Avanade leads in threat detection and security automation with Microsoft Azure Sentinel
CASE STUDY
Avanade leads in threat detection and security automation with Microsoft Azure Sentinel

With 36,000 professionals helping Microsoft solution clients, Avanade has to stay ahead of the curve on cybersecurity, both for its own operations and for its clients. To align with its cloud-first vision and up-level its security capabilities, Avanade decided to move to cloud-native Azure Sentinel to replace its on-premises security information and event management (SIEM) system. Now, Avanade has integrated data, improved automation and freed up its IT staff to focus on value-add projects—all while maintaining a commitment to its clients.

IT consulting companies need to stay on the leading edge of technology innovation. For Avanade, a Microsoft Partner Network member and software integrator, maintaining expertise on the Microsoft platform is in its DNA. Based in Seattle, Washington, Avanade provides IT consulting and services on AI, business analytics, application services, digital transformation, and security services to clients in 25 countries. Founded in 2000, today the company serves nearly half of the Fortune Global 500.

“By adopting Microsoft technologies as quickly as possible, we have the opportunity to inform our consulting practice, learn lessons and then model best practices for our clients and provide informed guidance,” said Kyle Carlson, SIEM platform service owner at Avanade.

“Using Azure Sentinel helps us move beyond managing our SIEM on-premises and instead focus on the value add that’s on top of it – how to do more interesting strategic work.”

– Greg Petersen, Senior Director, Security Technology and Operations Team, Avanade
Aligning cloud and security goals

While committed to a cloud-first strategy, Avanade still used an on-premises SIEM system for cybersecurity. Avanade wanted to access integrated data, speed threat detection and increase automation, while minimizing infrastructure maintenance for its IT team. In mid-2019, the company’s licensing agreement for its on-premises SIEM provider approached an end, making it a natural time to consider migrating to the cloud.

Avanade chose to deploy Microsoft Azure Sentinel, one of the world’s first cloud-native SIEM systems. “Deciding to use Azure Sentinel aligned with our cloud-first strategy and our goal to eliminate our data centers by 2020,” said Greg Petersen, senior director, security technology and operations team at Avanade. “Our team can take advantage of advanced features and automation to scale with the threats that we’re seeing.”

The company also uses Azure Security Center to help manage compliance according to Microsoft recommendations for security enhancement. Avanade has begun ingesting logs into Azure Sentinel and plans to migrate all data from the on-premises system before October 2019. The company is committed to maintaining six months’ worth of data and will then archive and turn off the on-premises SIEM instance.

Speeding deployment and data connection

Even while the full deployment was in progress, the Avanade team was impressed with how fast they got it running and transferred data. Azure Sentinel comes with approximately 25 connectors for Microsoft solutions, which provide real-time integration with Office 365, Azure Active Directory, Cloud App Security and more. “The team immediately started using 10 out-of-the-box Azure Sentinel connectors and brought in data from the Microsoft cloud in two clicks,” said James McDonald, senior consultant and lead SIEM engineer at Avanade. “There are also ready-to-use dashboards and queries, which helped us get started quickly.”

Now that Avanade has connected more of its data sources to its SIEM system, it catches potential issues more quickly. For example, since Avanade uses Azure Active Directory, its identity management data more closely ties into Azure Sentinel in the cloud than it did with the on-premises system. “It’s a huge benefit that our Microsoft data is connected, and we can verify the identity in Azure Active Directory as it relates to other downstream productivity apps and other system interactions,” said Carlson.
FREEING UP ADMIN TIME TO TRANSFORM

IT culture

With its SIEM system in the cloud, the IT team spends less time on maintenance, updates and fixes. For example, using the Azure Sentinel connectors, they establish the connections and can move on to other tasks. In the past, they had to set a calendar to track when keys would expire or manually check to make sure the keys still worked. “With Azure Sentinel, we can make the data connection and don’t have to think about it again,” said Carlson. “There’s no operational tail — we are confident that we can set it and forget it.”

As a result, Avanade has freed up IT staff time, which contributes to a larger shift in what’s possible for the team. “Using Azure Sentinel helps us move beyond managing our SIEM on-premises and instead focus on the value add that’s on top of it — how to do more interesting strategic work,” said Petersen. The team has automated its malware response processes and plans to automate responses to other types of incidents.

IMPROVING RESPONSE AND CAPABILITIES

Avanade appreciates the simplified management and maintenance with its cloud-native SIEM system, but the company is also taking advantage of next-level capabilities, such as machine learning. “By using Azure Sentinel, Avanade gains advanced defense tools to improve our threat-hunter response,” said Petersen. “We know that cyberattackers constantly upgrade their arsenal — they use automation and AI to help speed the attack and remain undetected. Now we have an opportunity to upgrade our capabilities to respond.”

Every security decision that Avanade makes for its own internal needs also benefits its clients. “As a solutions integrator on Microsoft products for global Fortune 500 companies, we know that many companies have the same questions around security,” said Petersen. “We work hard to showcase our security practice to our consultants so they can learn from the lessons we share.”

Petersen added, “With Azure Sentinel, we know we have room to grow. Avanade is investing in skills and expertise around machine learning and automation, so building on top of Azure Sentinel aligns with our strategic direction.”

ABOUT AVANADE

Avanade is the leading provider of innovative digital and cloud services, business solutions and design-led experiences on the Microsoft ecosystem. With 36,000 professionals in 24 countries, we are the power behind the Accenture Microsoft Business Group, helping companies to engage customers, empower employees, optimize operations and transform products, leveraging the Microsoft platform. Majority owned by Accenture, Avanade was founded in 2000 by Accenture LLP and Microsoft Corporation. Learn more at www.avanade.com

©2019 Avanade Inc. All rights reserved. The Avanade name and logo are registered trademarks in the U.S. and other countries. Other brand and product names are trademarks of their respective owners.