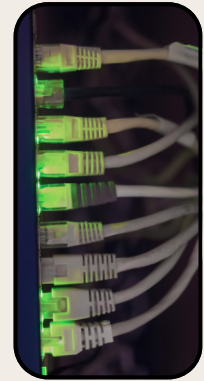# Safeguarding ASUS's Enterprise Computer, IoT, and Network Products with Cybellum's Product Security Platform

Driving Change with Tech: ASUS's Impact on Global Tech

ASUS is a Taiwan-based leader in computer hardware and consumer electronics since 1989, and is renowned for its innovation in smart technology. Globally, ASUS holds the top spot in motherboards and gaming and ranks among the top three in consumer laptops.

The company revolutionized the PC market in 2007 with the Eee PC™ and continues to set trends with products like the ZenFone™ series, as well as advances in VR, AR, IoT, and robotics. Its smart home robot, Zenbo, exemplifies ASUS's commitment to making technology accessible and helpful in daily life.

ASUS's dedication to quality and innovation has earned it global recognition, including Fortune's World's Most Admired Companies and Interbrand's ranking as Taiwan's top international brand. With over 17,000 employees and an elite R&D team, ASUS earned more than 57,156 awards since 2001 and generated US$19 billion in revenue in 2021.

ASUS's Enterprise Solution BU (ESBU) provides computing and networking solutions, such as servers, storage, and cloud services for a wide range of customers, from data centers to Accelerated Computing centers and Telco solution providers.

No-Compromise Cybersecurity: ASUS's ESBU Product Security Goals

To safeguard the enterprise solutions their customers depend on, ASUS has set a very high standard for their product security program, including the following goals:

- Reducing time to remediation: In addition to source code scanning the team at ASUS was looking for additional technologies to improve speed of detection, accuracy of detection, better vulnerability management and an improved mitigation process.
- Optimizing risk detection: Saving time by minimizing false positives to the minimum, by using additional sources of asset data (such as binary analysis) and optimizing vulnerability prioritization
- Improving risk management & governance across the Enterprise Solutions Business Unit: The ASUS team was looking for a way to improve risk tracking throughout the development lifecycle, as well as have an easier way to generate risk reports

Joining Forces: Choosing Cybellum's Product Security Platform
After testing multiple product security solutions, ASUS chose Cybellum's Product Security Platform for the following use cases:

- **Asset Management:** The ASUS team saw significant value in Cybellum's asset management capabilities, particularly in asset definition and binary analysis. This created a strong foundation for vulnerability management by detailing ASUS's products and components in the Product Security Platform, including SBOMs, HW BOMs, OS configurations, API calls, and more.
- **Assurance & Vulnerability Management:** the ASUS team was impressed with the platform's ability to both prioritize vulnerabilities automatically using the VM CoPilot (Cybellum's automated prioritization engine), and provide clear mitigation recommendations, which together save time and significantly reduce time-to-mitigation
- **Risk Management & Governance**: Management dashboards for risk and vulnerability management allow the BU managers to quickly track risks and identify gaps, across products, components and teams, which in turn provides much better visibility and control

> *"Cybellum's Product Security Platform helped us reduce product security resources significantly, reducing our vulnerability management efforts by more than 80%, and allowing us to save time by mitigating vulnerabilities much more quickly and effectively. This helps us reach our cybersecurity goals, helping the ASUS Enterprise Solutions Business Unit to focus on innovation and growth."*
>
> -Richard Liu, General Manager of Enterprise Solutions BU, ASUS

Results and Benefits

After deploying the Product Security Platform in their environment, the ASUS team measured the following results:

- An 11x reduction in vulnerability management efforts: By incorporating multiple data sources for asset management using the Product Security Platform, such as binary scanning, the team at ASUS saw significantly less false positives, and ended up spending much less time identifying and mitigating vulnerabilities
- Increased visibility and control over product risk - with better risk management tracking capabilities and reduced noise, risk governance has become much easier, allowing BU managers to identify gaps much more quickly
- 84% less error detection rate - by leveraging Cybellum's VM CoPilot and asset management capabilities, vulnerability detection error rate was significantly reduced, saving time and resources

"ASUS is a household brand name for a reason. For more than 30 years, they are leading the way in computer, network, IoT and Robotics innovations. We are proud to work with them in order to help secure the future of these industries for enterprises around the world".

-Eddie Lazebnik, VP Channel Sales at Cybellum

About Cybellum: Where Teams Do Product Security

Device manufacturers such as Jaguar Land Rover, Supermicro, Danaher, and Faurecia use Cybellum's Product Security Platform and services to manage cybersecurity risk and compliance across business units and lifecycle stages. From Asset & SBOM Management to Assurance & Vulnerability Management, Regulatory Evidence Creation, and Incident Response, teams ensure their connected products are fundamentally secure and compliant – and stay that way.

C/O CYBELLUM