

Mizuho Financial Group protects \$2 trillion in assets with Tanium

Advanced threat hunting enabled by
Autonomous IT Platform for global banking

**ORGANIZATION**

Mizuho Financial Group

INDUSTRY

Financial Services

EMPLOYEES

50,000+ globally

HEADQUARTERS

Tokyo, Japan

REVENUE

3.17 trillion JPY



As a global systemically important bank (G-SIB), Mizuho Financial Group holds a high degree of influence in global financial markets and in Japan where the 150-year-old megabank is also a pillar of cultural significance. With more than 100 locations in the Americas, Asia and Europe, and 22 million customers, Mizuho Financial Group is entrusted with managing \$2 trillion in assets. Like all highly connected and digitally transformed banks, it must anticipate and defend against a growing number of cyber risks, including ransomware attacks, third-party risks, and attacks by nation-state actors.

The company's Cybersecurity Management Department, led by the Group CISO, is continually boosting the capabilities and efficiency of its security operations center and incident response. Covering both domestic and international company infrastructure, the department uses a cybersecurity risk management framework based on industry standards issued by the National Institute of Standards and Technology (NIST), Cyber Risk Institute (CRI), and Japan Financial Services Agency (JFSA). The department established a proactive threat hunting discipline to counter evolving threats that are increasing in sophistication and preference for the financial services industry.

Confronting cyber risks with real-time endpoint intelligence from an Autonomous IT platform

To get an edge over cyber adversaries, Mizuho Financial Group turned to the capabilities of the Tanium Autonomous IT Platform that uses real-time intelligence across endpoints to help continuously investigate unknown threats. With Tanium, the team can run the necessary queries to investigate signs of malicious activity while conducting threat hunting activities.

The complexity of the work could not be overstated. Mizuho Financial Group manages hundreds of thousands of endpoints, including branch teller systems, trading workstations, corporate machines, back-office systems, and mobile devices for more than 50,000 employees. The challenges that typically arise with this scale—visibility, OS and device diversity, compliance, coordination, and latency—are readily addressed by Tanium's Autonomous IT Platform.

"Tanium provides a single, unified platform which allows us to effectively optimize our security operations," said Yohei Yonei, deputy general manager, Global Cybersecurity Promotion Team, Cybersecurity Management Department. "By making Tanium a standard part of our operations, we aim to optimize both costs and resources."

Challenges:

- High exposure to sophisticated cyber threats
- Massive global scale and complexity
- Visibility across heterogeneous IT environments
- Reliance on traditional rule-based monitoring approaches



"Tanium provides a single, unified platform for Autonomous IT which allows us to effectively optimize our security operations."

Yohei Yonei

Deputy General Manager, Global Cybersecurity Promotion Team, Cybersecurity Management Department, Mizuho Financial Group

Benefits:

- Strengthened resilience through a single, unified platform — driven by real-time intelligence for continuous detection and autonomous response
- Improved accuracy in detecting threats in real time
- Reduced operational burden from false positives
- Centralized, integrated security operations
- Foundation for expanding security use cases

Gaining the upper hand with active defense

Threat hunting with Tanium gave the Mizuho Financial Group team an edge over traditional rule-based monitoring. Since Tanium is already deployed on the endpoints across the company's global IT estate, it made it easier for the cybersecurity team to ingest and leverage indicators of compromise (IOCs). Using Tanium's real-time intelligence, they were able to determine on a case-by-case basis whether something was an actual IOC or a false positive, which improved the efficacy of security operations and boosted operational maturity.

"We've found that rule-based monitoring often results in a high number of false positives, which places a heavy burden on monitoring operations, but executing queries with Tanium's platform allows us to detect legitimate behaviors from scanning products and vulnerability assessment tools," said Yudai Doi, an associate on the department's Cyber Response Team.

"Tanium's Autonomous IT Platform has proven it can be used for broader threat hunting and detection as well, and we have plans to expand its use internally."

The Mizuho Financial Group also benefits from Tanium's world-class support team, saying that they receive very timely and thorough responses.

"They often created opportunities for discussion on the spot in response to our questions, and we feel that we have been provided with extremely attentive and robust support."

Expanding use case to harness autonomous IT

In addition to threat hunting, the Mizuho Financial Group Cyber Response Team plans to harness the power of Tanium's Autonomous IT capabilities to cover a broad range of security operations on a single, unified platform. New use cases include broader threat hunting and detection scenarios while further standardizing operations to deliver value and protect Mizuho Financial Group's critical systems and information.

For further information please visit www.tanium.com



"Tanium's Autonomous IT Platform has proven it can be used for broader threat hunting and detection as well, and we have plans to expand its use internally."

Yohei Yonei

Deputy General Manager, Global
Cybersecurity Promotion Team,
Cybersecurity Management
Department, Mizuho Financial Group



Autonomous IT. **Unstoppable Business.**