security program.



As businesses and users have shifted to remote work environments, Zoom has experienced unprecedented growth in their user base – from 10M daily meeting participants in December 2019 to 300M in April 2020. Not only did they grow their user base, but they also reported equally significant customer growth – approximately 265,400 customers with more than 10 employees, a number that's grown 354% year-over-year. To protect these new users, Zoom sought out continuous security testing to add to their robust security program.

Zoom allows each new business customer to create their own subdomains for their employees and contractors. Recognizing that they now needed to protect approximately 250K new subdomains that would become part of their overall attack surface, Zoom proactively sought out a solution that could scale. After talking with Bishop Fox security experts, Zoom realized they needed security testing that was more comprehensive and agile than a standard point-in-time assessment to protect their rapidly expanding attack surface.

As businesses grow their user bases, they add complexity to their attack surface – each piece of infrastructure (subdomains, domains, applications, software, etc.) becomes a potential target that an attacker can exploit. To lock down those assets, companies must not only have comprehensive visibility into their attack surface, but they must be able to continuously track emerging threats, new assets, and then prioritize those potential risks to secure their clients and their data.

zoom

WEBSITE:

<https://zoom.us/>

INDUSTRY:

Communications

SERVICES PROVIDED:

Cosmos (formerly CAST)

ABOUT ZOOM:

Zoom brings teams together to get more done in a frictionless and secure video environment. The easy, reliable, and innovative video-first unified communication platform provides video meetings, voice, webinars, and chat across desktop, phones, mobile devices, and conference room systems. Zoom helps enterprises with leading business app integrations and developer tools to create customized workflows.





Combining Technology and Human Expertise To Rapidly Identify Priority Security Risks

Continuous monitoring and tracking sounds daunting, as it often leaves security teams with a lot of noise and heaps of data, but no clear path on where to act first to make the biggest security impact for their business. What Zoom needed was human expertise to weed through this data and analyze them as an attacker would.

Bishop Fox partnered with Zoom in May 2020 to map their attack surface, which was growing rapidly not just in size, but in complexity, so that we could find any unknown assets and locate security risks for the company. With the Cosmos (formerly CAST) platform, Zoom could rely on Bishop Fox security experts to work through the potential security issues that existed on Zoom's 500K targets and create proof-of-concept exploits to prioritize which risks required immediate attention.

As a result, Zoom was able to remediate the risks before attackers could exploit them in order to proactively protect their clients.

The goals of the engagement:



- Assess the overall security of the Zoom environment
- Add continuous security testing to their robust security program to protect their significant customer growth
- Uncover misconfigurations to prevent them from becoming part of their public attack surface





Augmenting Zoom's Security Team to Provide Actionable Risk Insights

Zoom worked alongside the Bishop Fox Cosmos team, who helped to find, validate, and essentially act as a red team for every asset Zoom owned on the Internet. What Zoom needed was to complement their full-scale security program with a deeper, continuous view of their attack surface. The challenge was to get the deep security insights they needed on a broad scale and in real time in a way that was both manageable and actionable for their team.

The Cosmos team became an extension of Zoom's expert security group, helping them discover unknown infrastructure and new technologies within their attack surface to give them a full view of their assets. With Zoom's thorough bug bounty program in place, Bishop Fox was able to take input from those findings to validate and prioritize those issues for the security team to remediate.

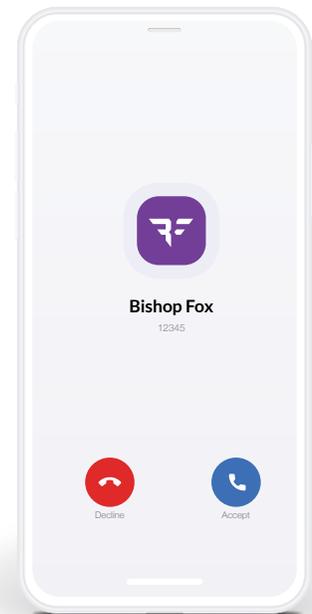
In addition, the Bishop Fox team was able to add that information to the Cosmos platform to quickly search for other areas within Zoom's attack surface that may have issues related to the vulnerabilities reported within the bug bounty program. The Cosmos team was able to help Zoom find misconfigurations to prevent them from becoming part of the public attack surface. With this information, Zoom was also able to learn from and prevent future misconfigurations from putting them at unnecessary risk.



Fixing Critical Issues Within Hours of Discovery

Armed with a highly curated, prioritized list of security issues, Zoom was able to jump into action and proactively mitigate vulnerabilities before attackers could actively exploit them. The company immediately fixed 5 critical or high-risk issues within hours of our Cosmos team finding and validating those issues. After we demonstrated the attack vectors and how our proof-of-concept exploits would work, the Zoom team escalated the mitigations internally to get the resources they needed to take immediate action.

Bishop Fox will continue to work alongside Zoom to help prioritize and validate new risks as they emerge and work toward remediating those issues. By continuously mapping their changing attack surface and discovering new issues, Zoom ensures that their clients, their application, and all stored data is secured – no matter when they're targeted.



ABOUT BISHOP FOX

The Leader in Offensive Security

Bishop Fox is the leading authority in offensive security, providing solutions ranging from continuous penetration testing, red teaming, and attack surface management to product, cloud, and application security assessments. We've worked with more than 25% of the Fortune 100, 8 of the top 10 tech companies, and hundreds of other organizations to improve their security.

Our Cosmos platform was named Best Emerging Technology in the 2021 SC Media Awards and our offerings are consistently ranked as "world-class" in customer experience surveys. We're an active participant in the security community and have published more than 15 open source tools and 50 security advisories in the last 5 years. Learn more at bishopfox.com or follow us on Twitter.

