EMBRACING SECURITY AS A CORE COMPONENT OF THE TECH YOU BUY

The study was sponsored by Intel.
Research independently conducted by ABI Research.

Senior Analyst: Andrew Cavalier
Content Manager: Jake Saunders

ABIresearch
THE TECH INTELLIGENCE EXPERTS™

CONTENTS

EXECUTIVE SUMMARY

Due to the rapidly evolving cybersecurity landscape, and the effort by hostile actors to find and exploit reported software and hardware vulnerabilities, companies are facing more sophisticated threats. While IT departments are using security assurance to help secure their systems, technology vendors are applying enhanced security assurance practices to proactively improving the resilience of their products and their responses when a security vulnerability is found in a product.

Product security assurance spans both hardware and software, consisting of people, practices, and processes that act as the first line of defense in any technology system. Systems, after all, are only as good as the components they are made of. Vendors must take a layered approach to product security assurance and invest in the personnel and processes, in addition to the technologies to embed security throughout operations and product development lifecycles. Security assurance is proving to be particularly vital in the chipset industry. Device supply chains are becoming more complex, raising concerns about counterfeiting, data exposure, and component substitution. Enforcing standards and regulations has, therefore, become challenging due to the lack of full transparency and visibility in the supply chain. As a result, demand is growing for holistic product security assurance frameworks that instill high levels of confidence in customers.

ABI Research sought to understand the product security assurance landscape from the perspective of enterprise customers, as well as the chipset semiconductor vendors that need to ensure that the most robust security assurance framework is in place.

A survey of 302 enterprise customer-based respondents was conducted to gain insight into how they view the product security assurance of the technology equipment they are purchasing. ABI Research delved into the issues, concerns, and priorities enterprise customers have regarding the security of the Information Technology (IT) equipment they are purchasing.

A mature Secure Development Lifecycle (SDL), bug bounty programs, well-structured internal product security training, and industry engagement are critical processes for implementing security assurance and compliance requirements into all stages of product development. These areas were raised as important distinguishing factors for a strong security posture in the survey. Some of these practices, like SDL, were also seen as the capability that needed the most improvement and transparency from technology vendors.

ABI Research also conducted in-depth, discursive interviews with enterprise customers that complemented the quantitative survey. A recurring theme that surrounded these conversations was the growing concern about data security, particularly in the cloud. The evolution of Artificial Intelligence (AI) and Machine Learning (ML), and their adoption in cybersecurity was also discussed, though it was viewed that regulatory intervention will be required to unlock the full potential of AI and ML. Overall, there was a consensus among both technology vendors and enterprise customers that the "individual" is central to security-driven processes. The value of adopting a security-first mindset throughout the product development process was recognized and appreciated. Enterprise customers also recognized that there was no, "one-size-fits-all" solution, for security assurance. Overall, this underscores that every industry has different requirements and demands, so security issues may vary by organization. For technology vendors, like those in the semiconductor industry, providing products into every industry in the market, they must find a way to provide security for the most sensitive industries while also prioritizing performance for other industries.

Following the survey and enterprise interviews, ABI Research conducted a competitive analysis assessment of five semiconductor and chipset vendors to evaluate their product security assurance frameworks. Where available, ABI Research integrated primary and secondary research including interviews, materials supplied by the vendors, and publicly available information. Intel emerged as a top implementer and innovator in the competitive assessment. Key features were their sophisticated and mature security assurance frameworks. Intel has a strong foundation built from mature SDL, Product Security Incident Response Team (PSIRT), and bug bounty programs. Overall, the company continues to push the industry forward in product security assurance as a semiconductor vendor. Qualcomm and AMD follow in second and third places respectively, as mainstream companies in terms of product security assurance capability.

Overall, this whitepaper underscores the need for security assurance to be ingrained in a company's culture and practices throughout a product's lifecycle, pre to post market. Furthermore, technology vendors, especially chipset and semiconductor vendors, have an essential role to play. They need to maximize their efforts to enhance their product security assurance framework credentials and capabilities. This report also covers the practices of a strong product security assurance framework such as SDL, security training, and vulnerability disclosure and mitigation, among others.

THE ROLE OF SECURITY ASSURANCE

Due to advanced threats and evolving research in security, technology vendors are investing more resources beyond just creating new security features in their products, but also towards improving the security of the product altogether. In today's complex technology solutions, this means considerations for the security of the software they acquire, their own Research and Development (R&D), operational processes, and upstream and downstream supply chains. Based on the U.S. National Institute of Standards and Technology (NIST), security assurance may be characterized as the measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediate and enforce the security policy. Firms need to maintain a robust, coherent, and 360° perspective throughout all stages of their product's lifecycle, as well as their operational processes. This must include investments in people, processes, and tools to instill confidence in customers that the security and performance of a company's products are able to meet the customers' requirements and expectations.

THE PRESENT CYBERSECURITY LANDSCAPE

According to the U.S. National Vulnerability Database (NVD), annual security vulnerabilities have more than doubled since 2016, with 2022 recording over 13,160 unique bugs and security vulnerabilities during that year. The number of software and hardware exploits continues to increase, while the Time-To-Exploit (TTE) duration continues to decrease.

While companies continue to evolve their security posture and capabilities, Mandiant has reported that technology vendors like Microsoft, Google, and Apple continue to be the most targeted vendors Year-over-Year (YoY). According to Mandiant's 2023 Trends on the Cybersecurity Landscape whitepaper, global detection rates are improving. They increased by 16% in 2022 and 63% in 2023. While there is greater detection, it also implies the number of threats in play are also ramping up. To respond to these threats, identify potential vulnerabilities before a malicious actor can, and build more resilient products, product security assurance practices are needed. ABI Research has seen the level of security assurance competence, and operational sophistication has grown markedly.

GOVERNMENT IS DEMANDING HIGHER STANDARDS

To combat the evolving progression of cyber threats, there has been an increase in policies and standards to improve cybersecurity compliance.

The United States has taken a proactive role in raising the profile of cybersecurity. These regulations (e.g., Executive Order (EO) 14208) mandate collaboration between service providers and executive departments and agencies, such as the Cybersecurity and

Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI), to work together to share threat information In November 2023, the European Council and European Parliament reached agreement on the Cyber Resilience Act (CRA), a legislative framework which will force manufacturers to greatly improve the security of digital and connected products throughout the whole development lifecycle. Under the CRA, manufacturers of in-scope hardware and software products will be required to adopt certain security measures in product design, conduct mandatory security assessments, implement vulnerability-handling and incident reporting procedures, support products with security updates, and provide necessary information to users to enable them to evaluate the security of products they purchase. In the United Kingdom, the Department for Science, Innovation & Technology (DSIT) has legislated a "Security & Telecommunications Infrastructure (PSTI)" bill to improve consumer products' and services' security compliance and processes throughout the manufacturing process. The PSTI regime aims to provide specifications for manufacturers to be aware of vulnerabilities in their products and how they may be exploited, and to call on manufacturers to address vulnerabilities, as well as implement security measures to mitigate

THE FUTURE OF SECURITY ASSURANCE

With the rise of AI and quantum technologies, the outlook on cyberthreats will inevitably increase. While AI will aid tremendously in various aspects of cybersecurity, such as threat detection and analysis, vulnerability scanning and mitigation, and malware detection, the same capabilities can be used to develop phishing and/or malware campaigns that are more human-like, making it more difficult to identify such risks. Cyberattacks may also transition to being automated and, therefore, more seamless in the way vulnerabilities are exploited. Therefore, there is an urgency globally to establish AI governance and regulation, like the recently introduced US AI executive order, which calls for AI models to be safe and secure.

Device Supply Chains

In the semiconductor industry, device supply chains are increasing in complexity as the number of players involved in developing and manufacturing the product has increased. This may make the device supply chain susceptible to counterfeiting and component substitution. With the increasing network of players within the supply chain, it also becomes more difficult to monitor the supply chain due to the lack of full transparency and visibility from design and manufacturing to distribution of the product. Also, due to the global span of the semiconductor supply chain enforcing standards and regulations becomes more difficult, and tracing breaches or attacks may become more challenging.

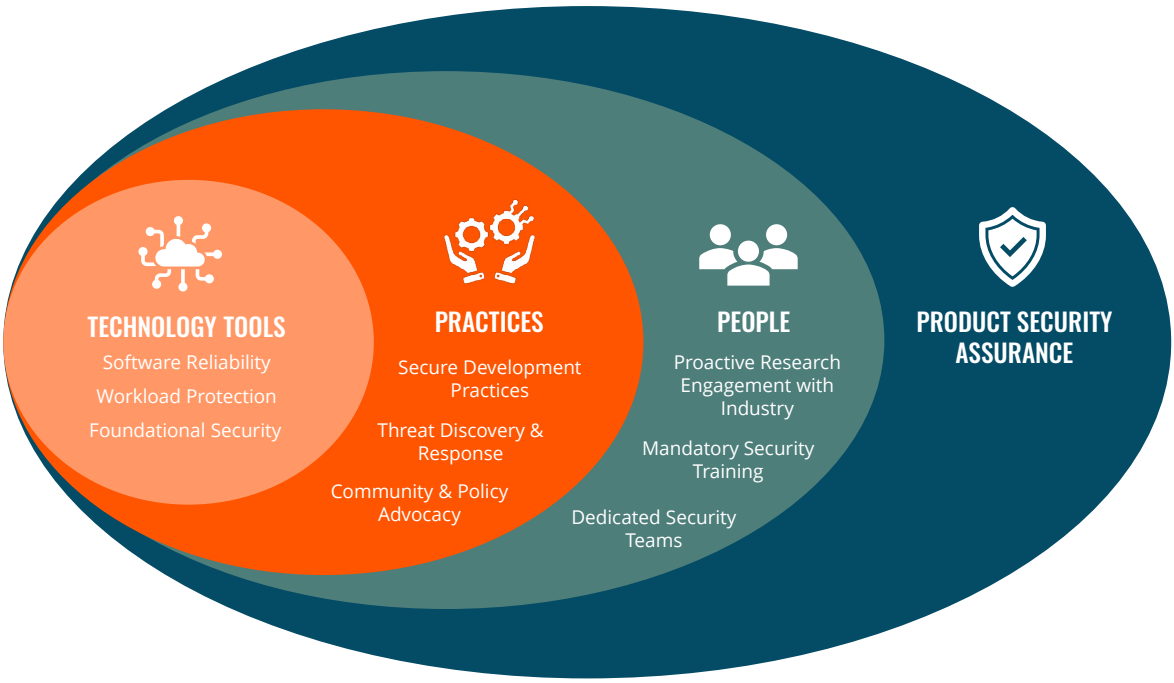
"Ultimately, the emphasis on security assurance must stem from internal company culture and practices that are carried out to ensure a solid foundation of security throughout a product's lifecycle." – Intel

It is imperative that semiconductor vendors such as Intel, NVIDIA, and Qualcomm, among others, are proactive toward applying strong security assurance practices toward their products and throughout their supply chain. For example, Intel and NVIDIA are vendors that actively assess and enforce security certification for key suppliers. Intel spearheads a Supply Chain Risk Management Program (SCRM), which enforces a high degree of certification, attestations, auditing, and monitoring of vendors. Looking to the future, there will be increased pressure on semiconductor vendors to consider security assurance frameworks and processes in every stage of their products' development.

To tackle more complex cyberattacks and to meet evolving enterprise and end-user expectations, there will be greater demand for more holistic and stratified security. Moving forward, a layered approach that combines technology tools, personnel, and practices will be essential for effective cybersecurity management. Technology tools such as 'fuzzing" tools can identify security vulnerabilities in third-party hardware components. Regarding personnel, they need to have the requisite level of training and prioritize security across every aspect of design and validation of products. In the case of operational practices, they have to be systematized to promote security. Good practice can take the form of code reviews and enhancing SDL. The key tenets and objectives of a robust product security assurance framework can be found in the figure below.

Figure 1: Key Features and Practices of a Robust Product Security Assurance Framework

(Source: ABI Research)



Security Assurance—Practices:

- **Secure development practices** consist of architecture considerations, penetration testing, secure coding, validation, and post-development support of products. Secure development practices integrate security principles at every lifecycle stage to help ensure that products are built with security in mind.
- **Threat discovery & response** delivers discovery through offensive security research, PSIRT and bug bounty programs. This process also includes routinely sharing security mitigations and updates.
- **Community & policy advocacy** consists of cross-industry efforts to advance standards, government policies, and industry best practices in security assurance.

Security Assurance—People:

- **Dedicated security teams** prioritize purpose-built teams (i.e., engineers, semiconductor design architects, developers, designers) that embody a security-driven mindset and capabilities that trickle down into the work carried out.
- **Mandatory security training** to reinforce the security-driven mindset and keep internal teams updated with the ongoing security landscape.
- **Proactive research engagement** with the industry sector includes collaboration on industry technology standards, product design, assurance & risk management standards, and/or domain-specific design & verification standards.

DELVING INTO SECURITY ASSURANCE CAPABILITIES

In this whitepaper, sponsored by Intel, but independently researched by ABI Research, ABI Research delves deeper into the product security assurance landscape, focusing on the enterprise customers and end-user perceptions of solutions on the market, as well as the internal practices and processes of semiconductor vendors, to analyze how they enforce security assurance to build more resilient products. The purpose of the study is to highlight what more can and should be undertaken by the ecosystem to enhance product security assurance for everyone's benefit.

Survey

To investigate the importance of product security assurance processes, a survey was conducted to delve into the issues, concerns, and priorities of IT and cybersecurity professionals across several key enterprise markets, including software development, consumer electronics, industrial manufacturing, automotive, and enterprise Internet of Things (IoT). The research was conducted across several markets in the Northern Hemisphere and was supported by 300 respondents. Key interviews with downstream customers from various industries such as telecommunications, industrial manufacturing, financial services, software development, and other solution providers were also conducted to gain deeper insights into the familiarity, satisfaction, current pain points, and market gaps related to product security assurance practices. The survey results can be found in Section 3, titled *"Enterprise Cybersecurity Priorities & Concerns."*

Competitive Assessment

For deeper analysis into product security assurance solutions among semiconductor vendors, ABI Research further conducted a competitive analysis to evaluate the current product security assurance frameworks and capabilities the semiconductor sector has adopted or developed. The competitive assessment results can be found in Section 4, titled "Product Security Assurance in Technology: Competitive Assessment."

ENTERPRISE CYBERSECURITY PRIORITIES & CONCERNS

ABI Research explored the concerns and priorities of IT and cybersecurity professionals across several key enterprise markets concerning technology equipment, solutions, and hardware that IT and cybersecurity managers are purchasing for their IT needs.

The research was conducted across 14 developed and emerging markets. Respondents were required to have IT or cybersecurity roles within their company. In all, they answered 22 questions that delved into their concerns and priorities. Highlights from survey results have been aggregated into three of the following themes: 1) importance of security features; 2) market gaps; 3) familiarity with security assurance products. The country and vertical industry deposition of the respondents can be found in the Appendix.

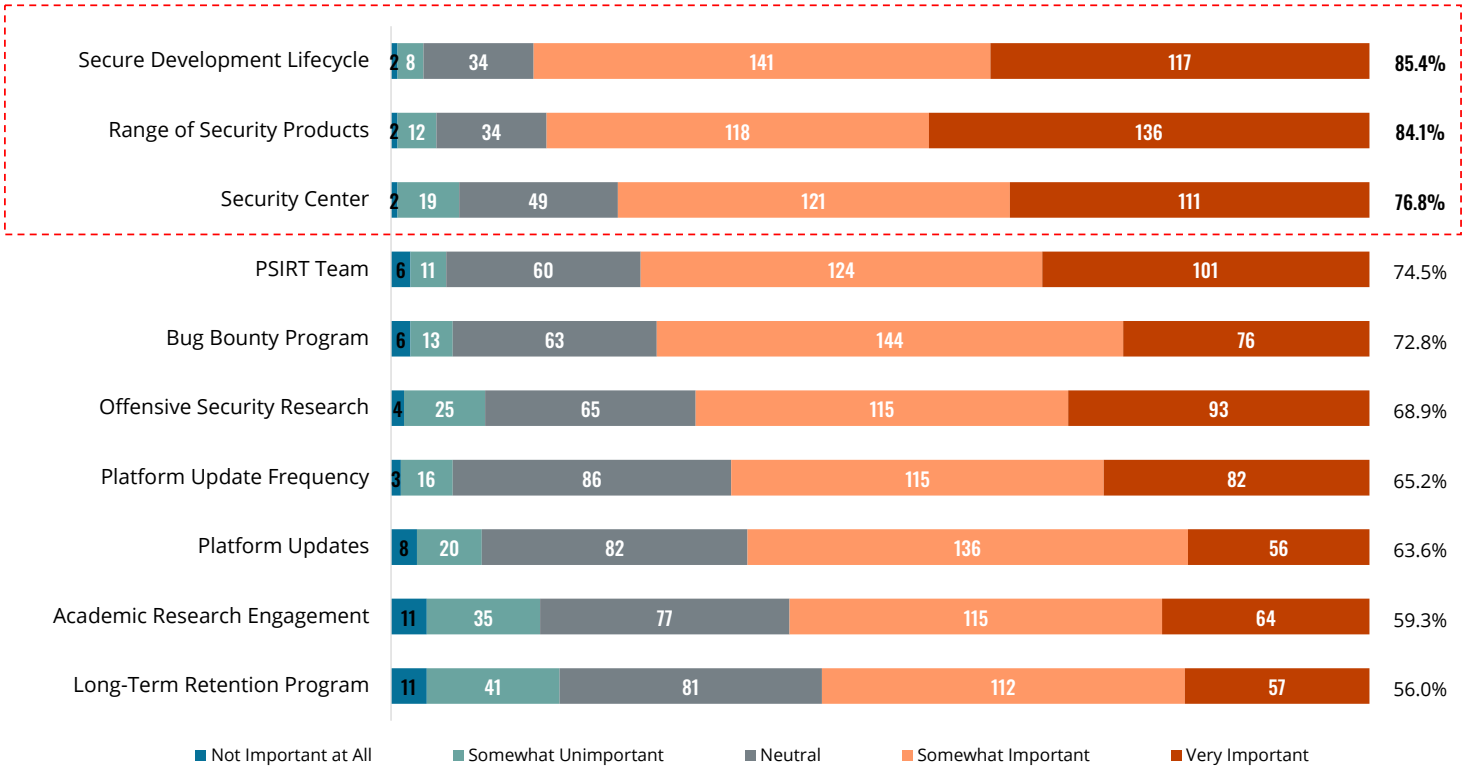
"SDL, vulnerability disclosure & mitigations and bug bounty programs are top considerations when evaluating security assurance solution."
—ABI Research.

IMPORTANCE OF SECURITY FEATURES

Q: How important is the following security feature?

Chart 2: Security feature importance

(Source: ABI Research)



From the survey, enterprise customers noted that the most important features of a security assurance framework are SDL (85%), security product variety (84%) and a robust security center (77%). For respondents, 258 participants regarded SDL as a top consideration. Given that SDL ensures the integration of security into every stage of a product's lifecycle, selecting a product with a solid SDL demonstrates a strong commitment and high maturity of a company's security practices.

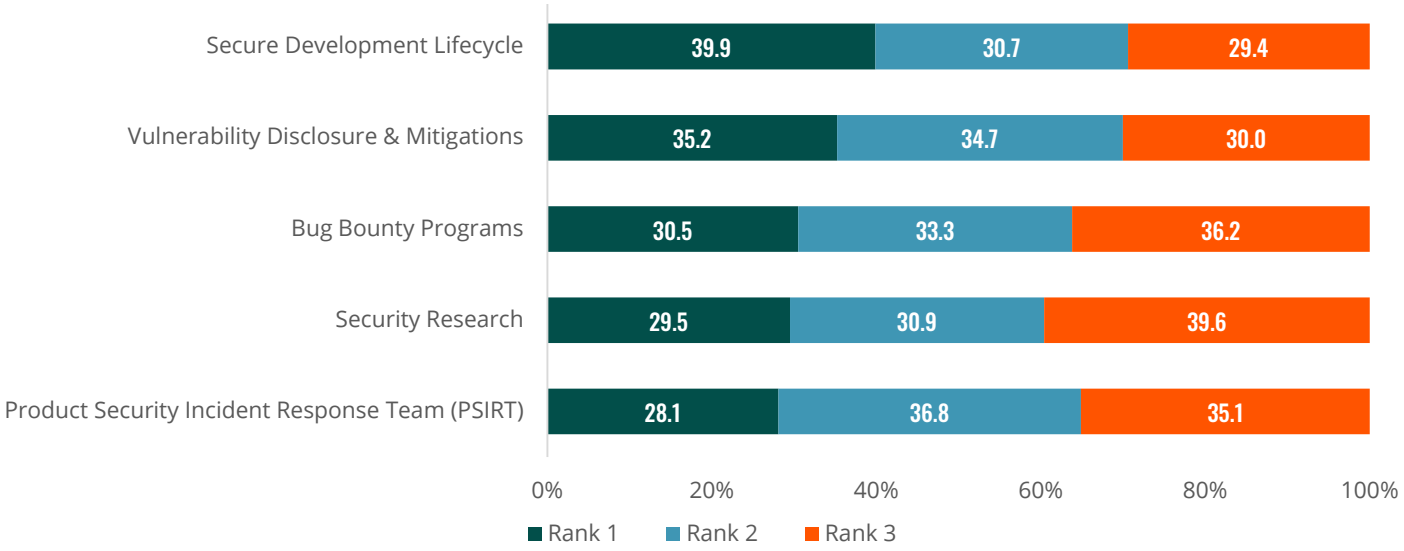
Meanwhile, 254 of 302 respondents (84%) noted that a company's range of market-proven security products for security assurance is an important feature for enterprise customers. Security products include software, services, and firmware IP, which deliver security features such as key generation, software guards, domain extensions, threat detection, confidential computing, and foundational security capabilities.

Among the respondents, 232 out of 302 (77%) mentioned a robust security center as an essential factor when considering the security assurance frameworks of technology vendors in the market. Robust security centers rapidly address issues related to potential security vulnerabilities and provide recommendations through security advisories and security notices. For customers of technology products, this is especially important, as the security center aids with addressing knowledge gaps about a product's security by providing vulnerability and exposure notifications. In this respect, users indicate a high preference toward vendors that provide greater transparency regarding vulnerabilities, bugs, and threat vectors impacting their products.

Q: Which of these aspects is your company's highest priority consideration when selecting a security assurance framework/service for the product you select?

Chart 3: The respondents' highest priority consideration by their company

(Source: ABI Research)



When it comes to selecting a vendor, respondents placed the most emphasis on the importance of an SDL (40%), vulnerability disclosure & mitigation (35%), and whether the vendor has bug bounty programs in place (31%). These aspects of a security assurance framework were given the highest level of priority when deciding which product or solution was best for them.

Taken together, these results underline the importance of a robust and thorough SDL within their overall security assurance framework. Because SDL includes architecture considerations, penetration testing, secure coding, and post-deployment support, enterprise customers place high expectations on vendors that have implemented a robust SDL practice. It is essential that a strong security assurance posture is reinforced by a well-rounded consideration of their product's security at every phase of development. This survey demonstrates that a company's dedication to SDL is a differentiating factor that can set a company apart from its competitors in the market.

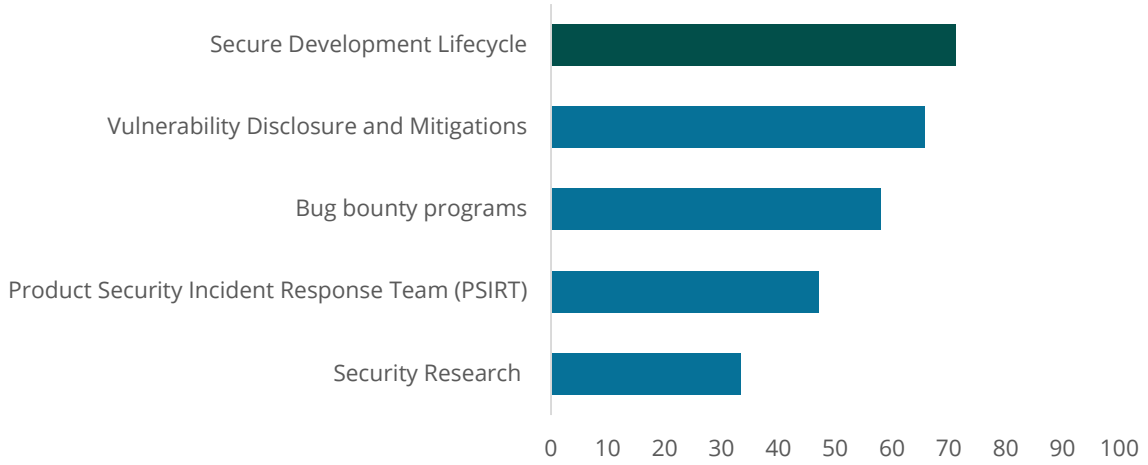
"SDL needs the most improvement (65%), while bug bounty programs need more transparency (71%)." —ABI Research

MARKET GAPS

Q: Which feature needs to be improved in the industry?

Chart 4: Features to be improved in the industry

(Source: ABI Research)

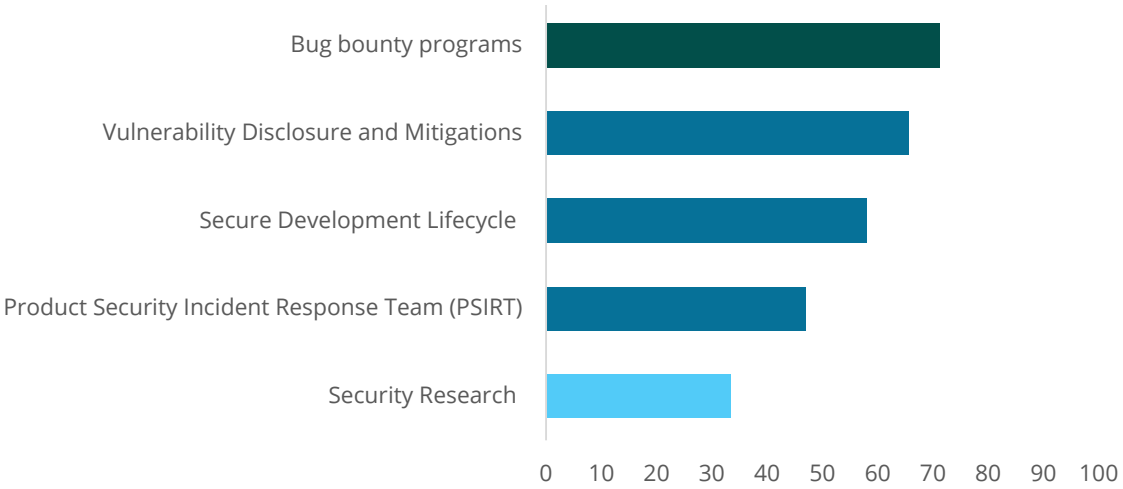


Despite having been recognized as the most important requirement in a vendor's security assurance framework, SDL was considered the area that needs the most improvement. Of the 302 participants, 196 of them (65%) responded in accordance with this. Enterprise customers, therefore, perceive the importance of a strong SDL practice in a security assurance framework, but may have concerns regarding the way that SDL is currently being implemented within their source vendor. In addition, 58% of respondents noted the need for greater transparency in SDL practices. Overall, a more robust SDL practice would stand to strengthen a security assurance solution and technology vendors should take note of this gap in the market.

Q: Which practices should be presented with more transparency?

Chart 5: Practices to be presented with more transparency

(Source: ABI Research)



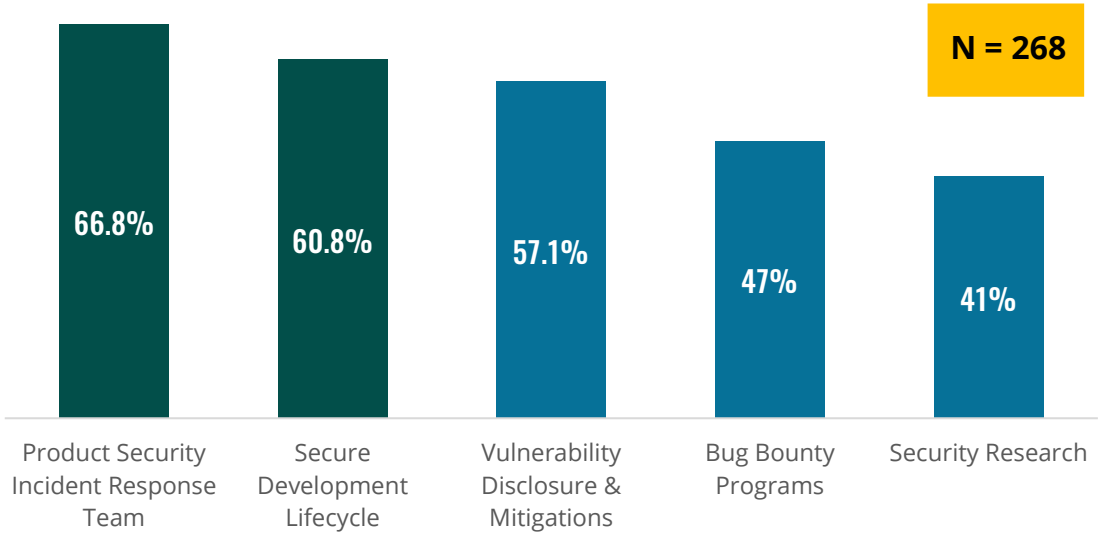
Bug bounty programs were highlighted to require greater transparency by 71% of respondents (n = 215). Bug bounty programs provide recognition to encourage external researchers to report security vulnerabilities on a company's product and collaborate on disclosure. The presence of a bug bounty program demonstrates a strong dedication and

commitment to enforcing a company's tight security posture. However, not all vendors are transparent about their security assurance practices such as bug bounty programs that they host and the impact that it has on their products. For example, some big companies like NVIDIA and AMD do not incorporate bug bounty programs into their product security assurance, which may have the potential to impact the amount of external security research being done on their products. Greater transparency and reporting would be a win-win for the company and the wider industry. Other vendors, such as Qualcomm and Intel, incorporate both static and proactive bug bounty programs into their product security assurance framework that have evolved since 2016 and 2017, respectively. Furthermore, this result demonstrates that end-user customers are attentive to the level of investment that a vendor inputs into their bug bounty programs. Thus, the presence of a bug bounty program and explicit reporting is a differentiating factor for customers.

Q: Which of the following would have mitigated the consequences of the security issue or breach related to a product?

Chart 6: Practices that would have mitigated the consequences of a security issue

Source: ABI Research)



Given the onslaught of malware attacks and spear phishing campaigns by hackers, it may not be surprising that 89% of respondents (n = 268) reported having experienced a breach in security or other security related issues. Of these respondents, it was indicated that a more robust PSIRT and SDL could have reduced the risks of security issues and breaches. The necessity and consequences of using a strong SDL were identified repeatedly as a market gap throughout the survey, showing demand for technology that implements the practices of security assurance through products that are developed with security at their core.

The survey responses indicate the importance of a resilient PSIRT program. A vendor's PSIRT works to minimize customer impact by intaking, triaging, and mitigating security vulnerabilities. The PSIRT also typically handles the public disclosure of vulnerabilities, in addition to the governing of policies, processes, and guidelines for addressing security vulnerabilities that may affect a company's products. By building a resilient PSIRT, a vendor can assure that it is adaptable and flexible in recognizing emerging threats, in addition to being quick to respond and address them. In line with this study, approximately 75% of respondents (n = 225) regarded PSIRT to be an important security assurance feature.

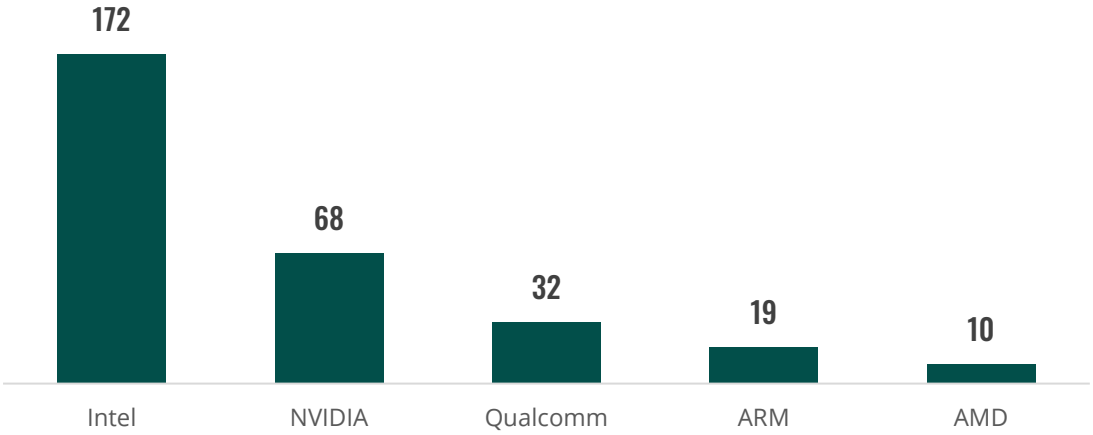
Considering that PSIRT is often the first line of defense for security breaches, the team's maturity and capabilities have a significant impact on the product's security, which is consistent with the findings of the overall study.

FAMILIARITY WITH SECURITY ASSURANCE FEATURES

Q. How familiar are you with the security assurance capabilities of the following vendors?

Chart 7: Survey respondent familiarity assessment of the security assurance capabilities of vendors

Source: ABI Research)



As part of the survey, the respondents were asked to rank the security assurance capabilities of semiconductor and chipset design vendors. Intel was most recognized for its practices, with 57% of participants selecting that they were familiar with Intel's security assurance capabilities. This was followed by NVIDIA (23%), Qualcomm (11%), Arm (6%), and AMD (3%).

SUMMARY AND CONCLUSIONS

Overall, the survey highlights several insights for the technology sector, in general, and the semiconductor and chipset design vendors, in particular. There is a growing chorus of frustration and dissatisfaction for the current security assurance frameworks that are in place.

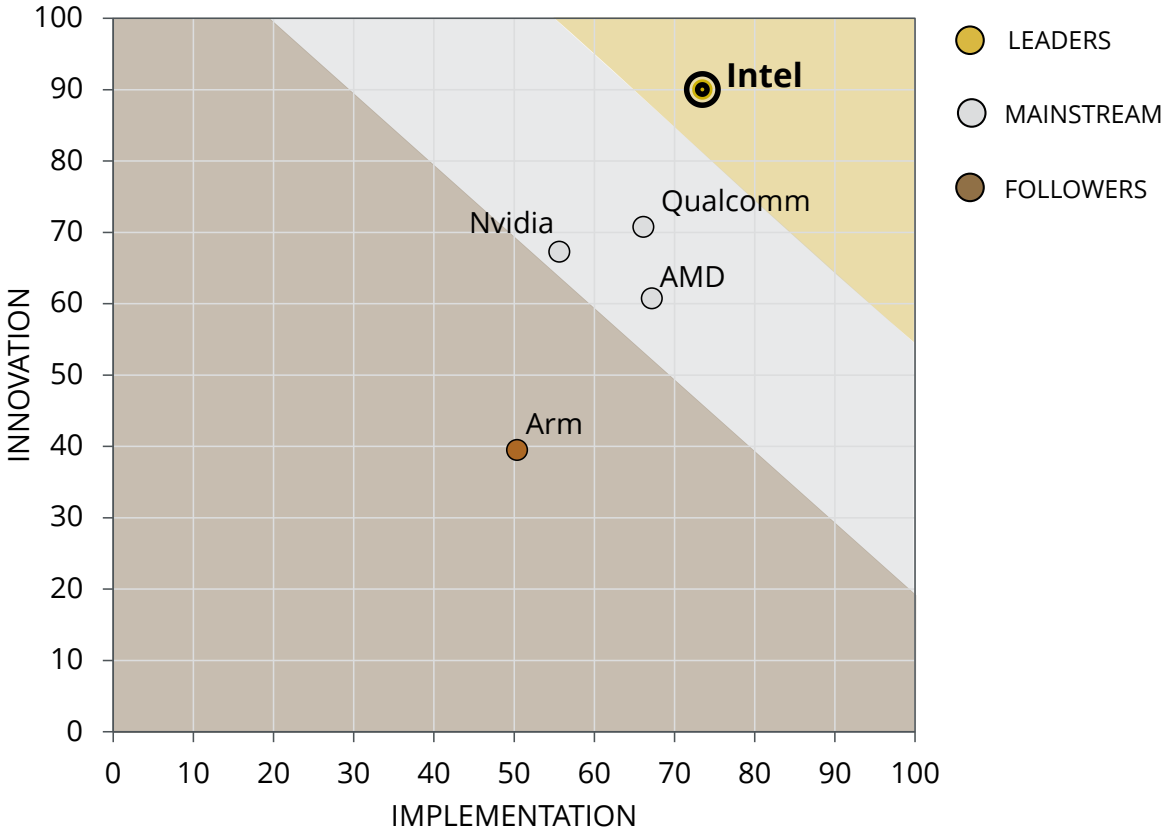
The emphasis on a strong SDL was raised consistently by enterprise respondents as the most important consideration when evaluating the security assurance framework of their source vendor. It is a feature that still needs significant improvement and one that is crucial to mitigate security threats and breaches. SDL is a process that spans the entire product lifecycle, pre to post market. It is the underlying foundation of a product's security, so it provides significant assurance and confidence for enterprise customers. This was a consistent finding throughout the survey. Vendors that are transparent with their SDL processes and practices across their product's lifecycle are more highly rated by enterprises.

Furthermore, vulnerability disclosure & mitigation, bug bounty, and PSIRT were raised as key components of a vendor's strong security assurance framework. Each of these aspects can be improved by providing greater transparency in their processes, increasing financial and personnel investment in security assurance expertise. Altogether, these aspects work in tandem to build confidence by enterprise end users that the product or solution has security in depth.

SECURITY ASSURANCE IN TECHNOLOGY: COMPETITIVE ASSESSMENT

This study conducted by ABI Research assesses security assurance in five semiconductor companies. Product security assurance focuses on the frameworks, processes, and people that improve the security of a product throughout its lifecycle. To address the increasing concerns around data security, technology companies must leverage their internal security processes like SDLs and PSIRTs. Thus, ABI Research developed this competitive assessment (CA) to offer a comparative assessment of the security assurance practices of major semiconductor vendors.

ABI RESEARCH'S VENDOR MATRIX



After individual scores are established for innovation and implementation, an overall company score is established using the Root Mean Square (RMS) method:

$$Score = \sqrt{\frac{innovation^2 + implementation^2}{2}}$$

The resulting overall scores are then ranked and used for percentile comparisons.

The RMS method, in comparison with a straight summation or average of individual innovation and implementation values, rewards companies for standout performance. For example, using this method, a company with an innovation score of 9 and an

implementation score of 1 would score considerably higher than a company with a score of 5 in both areas, despite the mean score being the same. ABI Research believes this is appropriate as the goal of these matrices is to highlight those companies that stand out from the others.

The following criteria were used to rank the vendors.

Innovation Criteria

- **Secure Development Lifecycle (SDL):** Includes architecture considerations like architectural hardening, penetration testing, secure coding, validation, and post-deployment support. Leading SDLs will be integrated at all phases of the development process and have the tooling, processes, and training to identify and remediate the root cause of any issue for both hardware and software. Leaders will also address hardware, software, and firmware considerations, and use customized processes for products. ABI Research's survey results indicated that SDL was ranked as a high priority by participants. (20% weighting)
- **Proactive Security Practices:** Leaders will leverage various mature and innovative programs (hack-a-thons, bug bounty programs, etc.), third-party and embedded solutions, and manual processes and automated tooling, including AI and ML for scanning, detection, and remediation. (25% weighting)
- **Incident Response Capabilities:** Leaders will have mature security response teams that cover various product categories, employ automation and manual remediation techniques and technologies, and provide a comprehensive disclosure policy (typically Coordinated Vulnerability Disclosure (CVD)). (25% weighting)
- **Security Center:** Leaders should have the digital infrastructure to support front-line security efforts for contacting security teams and provide access to security resources, such as CVEs (Common Vulnerabilities and Exposures), blogs, advisories, links to other programs, and guides/tools for developers. (10% weighting)
- **Security Research:** Leaders have a high level of ongoing research in academia, industry, offensive security, and other areas. Leaders should have ongoing internal and external efforts, and even use innovative programs with open-source communities and academia. (10% weighting)
- **Security Training:** Leaders will implement a range of internal training programs (across software, hardware, and firmware) to help establish a security-focused organizational culture. Programs may include one-time and ongoing training modules, such as hands-on practical exercises, customized training (for organizational roles), certifications and courses, and gamification. Leaders should have ongoing internal and external efforts and even use innovative programs with open-source communities and academia. (10% weighting).

Implementation Criteria

- **Regional Coverage:** Number of regions where the company operates. Companies with a global presence can better understand regional-specific requirements and sustain straightforward communication with customers in different locations. (30% weighting)

- **Market Influence (Market Share):** This gauges the company's influence on the market using revenue as a proxy. Revenue is derived from publicly available sources for each company that indicate revenue generated for the 2022 period. While this does not represent revenue tied exclusively to the company's security elements, it does provide insight into the scope of the company's size and operations, and its ability to invest in security R&D. (20% weighting)
- **Customer Diversity:** Number of verticals and applications that the company operates in, with leaders having a strong variety. (30% weighting)
- **YoY Growth 2022/2023:** YoY growth rate in sales. This criterion measures the company's growth and forward momentum in the industry. (20% weighting)

Table 1: Vendor Matrix Results

(Source: ABI Research)

Company	Score	Overall Ranking
Intel	82.2	1
Qualcomm	68.5	2
AMD	65.0	3
NVIDIA	61.7	4
Arm	45.3	5

ABI RESEARCH CATEGORIZES THE VENDORS INTO THREE CATEGORIES: LEADERS, MAINSTREAM, AND FOLLOWERS

The categories are described in more detail below:

- **Leader**: A company that receives a score of 75 or above for its overall ranking
- **Mainstream:** A company that receives scores between 60 and 74 for its overall ranking
- **Follower:** A company that receives a score of 59 or below for its overall ranking

Leaders: Intel

The leaders' group consists of companies that leverage highly innovative and comprehensive security assurance practices, while demonstrating high market influence and robust financial health.

Mainstream: Qualcomm, AMD, NVIDIA

The mainstream group consists of innovative companies that lag behind in implementation and, in some respects, innovation when compared to the competition.

Followers: Arm

The followers' group is composed of companies that have a niche strategy, for instance, limited capabilities and security assurance profile compared to the competition, or companies with lower implementation scores when compared to the competition.

INNOVATION RANKINGS

Intel is the top innovator of the companies assessed, scoring above 90 in innovation. Intel stands out as a leading semiconductor innovator in this assessment. The company employs a mature SDL and a variety of security programs that integrate security considerations at every stage of product development. Intel's proactive security measures are also best-in-class, leveraging robust bug bounty programs, hackathons (HaTs), and training programs. Additionally, the company's incident response capabilities constitute a highly capable team, with specially tailored training on Intel products and security areas. Furthermore, the company's innovative research and training initiatives are gamified, which helps develop a security culture throughout the organization. These characteristics together help establish the company as a foremost innovator in the field of security assurance.

Table 2: Innovation Table

(Source: ABI Research)

Company	Score	Innovation Ranking	Overall Ranking
Intel	90.0	1	1
Qualcomm	70.8	2	2
AMD	62.8	4	3
NVIDIA	67.3	3	4
Arm	39.5	5	5

IMPLEMENTATION RANKINGS

Intel is the top implementer of the companies assessed, scoring 73.5 in implementation. In 2022, Intel reported revenue of US$ 63.1 billion and exemplifies strong customer diversity across commercial (consumer) markets, government, automotive, and education sectors, and the cloud. The company has extensive global coverage, active in 65 countries across the Americas, Europe, the Middle East, and Asia-Pacific. Furthermore, the company employs close to 132,000 employees worldwide. Despite this, the company scored the lowest of the implementation criteria for YoY growth, citing a 16% decline in YoY growth in 2022, in addition to a 20% decline in its total revenue between 2021 and 2022. Nevertheless, Intel emerges as the top implementer among the vendors assessed.

Table 3: Implementation Table

(Source: ABI Research)

Company	Score	Implementation Ranking	Overall Ranking
Intel	73.5	1	1
Qualcomm	66.1	3	2
AMD	67.2	2	3
NVIDIA	55.6	4	4
Arm	50.4	5	5

INDIVIDUAL COMPANY ASSESSMENTS

The Individual Company Assessment profiles have been organized by overall score.

INTEL

Overall Score: 82.2 | Innovation: 90.0 | Implementation: 73.5

Innovation

Intel is one of the world's leading Integrated Device Manufacturers (IDMs) for semiconductors and supplies microprocessors for computer system manufacturers, motherboard chipsets, network interface controllers, and various other devices used in communications and computing. To secure this extensive portfolio of products spanning across industries, Intel employs more than 500 dedicated security staff and a robust security assurance framework that covers a particular electronic component from commercial release to years thereafter. This is achieved through a variety of systems, processes, tools, and dedicated personnel, which enable the company to embed security into its products and work culture.

Secure Development Lifecycle: Intel's security assurance framework relies on an SDL, which integrates security considerations at every stage of product development. This means that security is embedded in the entire product development process, starting from initial planning and assessment, through architecture, design, implementation, and testing, all the way to release, and ongoing post-deployment maintenance and support. Intel began exploring SDL practices in the 1990s and began wide-scale adoption of SDL practices in the early 2000s.

Intel's SDL is applied to the component level and follows a DevOps methodology, bridging the gaps between development and production infrastructure by automating infrastructure, workflows, and monitoring application performance. It is context-specific, targeting hardware, software, and firmware-specific requirements, and then identifies the SDL tooling, processes, and/or training for specific security concerns and considerations of the product. In this way, Intel states it supports a systematic approach for the specialized identification of a product's expected security risks, threat modeling, security and privacy analysis, continuous evaluation, security verification, release testing, and post-release support. Alongside this, Intel has demonstrated to ABI Research that its SDL is constantly evolving, despite having been in place for more than 20 years, especially on the automation and tooling front, to keep pace with advancements such as cloud and containers, AI and ML, and quantum-resistant cryptographic algorithms. Therefore, with Intel's SDL able to identify the unique security and support considerations for hardware, software, and firmware products at all stages of development, while evolving with new technologies, Intel's SDL scores 9.5/10.

Proactive Security Practices: Intel has stated that it leverages a variety of proactive security identification programs to help identify product vulnerabilities. Intel employs routine hands-on training experiences in the form of security HaTs and conducts more than 120 HaT events a year. Alongside this, Intel's PSIRT manages Intel's Bug Bounty Program, which leverages a Vulnerability Discloser Program (VDP), as per industry standard, and a Project Circuit Breaker program, where Intel invites elite and ethical hackers to test and evaluate pre-release technology. The Bug Bounty Program has been in place since 2017 and engages, on average, around 100 unique researchers a year and accounts for roughly 40% of all vulnerabilities addressed by Intel since 2019, with most submissions being in the

software category. Intel demonstrates its dedication to supply chain security by conducting cybersecurity controls and attestation assessments on key suppliers and vendors. The company also enforces certification among its vendors and suppliers, conducts audits, and attestations as part of its Supply Chain Risk Management (SCRM) program. With a comprehensive portfolio of proactive security processes and practices embedded into Intel products, in addition to world-class bug bounty and HaT programs, Intel scores 9/10 for proactive security practices.

Incident Response and Remediation Capabilities: Intel's PSIRT is mature, having been established in the early 2000s, and holds the responsibility of minimizing impact through the mitigation and public disclosure of security vulnerabilities. Alongside being responsible for the Intel Bug Bounty Program and ongoing security response efforts, Intel's PSIRT also manages the vulnerability handling process (identify, mitigate, and disclose), which follows the principles of CVD. Furthermore, intel was a driver in expanding Common Weaknesses Enumerations (CWEs) with MITRE to include hardware categories alongside software. Intel's PSIRT publishes security advisories, which are fixes or workarounds for CVEs discovered internally and externally, as well as announcements, product support, and other resources in a centralized webpage known as the Intel Product Security Center for easy access. Additionally, for security communications, Intel has a hub for developer guidance when it comes to security like other companies in the sector. Additionally, the assurance organization includes feedback loops that track the number of impact incidents and work with research teams to improve product architecture for future generations.

Intel leverages a unique program that preserves platforms and their design collateral, hardware, software, and documentation in a centralized location, known as a Long-Term Retention Program (LTRP). Through the LTRP, Intel maintains design collateral for over 5,500 electronic motherboards and 35,000 silicon items for live product support for up to 10 years, allowing teams to respond to reported vulnerabilities and develop mitigations quicker. Due to this program, along with a mature PSIRT that supports a range of security programs and disclosure capabilities, Intel scores 9/10 for incident response and remediation capabilities.

Security Center Operations: Intel's security center is a centralized access point for Intel's security resources and information about Intel's security approach. This includes information about the latest security updates, advisories, and resources for addressing security concerns related to Intel products. The webpage also serves as a hub for customers, developers, and security researchers to access security-related information, documentation, and tools to help protect their systems from potential vulnerabilities and threats. The site, however, does lack community forums, blogs, and links to dedicated security social media accounts with which some other sites are equipped. Overall, Intel provides a variety of security resources from CVEs, advisories, and links to other programs, and scores 8/10 for security center operations.

Security Research Activities: Intel's security research activities consist of three security research teams with different focus areas: Intel Security Threat Analysis and Reverse Engineering (iSTARE), Strategic Threats Offensive Research and Mitigations (STORM), and Offensive Security Research (OSR). These teams amount to a total of 80 researchers across 10 countries with specialized expertise, skills, and experience such as fault injection and supply chain security to automation pathfinding and embedded cryptography. Through

these teams, Intel dedicates resources toward proactive and reactive security research so that specialized teams continually monitor, test, and improve Intel products, and swiftly react to new vulnerabilities and exploits. Intel also has significant ecosystem engagement, funding 40+ academic research teams, and directly invests in academic research programs. With highly-skilled and specialized teams conducting security research within the company and across the security ecosystem, (I.e., academia and professional), Intel scores 9/10 in security research activities.

Security Training: Intel's security training is a structured and gamified training program known as the Security Belt Program. Intel personnel not only receive guided and hands-on learning of security principles, skills, and tools, but they also apply what they learn via mentorship, lead Intel's security-first culture, and influence industry practices. To date, more than 20,000 people have been trained through Intel's Security Belt Program. Intel also offers online courses, programs, professional certifications, and more through Intel Certifications and Training; however, no professional certification pathway for security is yet available. With well-structured internal programs that support hardware and software topics, Intel scores 9/10 in security training.

Implementation

Intel is a globally recognized device manufacturing company that primarily supplies semiconductor chips. With extensive regional coverage over Greater America, Europe, the Middle East, and Asia-Pacific, Intel has more than 131,900 employees located in 65 countries. It is one of the largest microprocessor manufacturers by revenue. Intel experienced a 20% decline in its total revenue between 2021 and 2022, amounting to US$ 63.1 billion in 2022. This decline may be attributed to various factors including uncertain economic and geopolitical circumstances related to inflation, the Russia-Ukraine war, supply chain difficulties, market share loss, and higher capital expenditures due to reentering the fabrication business. Nevertheless, Intel ended 2022 with a total net worth of US$ 182.1 billion in assets and US$ 32.2 billion in liabilities. Therefore, Intel demonstrates strong regional coverage with a score of 9.5/10, 7.4/10 for market influence, and 4.2/10 for YoY growth. As for customer portfolio and diversification, Intel is active in the commercial (consumer), government, automotive, and education sectors, as well as cloud service providers, among others. Thus, it receives a score of 7.4/10 in terms of customer diversity and its range of industry verticals and applications.

Concluding Remarks

In the semiconductor industry, Intel has been pioneering the way for product security assurance, placing high importance on investments in personnel, practices, and processes that embed security assurance into daily operations and silicon. Intel has adopted a "Security-First Pledge" that prioritizes customer needs in security decisions, demonstrating commitment and adaptability toward the advancement of security, robust incident response (including vulnerability management and offensive security research), community advocacy, and security.

Intel emerges as a leading company in product security assurance, with its sophisticated security assurance framework. With an exemplary SDL and incident response and remediation strategies, in addition to the long-term retention program, that has helped position Intel in first place in the competitive assessment. Moreover, the company is continuing to establish its balance in this new macroeconomic environment and challenging manufacturing environment.

QUALCOMM

Overall Score: 68.5 | Innovation: 70.8 | Implementation: 66.2

Innovation

Qualcomm is an American multinational company that designs and produces processors, modems, platforms, Radio Frequency (RF) systems, software, and services related to connectivity technologies. The company's solutions span a wide range of applications, such as mobile, smart home, automotive, IoT, audio, and Wi-Fi devices, etc. Qualcomm has employed hundreds of people to work on matters related to privacy and data security, specializing in areas such as security, privacy, information security, risk management, application security, third-party security assessments, investigations, counter-threat analysis, security operations, etc.

Secure Development Lifecycle: Qualcomm's SDL is applied at the software and hardware component levels as opposed to its competitors like Intel that cover the full range of SDL integrated security that includes firmware as well. The company adopts DevOps into practice for its SDL and prioritizes security throughout the entire product development lifecycle. In this regard, Qualcomm's security developers are trained in secure software design and development lifecycle practices, including the practice of detecting and resolving security vulnerabilities. However, the maturity of Qualcomm's SDL was not disclosed, and transparency is lacking about the company's SDL evolution over the years. Overall, Qualcomm's commitment to embedding security into its entire product lifecycle, along with its practices to enforce security assurance, enables the company to achieve an SDL score of 7/10.

Proactive Security Practices: Qualcomm has implemented a proactive vulnerability rewards program, akin to a bug bounty program, since November 2016, which offers invited researchers up to US$ 15,000 to improve the security of the Qualcomm Snapdragon family of processors, 5G modems, and related technologies. As reported by the company, the program has been successful, with almost 350 bounties, amounting to over US$ 750,000 being paid out within 2 years of its inception. Despite this, the program appears to focus on a single product line and is smaller in scope in comparison to leaders in the sector. Furthermore, Qualcomm conducts cybersecurity and privacy assessments on key vendors and suppliers to ensure safe security practices in its supply chain. There was no mention, however, of whether Qualcomm enforces specific certifications or monitoring practices on its suppliers and vendors. As a result, Qualcomm's proactive security practices score 9/10.

Incident Response Capabilities: Qualcomm operates a PSIRT that addresses security issues and vulnerabilities that are reported to it. As part of the company's policy, the team is committed to addressing and publishing information related to reported issues within 90 days. Qualcomm's PSIRT has been observed to be highly reactive and has received commendations from Binarly for its ability to manage threats and address security issues promptly. Nevertheless, the maturity and volume of the company's PSIRT has not been disclosed. Meanwhile, the company has malware protection practices in place for the real-time detection of "zero-day" threats.

Qualcomm is committed to transparency and publishes the latest discovered security vulnerabilities and related code fixed monthly via its Security Bulletin. The company is also a member of Code Aurora Forum (CAF) and actively shares information on security vulnerabilities with the CAF and the larger open-source community. On the other hand, Qualcomm is not a FIRST member, and it is unclear when its PSIRT was established. While the company's PSIRT maturity is unclear, through a combination of incident response capabilities, simple incident reporting processes, and transparent disclosure policies, Qualcomm's incident response capabilities score a 6.5/10.

Security Center: Qualcomm's dedicated security portal provides a wide range of tools for end users, such as security-related whitepapers and resources, announcements, blogposts, and the security bulletin, which updates customers on the latest security updates, discovered vulnerabilities, and patches that affect Qualcomm products.

Qualcomm also provides a range of support portals to help customers gain easy access to the resources they may require. CreatePoint provides customers with access to product kits, hardware and software documents, software code and tools, support communities, and technical support from Qualcomm. Despite these features, the security center does not provide links to other security programs the company offers, like some of the competition does. As a result of this, as well as a range of portals with readily available documentation and resources, and access to community support and Qualcomm technical assistance, Qualcomm scores 8/10 for security center.

Security Research: Qualcomm heavily invests in research and has established R&D centers around the world, primarily located in Europe, China, India, and the United States. For example, Qualcomm Research Silicon Valley is one such R&D center that is focused on conducting leading research in security-related matters. The Qualcomm Innovation Center has also been established to enable and optimize open-source software for use with Qualcomm technology. Separately, the company also contributes to the security community by publishing research papers and articles on its Security website.

Qualcomm regularly supports industry innovation with a range of initiatives, including but not limited to university programs, incubation, and mentorship programs. Funding is also available through the Qualcomm Innovation Fellowship (QIF). For example, the European QIF program recognizes and rewards researchers in the areas of AI and cybersecurity with monetary awards of up to US$ 40,000. Despite the presence of significant R&D around the world, it is unclear the number of researchers Qualcomm enlists for security or security research in general. Additionally, industry engagement and research topics appear to cover a broad spectrum and lack emphasis on security assurance, as some of the competition. As a result, Qualcomm's security research scores 5/10.

Security Training: Internally, Qualcomm provides mandatory annual cybersecurity training to over 43,500 employees. Qualcomm's developers are also trained in secure software design and development lifecycle best practices. Despite the large number of employees impacted by Qualcomm's security training, it appears that training for most of the organization covers a spectrum of security topics and does not focus on product security assurance. Furthermore, it is unclear when Qualcomm's security training programs were established, so program maturity and depth is unknown. As a result, Qualcomm scores 5/10 for security training.

Implementation

The company employs approximately 50,000 employees in 170 offices across 30 countries today. Its regional coverage spans Asia Pacific, the Americas, and Europe, with manufacturing facilities in Asia and Europe. Despite this, an estimated 62% of its business derives from China, specifically Chinese Original Equipment Manufacturers (OEMs).

In Fiscal Year (FY) 2023, Qualcomm generated a total of US$ 35.8 billion, down 19% from FY 2022 when the company brought in US$ 44.2 billion. The company experienced economic headwinds and uncertainties due to the U.S./China trade and national security tensions. Nevertheless, much of its business revenue derives from equipment and services (84%) and the remainder consists of licensing for products and services.

Qualcomm's customer diversity includes a wide range of industry verticals and applications. For instance, the company's main markets are commercial (consumer) markets, governments, IoT, and automotive sectors, service providers, and others. Qualcomm receives a score of 7.4/10 for regional coverage, 5.3/10 for market influence, and 4.2/10 for YoY growth. Despite this, the company's customer portfolio receives a score of 8.4/10 for customer diversity.

Concluding Remarks

With a heavy emphasis on proactive security practices and SDL, Qualcomm demonstrates its commitment to security in product R&D. Qualcomm further demonstrates its market standing with a comprehensive customer diversity portfolio across several markets and industry verticals. Overall, ABI Research acknowledges that Qualcomm has strong product security assurance capabilities.

AMD

Overall Score: 65.0 | Innovation: 62.8 | Implementation: 67.2

Innovation

AMD is an American global semiconductor company that designs and sells processors, graphics, adaptive Systems-on-Chip (SoCs), Field Programmable Gate Arrays (FPGAs), and related software. Most notably, AMD completed the acquisition of Xilinx in February 2022 to become one of the leading industry players in the high-performance and adaptive computing market.

Secure Development Lifecycle: AMD takes a holistic approach to SDL, covering the entire product lifecycle and value chain, beginning from the supply chain to the application layer (software). AMD's approach to SDL covers software, hardware, and firmware-specific development. While it is one of the few companies that covers all three development areas, it is unclear when the company began using SDL and for which development areas. Furthermore, it is unclear whether a waterfall, agile, or DevOps methodology is used for the company's SDL. This could impact the length of development phases' potential benefits of more iterative and collaborative development practices like an agile or DevOps methodology. Despite the company's unclear approach and maturity of SDL, the company appears to cover all development stages and hardware and software-specific development, enabling AMD's SDL to achieve a score of 7/10.

Proactive Security Practices: AMD does not appear to have a static or proactive bug bounty program in place. On the other hand, AMD does sponsor HaT events, though these seem to be on an irregular cadence and with unknown participation and outcome metrics. AMD also enforces security in its supply chain by conducting background checks and qualification processes for key vendors and suppliers. While AMD prioritizes supply chain security and risk management as key focus areas of security assurance, the company overall lacks transparency into its proactive security processes, as well as innovative programs used by other companies, such as bug bounty programs. As a result, AMD's proactive security practices scores 4.5/10.

Incident Response Capabilities: AMD's PSIRT is relatively new in comparison to other players, having been established in 2020 as indicated in its FIRST membership records. AMD's PSIRT interacts with the security ecosystem, including researchers, industry leaders, government organizations, and other vendors to report potential security issues. AMD is a member of a CVE Numbering Authority (CNA) and encourages security vulnerability reporting following the CVD framework. While the company's PSIRT is relatively new in comparison to other companies, the team appears committed to enabling a seamless incident reporting process and is consistent in maintaining security bulletins of CVEs. Therefore, through a combination of seamless incident reporting processes, and transparent disclosure policies, AMD's incident response capabilities score 7/10.

Security Center: AMD's security page acts as the company's centralized access point for CVEs, policies, procedures, and Pretty Good Privacy (PGP) key. AMD features security bulletins that date back to 2018 and is transparent about its vulnerability disclosure policy, security support policy, and AMD PGP key. The company, however, lacks security-specific whitepapers, as well as links to security research blogs, journals, and programs that help inform and update customers. As a result, AMD scores 8/10 for security center.

Security Research: Transparency on AMD's security teams, the size of the teams, and their activities are unclear. Despite this, AMD's acquisition of Xilinx is starting to show a transition in the company's transparency of security research activities. Particularly, AMD organizes the AMD Xilinx Security Working Group, which is an annual event that invites AMD customers, academia, industry partners, and governments to gather and share perspectives on the latest security topics and trends. AMD's security research appears to focus more on security technologies and less on product security assurance. While Xilinx does have some competitive work in assurance, the acquisition is still recent, and AMD's overall security research is lacking in comparison to other companies in the sector. As a result of all these factors, AMD's security research scores 5/10.

Security Training: AMD conducts periodic mandatory cybersecurity training for its 24,500 employees to cultivate awareness on the company's intellectual property and information assets. The security elements of the training, however, focus more on cybersecurity and information security, with no mention of product security assurance topics. The company also employs a Business Information Security Officers (BISO) program, which fosters active participation of individual business units in cybersecurity strategy, risk, and control discussions, and works with the cybersecurity team to identify, communicate, and manage risk. While AMD offers a wide variety of role-specific training programs, resources, and knowledge material readily available online for its customers, there is little evidence that these programs are used to train internal architects, engineers, and developers on product security. As a result, AMD scores 5/10 for security training.

Implementation

AMD is a global microprocessor chip supplier, with more than 25,000 employees as of 2022. The company has 99 corporate offices split across the Americas, Europe, the Middle East, and Africa (EMEA), as well as Asia-Pacific. AMD strengthened its financial stance in 2022. With the two acquisitions of Xilinx and Pensando Systems, the company generated a total of US$ 23.6 billion in 2022, following a 44% increase from US$ 16.4 billion in 2021. The driving factor that led to this growth may be attributed to revenue from AMD's data center, gaming, and embedded business segments. These business segments experienced higher semi-custom product sales, as well as greater product sales of Xilinx products.

AMD serves a range of customers, including but not limited to commercial (consumer) markets, governments, the IoT, and automotive sectors, and service providers, among others. The company works with OEMs, large public cloud service providers, Original Design Manufacturers (ODMs), system integrators, and independent distributors. It expanded its network of partners and customers in 2022 by expanding its product portfolio to compete against its direct competitors—Intel, NVIDIA, and Arm.

AMD receives a score of 7.4/10 for regional coverage, 1.1/10 for market influence, and 5.3/10 for YoY growth. As for customer diversity, AMD receives a score of 5.3/10 due to its range of customers and partners across industry verticals and applications.

Concluding Remarks

In 2022, AMD showed significant growth as a company and may continue to benefit from the recent AI boom. AMD has a new SDL (adapted from the acquisition of Xilinx) in place, which sets a reasonable foundation for its incident response capabilities and proactive security frameworks to follow in the future. Hence, ABI Research considers AMD to have substantial potential should it continue to build its resources and its strong product security assurance posture.

NVIDIA

Overall Score: 61.7 | Innovation: 67.3 | Implementation: 55.7

Innovation

NVIDIA is a leading fabless technology company specializing in designing and developing Graphics Processing Units (GPUs), SoCs, and software, such as Application Programming Interfaces (APIs), for applications in data science, AI, and High-Performance Computing (HPC). NVIDIA has become a pivotal player in emerging technology fields such as ML, AI, and digital twins, with its GPUs serving as the backbone. Therefore, NVIDIA's product security assurance profile is incorporated into various aspects of its products, in the form of software, hardware, and firmware.

Secure Development Lifecycle: NVIDIA incorporates SDL into all stages of its product development lifecycle pertaining to hardware- and software-specific development. The company adheres to a DevOps methodology to SDL practices, though there is no publicly available information on how mature or evolved the entire NVIDIA SDL is. Thus, the complete maturity of NVIDIA's SDL processes and practices is unclear, so it receives an SDL score of 7/10.

Proactive Security Practices: NVIDIA provides HaT programs to incentivize researchers from across the world to uncover security or privacy vulnerabilities for NVIDIA Data Processing Units (DPUs), AI, the cloud, and more. The number of these events held each year and engagement for these events is unclear. On the other hand, NVIDIA does not leverage a bug bounty program for security assurance like some of the other companies assessed. For supply chain security, NVIDIA conducts audits and other internal assessments on its suppliers to enforce a secure supply chain, specifically evaluating adherence to SO 27001, ISO 28001 and C-TPAT standards. While NVIDIA has a successful HaT program, the lack of a mature bug bounty program leaves gaps in the company's assurance practices. Therefore, NVIDIA's proactive security practices score is 5/10.

Incident Response and Remediation Capabilities: NVIDIA's PSIRT supports day-to-day incident response activities and drives the resolution of complex security incidents and investigations. The team was established in 2013 and has been evolving for the past 11 years. Additionally, NVIDIA employs a vulnerability disclosure program where researchers document reported vulnerabilities and remediate the vulnerability before disclosure, protecting existing customers from potential threats. However, NVIDIA does not guarantee specific resolutions or timelines for any given issue. With the combination of mature response teams, solutions, and disclosure policies, NVIDIA's incident response and remediation capabilities score an 8.5/10.

Security Center Operations: NVIDIA's online security resources are located on the NVIDIA webpage, Product Security. This webpage features security bulletins with CVEs, and security notices, functionality to report vulnerabilities, PSIRT policies, PGP key, links to other site resources, and blogs. Uniquely, the company provides a dedicated PSIRT social site and social media account on X (previously Twitter) to discuss security-related issues and news. While the site lacks links to other security programs and content like other company sites, NVIDIA's PSIRT social media presence enables greater reach than a single website. Therefore, the combination of resources and links available on the NVIDIA security website earns NVIDIA a security center operations score of 8/10.

Security Research Activities: NVIDIA's security research teams conduct offensive and defensive security research in the fields of AI, ML, data science, edge computing, and more. The size of NVIDIA's security research teams, however, is unclear. In general, external research activities are more focused on developing new security technologies (as opposed to researching classes of attacks and novel threat vectors that may lead to security vulnerabilities in products) and include participating in open-source security initiatives, releasing tools, industry conference participation, hosting educational competitions, and providing training. In this respect, NVIDIA does not appear to engage with security-focused research communities or spearhead internal research activities that are product security assurance-specific. However, the company has reportedly provided some opportunities that focus on AI and ML-driven security through workshops and presentations. There is room to improve with NVIDIA's security research activities and NVIDIA's security research activities score 6.5/10.

Security Training: For internal training, NVIDIA employs webinars, workshops, and annual cybersecurity awareness training of its 26,000 employees. The training does not appear to focus on product security assurance, focusing more on general security awareness like through simulating phishing campaigns across the company. NVIDIA has also not released the impact (i.e., number of trainees and investment) of its security training on

its employees. As a result of limited transparency on internal training activities that the company employs for security assurance, NVIDIA scores 5/10 for security training.

Implementation

NVIDIA is best known for providing its computing platforms (GPUs, DPUs, and Central Processing Units (CPUs)) to accelerate AI applications by integrating processors, software, algorithms, systems, and services. As of January 2023, the company employed approximately 26,196 employees across 35 countries. A significant proportion (75%) of employees are dedicated to R&D, while the remainder (25%) are involved with operational, sales, marketing, and administrative roles within the company. NVIDIA welcomed a revenue of US$ 27 billion as of January 2023, which represented flat growth for the company from FY 2022. Data centers contributed to 55% of the company's total revenue (US$ 15 billion) and experienced an upswing of 41% from 2021. NVIDIA reported that the stagnant growth may have been affected by economic and geopolitical uncertainties, aside from the unstable product supply chain. Despite this, NVIDIA launched its flagship H100, a Hopper-based GPU, designed to accelerate the training of AI transformer models in 2022. NVIDIA also expanded its data center portfolio to include DPUs during the same year. These initiatives may have contributed to the 41% growth in data center revenue for the company. NVIDIA's revenue mainly derives from the United States and Taiwan. However, revenue from outside the United States contributed to approximately 69% of the company's total revenue in 2022, down from 84% in 2021. This decline was primarily driven by the Chinese and Taiwanese markets in relation to gaming and data centers. On the other hand, the company closed 2022 with US$ 41.2 billion in total assets and US$ 19.1 billion in total liabilities. Meanwhile, NVIDIA's expertise lies mainly within data center, gaming, professional visualization, and automotive sectors, citing its main customers to be from commercial (consumer) markets, governments, the automotive industry, service providers, and others.

Overall, NVIDIA receives scores of 4.2/10 for regional coverage. On market influence and YoY growth, however, NVIDIA scores 4.2/10 and 6.3/10, respectively. Further, the customer portfolio that NVIDIA serves receives a score of 7.4/10, considering the company's expertise is only within four main markets.

Concluding Remarks

Taking account of NVIDIA's strong position with computing platforms, AI, and technological applications, the company excels within its target markets. Nvidia's strong AI strategy is expected to significantly contribute to the company's rapid growth. Due to NVIDIA's current product security assurance capabilities, this may limit its positioning against its competitors. Nevertheless, NVIDIA holds reputable market influence in the industry and is well positioned as a leader in the AI boom.

ARM

Overall Score: 45.3 | Innovation: 39.5 | Implementation: 50.4

Innovation

Arm is one of the world's leading semiconductor designers for CPUs, as well as software development tools, computing platforms, and SoC infrastructure. Arm licenses its Intellectual Property (IP) to other companies (e.g., Apple, Google, NVIDIA, Microsoft, and Qualcomm), which then use it to design and manufacture processors based on Arm's architecture. Therefore, Arm plays a central role in the semiconductor value chain as

a Third-Party Intellectual Property (3PIP, IP) provider and provides security collateral (documentation and support) for its technologies to enable partners to apply quality product security assurance processes toward their solutions.

Secure Development Lifecycle: Arm is the creator of the Platform Security Architecture (PSA) framework, which introduced security protocols such as Root of Trust (RoT) for IoT devices and services, catering to the needs of both software and device manufacturers. Arm's SDL is backed by the PSA, which indicates common principles for security design, and provides a holistic set of resources for the requirements analysis, architecture, and implementation phases of device design.

With consistent contributions via documentation, guidelines, and reference designs for Arm-based architectures, the company empowers its licensees to implement security features effectively from the conception of their solutions. Despite having extensive customized SDL methodologies to supply to its partners, as an IP-vendor, Arm does not implement these practices itself and relies on its partners to implement and follow the methodology. Hence, Arm lacks in-house deployment of these methodologies even though there would be opportunities to benefit from these processes, so it achieves a score of 1/10.

Proactive Security Practices: With a variety of foundational security practices embedded in Arm's designs, developers and manufacturers have a solid framework to build upon, enhancing the overall security posture of devices powered by Arm architectures. However, Arm has less diverse proactive security practices than some of the competition, as it does not employ bug bounty programs or HaT events to improve overall security assurance of its products. Additionally, as the company's business is fundamentally semiconductor IP, the company does not employ any supply chain cybersecurity checks or conduct background cybersecurity assessments for key vendors. Arm achieves a score of 2/10 for proactive security practices.

Incident Response and Remediation Capabilities: Arm employs a PSIRT, which defines the standardization process for handling security vulnerabilities at Arm. Therefore, like other PSIRTs, the team continually monitors Arm products for potential weaknesses and manages both the resolution and disclosure of vulnerabilities. Arm's PSIRT also collaborates with a dedicated vulnerability research team, which assists in analyzing and addressing security incidents of its partners. These teams work in tandem with a 24/7 cyber detection and response capability that uses a suite of methods and tooling to identify and contain anomalies. Despite these capabilities, the company's PSIRT is not a FIRST member, and it is unclear when it was established. Overall, through a combination of specialized response teams and industry-standard coordinated disclosure policies, Arm's incident response and remediation capabilities receives a score of 6/10.

Security Center Operations: Arm operates a dedicated and comprehensive security center under the Arm Developer Hub known as the Arm Security Center. The webpage includes an expansive catalog of guides, documentation, links, blogs, and security bulletins (CVEs) for all things related to Arm products. The webpage also acts as a central location for reporting security vulnerabilities and provides information on the PSIRT and security vulnerability disclosure process. These resources position the Arm Security Center as a centralized location for up-to-date security guidance, documentation, and knowledge. Despite this, the page does not appear to have blogs or links to special security social sites like some of the other companies in this space. As a result of the feature-rich webpages that span Arm's portfolio of products, Arm scores 8/10 for security center operations.

Security Research Activities: Arm actively engages with the security research community, taking the lead in implementing the PSA certification, and publishing numerous whitepapers on advanced subjects like resisting security threat with post-quantum cryptography and other attack vectors. Arm actively collaborates with academic and open-source research communities, including partner programs with institutions like the University of Cambridge (UK), and manages 174 Software Git repositories and 679 Arm Mbed Git repositories, a development platform and Real-Time Operating System (RTOS). Despite this, the company's research activities that are specific to product security assurance are unclear. Its major academic and industry engagement initiatives are mainly focused on IP development and training. Overall, Arm's security research activities seem to be focused more on industry engagement events and programs that focus on security as a whole and not on security assurance. Therefore, Arm's security research activities score 3/10.

Security Training: Arm offers a catalog of product security training programs annually for its 6,950 employees on a range of topics covering hardware design, software development, and system design. Alongside this, Arm has introduced a Security Champion program, which help build a security culture by advocating for security and delivering training and awareness throughout the company. The impact of these training programs (i.e., number of trainees and investments made) has not been publicly disclosed.

Considering that Arm mainly focuses on the IP development and licensing of security, its internal security training practices on hardware, software, and firmware lacks depth and maturity compared to its competitors. However, its range of product security assurance training topics alongside its security champion program show the company's dedication in developing a strong product security culture. Therefore, Arm receives a score of 6.5/10 for security training.

Implementation

Arm has established its recognized position and strong market influence as a manufacturer of microprocessors. According to the company, 70% of the global population currently uses Arm-based products; more than 270 billion Arm-based chips have been shipped as of 2023 and 50% of all CPU processors are manufactured using Arm IP.

The company has 16 offices in 16 countries across North America, EMEA, and Asia Pacific. In FY 2023, Arm generated a total of US$ 2.68 billion, experiencing a 0.9% decrease in revenue from FY 2022, when FY 2022 generated US$ 2.7 billion in revenue. Its revenue consists of licensing, royalty revenue, and miscellaneous revenue, of which royalty revenue is greater. Licensing revenue demonstrated an increase due to embedding AI-embedded services in end devices, whereas royalty revenue experienced a decrease due to slower smartphone sales and higher royalty rates.

Concerning Arm's customer profile, the company's main markets include commercial (consumer), IoT, and automotive, among other sectors (i.e., industrial, Personal Computer (PC) systems, data centers). On a similar tangent, mobile application processors are Arm's main growth driver, while cloud computing capabilities are the company's fastest-growing market. Overall, Arm receives a score of 7.4/10 for regional coverage, 1.1/10 for market influence, and 5.3/10 for YoY growth. Its customer diversity also receives a score of 5.3/10.

Concluding Remarks

While ABI Research recognizes Arm's initiatives toward product security assurance, the current framework has implications for its ranking against its competitors.

APPENDIX

GLOSSARY

Artificial Intelligence (AI): AI involves the development of Large Language Models (LLM) and algorithms so that computers may perform tasks that mimic human intelligence.

Application Programming Interfaces (APIs): The sets of tools and protocols that allow software applications to communicate with each other and share data.

Bug Bounty: A financial incentive program that rewards internal employees or independent security researchers who discover and report vulnerabilities in their products.

Common Vulnerabilities and Exposures (CVE): A standardized system for identifying and publicly describing security vulnerabilities.

Cybersecurity and Infrastructure Security Agency (CISA): The agency of the U.S. government that is responsible for protecting critical infrastructure from cyberattacks and promoting cybersecurity best practices.

Department for Science, Innovation & Technology (DSIT): The branch of the U.K. government responsible for setting policy and overseeing Research and Development (R&D) in science, technology, and innovation, including cybersecurity.

Federal Bureau of Investigation (FBI): The law enforcement agency of the U.S. government responsible for investigating cybercrimes and threats to national security.

Hackathons (HaTs): Short, time-bound, and organized hacking events during which individuals or teams (i.e., product and security teams) work together to identify and address security issues in a company's products.

Information and Communications Technology (ICT): The infrastructure and components that allow for modern computing through the technologies, systems, and tools.

Intellectual Property (IP): The creation of inventions and designs that may be used commercially.

Internet of Things (IoT): A network of physical devices that are embedded with sensors, software, and other technologies that enables devices to connect and exchange data with each other over the Internet.

Machine Learning (ML): A subfield of AI that allows computers to learn without being explicitly programmed, by analyzing data and identifying patterns and relationships.

National Institute of Standards & Technology (NIST): A U.S. government agency that is responsible for developing and promoting regulations and standards for technology.

Product Security Incident Response Team (PSIRT): The team of security experts who supports identification, mitigation, and disclosure of potential security vulnerabilities within an organization that may affect its products.

Platform Security Architecture (PSA): The design of systems to safeguard information while ensuring its integrity, confidentiality, and availability against threats.

Root of Trust (RoT): The foundation on which all secure operations of a computing system depend on, i.e., secure boot and encryption. RoT refers to the authenticity, reliability, and integrity of a system's components. RoTs must be secure by design, as they provide a firm foundation on which to build security and trust.

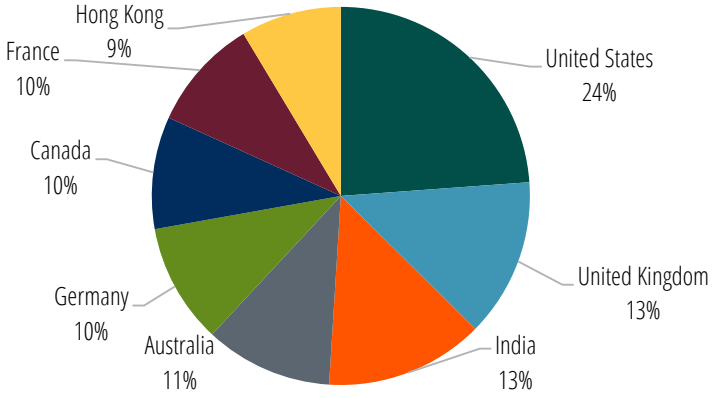
Secure Development Lifecycle (SDL): The process of applying privacy and security practices across every stage of a product's lifecycle. This encompasses software, firmware, and hardware.

Semiconductor: The material or compound substance, typically consisting of silicon, that provides the foundation for computers and other electronic devices.

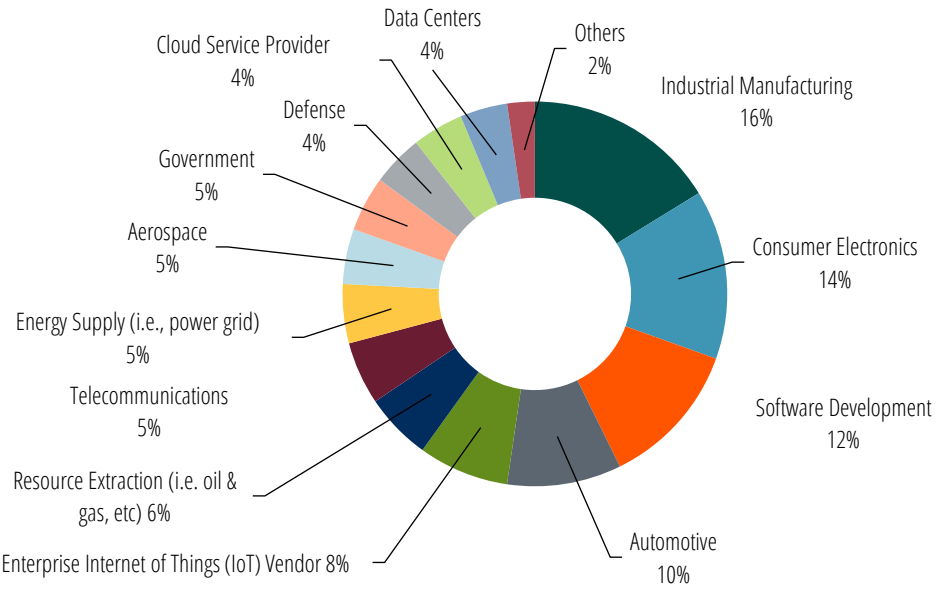
Supply Chain Risk Management Program (SCRM): A program spearheaded by Intel that provides assurance and supply chain practices to customers, complementary with their security capabilities.

Time-To-Exploit (TTE): TTE refers to the time between the discovery of a vulnerability and the successful exploitation of that vulnerability by an attacker. This metric assesses the efficacy of security measures and response capabilities.

SURVEY RESPONDENT DEMOGRAPHICS



This survey sourced its respondents from eight countries. These include the United States, the United Kingdom, India, Hong Kong, France, Canada, Germany, and Australia. The distribution was approximately 10% evenly spread across the countries surveyed, although the United States represented the largest number of respondents, with 24%.



Respondents were also qualified by industry sector. The survey included 14 distinct categories. The majority of respondents (60%) were derived from industrial manufacturing, consumer electronics, software development, automotive, and enterprise IoT. The remainder of participants were split between resource extraction (i.e., oil & gas), telecommunications, energy supply, aerospace, government, defense, cloud service provider, data centers, and others.

February 2024
157 Columbus Avenue
New York, NY 10023
Tel: +1 516-624-2500
www.abiresearch.com

WE EMPOWER TECHNOLOGY INNOVATION AND STRATEGIC IMPLEMENTATION

ABI Research is uniquely positioned at the intersection of end-market companies and technology solution providers, serving as the bridge that seamlessly connects these two segments by driving successful technology implementations and delivering strategies that are proven to attract and retain customers.