NETSOL

Cyber Shield: Strengthening MINI USA's Digital Ecosystem

Industry: Automotive
Client: MINI USA
Challenge: Strengthening the security of a container-based web application hosted on Azure to defend against sophisticated and evolving cyber threats.

Overview

As the automotive industry undergoes rapid digital transformation, leading automakers increasingly rely on web applications to streamline operations and enhance customer experiences. MINI USA wanted to develop a container-based web application hosted on Microsoft Azure, enabling seamless interactions with suppliers, partners, and customers. However, as their digital footprint expanded, so did their vulnerability to evolving cyber threats. The company recognized the need to proactively secure their web applications and cloud infrastructure to protect critical data, maintain compliance, and ensure uninterrupted service. To address these needs, MINI USA partnered with NETSOL to implement a comprehensive and resilient cybersecurity solution.

Challenges

The MINI USA faced a variety of cybersecurity challenges that threatened the integrity of their Azure-hosted web application:

Evolving and Sophisticated Cyber Threats:
As global cyberattacks became more sophisticated and prevalent, the automaker needed to defend against advanced persistent threats (APTs), zero-day vulnerabilities, and other emerging risks. They required advanced security solutions that could anticipate and thwart attacks before they could cause damage.

Regulatory Compliance Pressure:
The automaker had to adhere to stringent regulatory standards, including ISO/IEC 27001, SOC2, CCPA, and US Data Privacy Law. Ensuring compliance across their cloud infrastructure was crucial to avoid regulatory penalties and maintain customer trust.

Real-Time Threat Detection and Incident Response:
With increasing cyber risks, it became imperative for the automaker to have continuous, real-time monitoring of their application for potential threats, and to ensure that any detected vulnerabilities or attacks were quickly mitigated. Minimizing response time was critical to reducing the impact of security incidents on the organization.

Solution

NETSOL provided a multi-layered security solution that was tailored to the automaker's specific needs, combining advanced technologies and expert services to fortify the protection of web application and their cloud environment. The solution was implemented using the following key strategies:

1. Managed Security Operations Center (SOC) for 24/7 Monitoring

NETSOL seamlessly integrated the automaker's Azure-hosted environment into its fully Managed Security Operations Center (SOC), delivering 24/7 monitoring and advanced threat intelligence services. This integration provided the automaker with continuous oversight, enabling proactive detection and swift mitigation of security incidents. The SOC team actively conducted real-time threat hunting, utilizing cutting-edge technologies to identify traffic anomalies and address potential intrusions with immediate, targeted countermeasures, ensuring maximum protection.

- **Advanced Threat Intelligence:**
  NETSOL's SOC leveraged state-of-the-art threat intelligence feeds, aggregating data from global cybersecurity sources to stay ahead of emerging risks. These feeds provided real-time insights into global threat landscapes, allowing the automaker to bolster its defenses against zero-day exploits, new vulnerabilities, and advanced persistent threats. This ensured that the automaker's security posture remained adaptive and robust against ever-evolving cyber threats.

- **Proactive Threat Hunting:**
  NETSOL's SOC employed behavioral analytics, machine learning (ML), and artificial intelligence (AI) to continuously monitor and analyze network traffic and system behavior. This enabled the detection of abnormal patterns, suspicious activity, and emerging threats early in their lifecycle, allowing to intercept potential attacks before they could escalate.

- **Rapid Incident Response:**
  Equipped with automated playbooks and predefined workflows for handling common and complex cyber threats, the SOC team drastically reduced incident response time. By automating routine threat mitigation tasks and focusing on advanced incident handling, the team minimized the impact of cyberattacks on the automaker's operations.

- **SIEM and SOAR Implementation:**
  NETSOL implemented IBM QRadar for Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR). This has allowed for centralized log management, real-time security event monitoring, and automated threat response, significantly enhancing the automaker's ability to detect and address security incidents efficiently.

2. Comprehensive Vulnerability Assessments & Penetration Testing

To ensure that the automaker's web application and cloud infrastructure remained resilient to new threats, NETSOL conducted regular vulnerability assessments and penetration testing. These assessments involved in-depth analysis of the application's codebase, network configurations, and third-party integrations, identifying weak points before malicious actors could exploit them.

- **Continuous Scanning for Vulnerabilities:**
  Automated scanning tools were deployed to continuously monitor for new vulnerabilities, ensuring rapid remediation of security gaps.

- **Red Team Testing:**
  MINI USA engaged NETSOL's Red Team for simulated cyberattacks, stress-testing the application's defenses, and preparing for real-world attack scenarios.

3. Microsoft Defender Implementation

To secure their cloud-based container environments, MINI USA utilized Microsoft Defender, which provided advanced protection against a wide range of threats.

- **Cloud Workload Protection:**
  Continuous protection of workloads running on Azure, securing virtual machines, databases, and storage systems from external and internal threats.

- **Container Security:**
  Comprehensive security for the containerized applications, including real-time monitoring of container deployments, identification of misconfigurations, and runtime security to prevent container escape attacks.

- **Runtime Protection:**
  Defender provided enhanced runtime protection to secure the automaker's applications during operation, preventing exploitation of application vulnerabilities or unauthorized code execution.

4. Distributed Denial-of-Service (DDoS) Protection

Given the automaker's need for high availability, NETSOL deployed Azure DDoS Protection to shield the application from different attacks that could disrupt service. DDoS Protection automatically detected and mitigated large-scale attacks before they could impact performance, ensuring that legitimate users were not affected during periods of high demand or cyberattacks.

- **Adaptive Threat Detection:**
  Azure DDoS Protection leveraged machine learning models to distinguish between legitimate traffic surges (such as during a product launch) and malicious traffic spikes, ensuring the application remained available.

5. Azure Web Application Firewall (WAF)

To defend against common web-based vulnerabilities, NETSOL integrated Azure WAF into the automaker's cloud environment. The WAF actively blocked malicious traffic, such as SQL injection, cross-site scripting (XSS), and other attacks identified in the OWASP Top 10, while also offering customization based on the automaker's specific web application architecture.

- **Custom Rules:**
  NETSOL used tailored WAF rules to block known threat vectors and reduce false positives, ensuring optimized protection without affecting legitimate traffic.

- **Threat Intelligence Integration:**
  The WAF was integrated with threat intelligence feeds, allowing for real-time updates to the automaker's security posture based on the latest global threat data.

Results

The comprehensive security measures implemented by NETSOL led to a dramatic improvement in the MINI USA's cybersecurity posture:

99.9% **Reduction in Security Threats:**

Continuous monitoring and proactive threat hunting by the Managed SOC team reduced the automaker's exposure to cyber threats by almost 100%, ensuring that vulnerabilities were swiftly identified and mitigated.

100% **Compliance with Regulatory Standards:**

MINI USA achieved full compliance with industry regulations, including ISO/IEC 27001, SOC2, CCPA, and US Data Privacy Law, allowing them to maintain customer trust and avoid costly penalties. The SOC provided detailed reports for audits, ensuring transparency and readiness for compliance reviews.

30% **Reduction in Incident Response Time:**

Real-time alerts and automated incident response workflows allowed the automaker to resolve security incidents 30% faster than before, minimizing downtime and operational disruptions.

Resilience Against DDoS Attacks:

MINI USA's web application remained consistently available, even during attempted DDoS attacks, thanks to the robust protection provided by Azure DDoS Protection. This ensured high availability and service continuity, particularly during critical business events.

Enhanced Customer Confidence:

By reinforcing their web application's security, the automaker not only safeguarded sensitive data but also enhanced the user experience, ensuring customers could securely interact with the application without disruptions.

Conclusion

This case study highlights the critical role that NETSOL played in enhancing the cybersecurity of MINI USA's web application hosted on Azure. By leveraging a combination of 24/7 SOC services, advanced vulnerability management, Microsoft Defender for Cloud, and other Azure-native security tools, NETSOL helped MINI USA mitigate cyber risks, achieve regulatory compliance, and ensure continuous protection against evolving threats.

The success of this collaboration showcases how a proactive, multi-layered security approach can not only protect business-critical applications but also instill greater confidence among stakeholders and customers in an increasingly digital automotive industry.

About NETSOL

NETSOL Technologies is a trusted global partner, renowned for its deep industry expertise, customer-centric approach, and commitment to excellence. Delivering cutting-edge IT solutions with a strong emphasis on cloud technology and professional services, NETSOL ensures client success across 30+ countries, solidifying its position as a leading global IT solutions provider.

PARTNERSHIP

IBM
SentinelOne
Forcepoint
aws
Microsoft Azure
splunk>
FORTINET

CERTIFICATIONS

Microsoft Certified Azure Solutions Architect Expert
Lead Auditor ISO 27001
CISSP Certified Information Systems Security Professional
CRISC Certified in Risk and Information Systems Control. An ISACA® Certification
eWPT V1
IBM Professional Certification – IBM QRadar SIEM V7.3.2 Associate Administrator – IBM Security
CEH Certified Ethical Hacker – ETHICAL HACKER PRACTICAL
CISA Certified Information Systems Auditor. An ISACA® Certification
eCPPT V2
OFFENSIVE SECURITY OSCP
EC-Council CHFI CERTIFIED
CISM Certified Information Security Manager. An ISACA® Certification

COMPLIANCE POSTURE

International Organization for Standardization ISO 27001
Information Security Management Standard

AICPA SOC SOC 2 TYPE I CERTIFIED
System and Organization Controls

AICPA SOC SOC 2 TYPE II CERTIFIED
System and Organization Controls

International Organization for Standardization ISO 2000-1
System Management System Standard

International Organization for Standardization ISO 9001
Quality Management System Standard

NETSOL

Get in touch!

NETSOL Technologies Inc.
(Headquarters),

16000 Ventura Blvd.,
Suite 770 Encino, CA 91436

Schedule a Meeting

Website:
www.netsoltech.com