Powering clients to a future shaped by growth

A Frost & Sullivan White Paper in Partnership with Rezilion

End-to-End Software Attack Surface Management for Fast and Secure Innovation

Actively managing vulnerabilities across the entire software attack surface through discovery, prioritization, and automated remediation.

Rezilion

FROST & SULLIVAN

Contents

Security Demands in Software Development Today Are Leading to Software Supply Chain Risk Sprawl

Unprecedented Software Development to Meet Market Needs

Many industries are developing software to meet internal and external customers' vital needs. The global public cloud Software-as-a-Service (SaaS) market grew from $69 billion in 2015 to $157 billion in 2020.[1] A requirement for innovation and development to meet industries' business needs persists. The number of software users is increasing daily. Mobile users, eCommerce, and remote work contribute to the growing demand for application development. Each user has unique preferences and specifications, driving competition, application differentiation, and ongoing development.

Software Development Drivers

Lives across all countries and societies are becoming more digital. The enormous uptake of mobile and web applications creates the need for more innovation and development from companies and their coders. Pursuing innovation is a requirement for competing, but it does not come without challenges.

Increasing Compliance Burden

Compliance is a stringent requirement in certain industries. The software must comply with regulatory bodies and industry standards in highly regulated areas, such as financial services, healthcare, and connected devices. The National Institute of Standards and Technology's special publications include computer, cybersecurity, and privacy guidelines. Compliance mandates include scanning for vulnerabilities, encrypting data, and ensuring access controls. To comply, an organization must do its due diligence by ensuring its vendors and supply chain meet the required operating standards. Supply chain management is even more essential following high-profile incidents, such as the software developer SolarWinds' hacking and the subsequent supply chain incident. Organizations must monitor companies along the supply chain and the open-source code

1. Statista, 2019. "Total size of the public cloud software as a service (SaaS) market from 2008 to 2020." Last modified 2022. https://www.statista.com/statistics/510333/worldwide-public-cloud-software-as-a-service/

that many developers employ. The extensive use of code does not necessarily mean sufficient vulnerability scrutiny. The Log4Shell, a software vulnerability in Apache Log4j (a Java library for logging error messages in applications), enabled massive exploitation of victims' devices for cryptocurrency mining, ransomware attacks, sending spam, establishing backdoors, and other activities.

Security is crucial for all organizations, but in regulated industries, such as financial services, healthcare, and connected devices, enterprises face a unique challenge in achieving security and proving compliance while improving and innovating their products. Companies developing software for connected devices and SaaS companies have strict requirements for security but cannot spend all their time on patching and neglect development.

Software development, security, and operations (DevSecOps) are taking security into the software development life cycle. A core DevSecOps principle is that change implementation can quickly occur consistently across environments to ensure compliance. This approach integrates security testing and protection through automation, writing compliance policies as code to reduce human error and improve consistency. Ensuring compliance is crucial because code is vital to DevSecOps, wherein enterprises build internal code and configuration reviews into the development pipeline. Unfortunately, achieving robust compliance this way can be troublesome to achieve.

Compliance as code defined: Compliance policies are written as code and used to automate the implementation, verification, remediation, and compliance status monitoring.

Need for Innovation Creates Challenges

The requirement for innovation and development increases the volume of code. This requirement increases the complexity of managing code that third parties wrote and sourced and requires greater attention to software supply chain management. Companies are eager to experience robust compliance through automation, but this can be difficult to achieve.

To maintain security while pursuing innovation, companies must address tight timeline issues for developers, extended software supply chain risk, and friction between development and operations (DevOps) and security teams.

Achieving Innovation and Business Agility While Actively Managing Cybersecurity

Innovation and Business Agility is Leading to Development Complexity

Enterprises are pursuing innovation in software development to meet both internal and external customers' changing needs. To achieve this, developers have to create massive amounts of code while facing tight deadlines. They often lack the time to deal with extensive patching responsibilities.

The number of coders is increasing dramatically, enabling a tremendous growth in software development. There were 23 million software developers globally in 2018 and there will be 28.7 million by 2024.[2] The book Mythical Man-Month[3] claims programmers write 10 lines of code daily. This results in a huge volume of programmers writing thousands of lines of code each week and creating the principal expanding attack surface—the software attack surface. The software attack surface is the sum of all points where data can be extracted or entered without authorization. This creates a need to protect the software attack surface through continuous monitoring, discovery, classification, prioritization, and automated remediation.

In response to the tight deadlines that managers and clients set, programmers naturally want to spend more time writing code and achieving feature functionality and less time on patching. This contradiction between needs and priorities creates friction between coders, operators, and security teams. The Frost & Sullivan survey found the main challenge in pursuing DevSecOps was a lack of communication between teams. With no open communication, conflicting priorities, and tight deadlines from managers and clients, friction exists between DevOps and security teams. While DevOps teams care about security, they face a dilemma in how to best use their time and require a way to reduce unnecessary activities.

28.7 million

global software developers by 2024

> **Top challenge in pursuing DevSecOps was a communication deficiency between teams.**
>
> Frost & Sullivan C-level survey

2. Statista, 2021. "Number of software developers worldwide in 2018 to 2024". Last modified 2022. www.statista.com/statistics/627312/worldwide-developer-population/
3. Brooks Jr, F. P. (1975) 1995, The Mythical Man-Month, Addison Wesley Longman Publishing Co., Boston.

Extended Software Supply Chain

Developers use third-party code to drive innovation and meet business needs. This draws on other developers' work and enables faster end product development, making it more complex for businesses to identify patches and implement a robust patching system. Developers drawing code from other sources increases the potential for vulnerability and increases threat management complexity.

The most prevalent challenge for threat analysts when supporting incident response processes globally in 2021[4] was systems generating too many low-value alerts. This noise affects an analyst's ability to focus on essential items requiring remediation. Further, a Frost & Sullivan survey found that most organizations do more than half of their code risk management manually.[5]

> **Most organizations do more than half of their code risk management manually.**
>
> Frost & Sullivan C-level survey

The Need for Software Attack Surface Management (SASM)

Detecting and remediating vulnerabilities is a challenge that results in slower innovation or less security. Spending more time ensuring security detracts from innovation, while spending less time on security results in many unaddressed vulnerabilities in innovation pursuits.

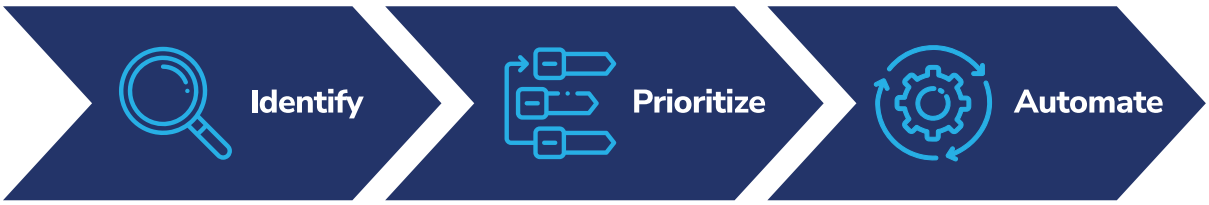
Organizations require a SASM approach that considers the many disparate code sources and actively patches as necessary. To identify patch requirements, visibility is paramount. Identifying and monitoring vulnerabilities is a major challenge without a clearly defined perimeter. Low-value alerts lessen productivity, meaning prioritization is necessary for efficiency. Spending time on remediation takes away from innovation, which means automation is integral to a productive vulnerability management platform.

4 Statista, 2021. "Challenges faced by threat analysts when supporting incident responses worldwide 2021". Last modified 2022. https://www.statista.com/statistics/1273782/threat-analysts-challenges-incident-response-processes/

5 Frost & Sullivan, March 2022 "C-Level Survey on Cybersecurity in the Republic of Singapore, the United States and Australia."

Best Practices: Prioritizing the Exploitable and Implementing Automation

Enterprises must recognize all vulnerabilities and their exploitability within their organizations. Securing the supply chain is much more difficult without the visibility of the relationships between software components. Frost & Sullivan recommends 3 best practices to protect the enterprise and the extended software supply chain.



Identify with a Dynamic Software Bill of Materials (SBOM)

An SBOM is an inventory of all software components present in an environment and contains the supply chain relationships. An SBOM is useful for anyone who produces, chooses, or operates software because it enables developers to build and maintain software, including all the components that rely on code being written or changed. A dynamic SBOM responds to real-time changes in the software environment to create and maintain an accurate software supply chain. This ability is vital for organizations that build and manage many software products. During the build phase, the dynamic SBOM supports testing for vulnerabilities while integrating the changes to code in real time. Upon release, the dynamic SBOM continues to reflect any software changes. When using a traditional SBOM, concurrent versions often occur with no reconciliation, leading to missing components and complex version management. With patch deployment, the SBOM must reflect the changes. A dynamic SBOM shows the organization's software components and provides accurate and real-time information. Using a dynamic SBOM provides visibility and enables security control management and implementation across the attack surface, from development to production.

Prioritize with Focused Vulnerability Management

Using software components in organizations will affect vulnerability perception. Effective vulnerability management relies on an active approach, using vulnerability validation. Rather than treating each vulnerability, organizations should analyze the data to reveal if any vulnerability is exploitable and how applications use it. Using run-time analysis to monitor the behavior of applications and information from a dynamic SBOM, it becomes clearer where actual threats lie. For example, if some code has a vulnerability but is not in the memory, it may not be as crucial to patch, and developers can prioritize other vulnerabilities

With better information, organizations can filter the noise and prioritize the most dangerous vulnerabilities or the ones that affect the most applications. By prioritizing the threats and dealing with the most impactful first, developers can focus on vulnerabilities their organization's policy defines as exceeding their risk tolerance. Ultimately, this practice reduces patching efforts and leaves developers more time to innovate.

React with Automation

Without automation, visibility and prioritization are not feasible. An automated and dynamic SBOM is integral to providing real-time component visibility. Further, the means of scanning and filtering vulnerabilities must be automated to reduce remediation time and enable companies to benefit from this approach. Using dynamic tools to monitor vulnerabilities helps organizations catch and remediate the most essential vulnerabilities before exploitation. This addresses the recent concerns with supply chain vulnerability management, allowing organizations to use third-party or open-source code while negating the risk.

The ideal process should employ scanning automation and filter vulnerabilities based on exploitability and policy definition and then remediate the vulnerabilities, starting with the most detrimental. This process ensures greater time efficiency, less inappropriate action, and a better relationship between DevOps and security teams.

Medical Software Developer Reduces Patching by 75%

Patching and vulnerability management are especially important to reducing a medical software developer's burden. Because the company is in the medical field and works closely with physicians, it must document all patches and provide information upon request to the Food and Drug Administration. Engineers were manually identifying, patching, and recording, drawing focus away from product development. The company sought a better way. It worked with the automated DevSecOps platform provider, Rezilion, to achieve a 75% reduction in patching by identifying the real risks. Rezilion provides the company patching reports and container certification reports to inform it where teams should spend their time for a release, based on the number of loaded and high-risk vulnerabilities. This allows the company to focus on the packages that will have an immediate impact and save the not-yet-loaded packages for later. The result is a sustainable vulnerability management practice that reduces unnecessary time on patching and provides the highest security level at any given time based on the company's activities.

Other companies were able to reduce patching efforts:

A global industrial equipment manufacturing company **reduced its patching by 77%.**

A European online marketplace platform **reduced its patching by 82%.**

A mobile applications development and analytics company **reduced its patching by 80%**

A recent research study published by Rezilion discovered that **85% of the vulnerabilities discovered in 20 public container images and hosts were not exploitable.**[6]

6 Rezilion, 2022. "A Matter of Patch: Managing Vulnerabilities with Runtime Memory Analysis". Last modified 2022. https://www.rezilion.com/runtime-analysis-research/

Excelling in Development Efficiency While Achieving Secure Innovation

Through dynamic SBOM and automation, businesses can improve efficiency and outcomes from development to production. It costs less to reach feature functionality when developers spend less time on patching and more on coding. Without diverting as much time to patching, developers become more productive and can innovate faster and more securely.

With specific policy and threshold definitions, remediation and expectations are more explicit and DevOps and security teams feel more in sync. Policies define priority and thresholds set the limit for actionable alerts. Prioritization reduces low-value alerts, meaning the security team is freer and DevOps teams appreciate spending less time on patching. Using prioritization and automation diffuses friction between teams and leads to better and more secure collaboration and innovation. Ultimately, the approach is more secure, as it promptly deals with the most significant threats.

About Rezilion

Rezilion's platform automatically secures the software you deliver to customers. Rezilion's continuous runtime analysis detects vulnerable software components on any layer of the software stack and determines their exploitability, filtering out up to 95% of identified vulnerabilities. Rezilion then automatically mitigates exploitable vulnerabilities across the SDLC, reducing vulnerability backlogs and remediation timelines from months to hours, while giving DevOps teams time back to build.

Learn more about Rezilion's software attack surface management platform at www.rezilion.com and get your 30-day free trial.

FROST & SULLIVAN

Growth is a journey. We are your guide.

For over six decades, Frost & Sullivan has provided actionable insights to corporations, governments and investors, resulting in a stream of innovative growth opportunities that allow them to maximize their economic potential, navigate emerging Mega Trends and shape a future based on sustainable growth.
Contact us: Start the discussion