CUSTOMER SUCCESS STORY

Coincheck Prioritizes Threats with VMware Carbon Black

Coincheck

With cryptocurrency on the rise, Tokyo-based company Coincheck has expanded its services to 10 different types of virtual currencies. Coincheck was looking to provide reliable services and an easy-to-use interface for its employees. With an environment entirely on the cloud, Coincheck deployed the next-generation antivirus (NGAV) and endpoint detection and response (EDR) solution VMware Carbon Black Cloud Endpoint™ Standard to 200 of its Mac OS endpoints.

Reevaluating endpoint security

After a data leakage incident in early 2018, Coincheck reconstructed its infrastructure and the security development department, which enhanced its security by using multiple computing systems for in-depth defense, such as controlling networks, endpoints and mobile devices. The department's cybersecurity analyst spoke of the direction of Coincheck's security measures: "Security is recognized as one of the top priorities for our business. Every day, we are putting forth great efforts for enhancing [company] security in order to prevent unauthorized leakages." The team knew they needed to bring both antivirus (AV) and EDR products into their environment. After introducing these products, they started seeing problems with mis-detections, resulting in an increase in operational labor and costs. As stated, "Mis-detections masked the alerts that required urgent correspondence… and consumed CPU terminal resources, causing serious impact on engineer productivity."

As a result, Coincheck began looking into replacing both its AV and EDR products, narrowing their options down to seven different security vendors. Coincheck tested each product for its detection abilities, console performance and cooperation with its existing log management products. Only Carbon Black Cloud Endpoint Standard provided stable performance and ran as expected. "Implementing [Carbon Black Cloud Endpoint Standard] did not cause any burdens to terminal operations, [which] was one of the major reasons for product selection."

INDUSTRY
Finance

COMPANY SIZE
200+ employees

SECURITY CHALLENGES
False positives
Endpoint security in the cloud

PRODUCT
VMware Carbon Black Cloud Endpoint Standard™

KEY BENEFITS
Easier investigation into security incidents
Ability to integrate via APIs

Prioritization of threats

With a short and concise deployment, Carbon Black Cloud Endpoint Standard has given the team an all-encompassing view of their workstations. Implemented on their Mac OS terminals, false positives produced by other products have been eliminated, and the VMware Carbon Black solution has saved the team time. "Other logs [give] us partial information, so we use Carbon Black Cloud Endpoint Standard to search for those details quickly and are able to cut down on research time." With better foundational information and an easy way to maneuver through it all, Coincheck is able to identify emerging threats immediately.

"After introducing Carbon Black Cloud Endpoint Standard, [we achieved] burden-free security for operations."

CYBERSECURITY ANALYST, COINCHECK

Conclusion

Looking to the future, Coincheck anticipates that the attacks toward Mac endpoints will continue to increase at an advanced rate. As Coincheck says, "If the level of an attack is upgraded, we are required to take appropriate measures in a timely manner. [We are confident that] Carbon Black Cloud Endpoint Standard will [stay on top of updates] against the latest attacks."

Discover more companies who have found success with VMware Carbon Black. Visit: carbonblack.com/why-cb/customer-success.

vmware Carbon Black

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com