Contrast SECURITY

WHITE PAPER

Navigating turbulent times: How businesses will need to overcome adversity in 2023

Businesses have overcome incredible challenges over the past few years and have experienced considerable change. The global pandemic that began in 2019, Russia's invasion of Ukraine in 2022 and the long-term impact of inflation will have prolonged effects on the economies of many countries. Economic challenges, combined with an ever-growing pool of new technologies, will require businesses to adapt and grow more resilient than ever.

Look back at 2022

Looking back at 2022, it was a year that presented significant challenges in the realm of cybersecurity. A recent study by Akamai Technologies revealed that web applications and application programming interfaces (APIs) were the primary targets of cyberattacks, with an alarming increase of 257%. These attacks were highly sophisticated and affected a broad range of organizations across various industries. One of the most concerning developments was the 3.5x growth in app and API attacks on financial services, which represented the most significant year-over-year growth in any attack vector, apart from gambling. This necessitated businesses to allocate more resources toward cybersecurity and to implement more advanced security measures to safeguard themselves. Organizations had to remain vigilant and adapt their strategies continuously to keep up with the rapidly evolving cybersecurity landscape and stay ahead of potential threats.

What to anticipate in 2023

1. TIGHT BUDGETS AND HEADCOUNT REDUCTIONS

All that hiring is finally catching up to tech companies, with more than 105,000 job cuts within the tech sector. These increasing numbers of layoffs are not isolated to just the Bay Area or startups. As of Dec. 13, 2022, a total of 54 cybersecurity firms had announced layoffs or some sort of restructuring. These retrenchment movements are not without cause. According to the 2023 State of IT report, a majority of companies are taking steps to encounter a recession in 2023, and businesses are taking steps to brace for economic impacts.

Cybersecurity professionals are a scarce resource, and they're always in demand. But when times get tough, IT departments are forced to make hard choices about where they spend their limited budgets. It makes sense that cybersecurity is often affected dramatically until budget constraints are lifted.

The financial damages from cyberattacks are expected to exceed $10.5 trillion annually by 2025; according to McKinsey, every size of the organization will need to invest more in its defenses and work closely with its developers to address attacks earlier in the Continuous Integration/Continuous Deployment (CI/CD) pipeline.

For small and midsize businesses, the challenge is doubled. Smaller businesses must compete against larger enterprises for talent while improving their application release rates.

For security teams, this equates to creating more secure applications and environments. Contrast Security Assess is a powerful tool that addresses this exact problem. Contrast Assess works toward reducing the need for traditional security experts by improving the accuracy and efficiency of existing security methods to increase protection against cyber threats without compromising any aspect of efficiency or accuracy. It is easy to use and works with developers early in the development cycle to eliminate vulnerabilities as the application is being produced.

2. THE BACKLASH OF SHIFTING RESPONSIBILITY

There is a strong backlash against shifting responsibility too far left. Rather than placing the majority of the burden on developers, security teams need to focus on best integrating security practices into the application development process. Such a shift will involve collaboration between all parties to ensure security is considered and implemented throughout the process. By taking a collaborative approach to security, we can create applications that are secure and meet the needs of all stakeholders.

Security must be embedded within every phase of DevOps, not just as a separate stage. It's not about shifting security left or right; instead, it's about ensuring that security architecture is correctly integrated into the DevOps pipeline. Companies must remember that security is a fundamental function of the right — i.e., the operations part of the DevOps cycle that ensures performance, resilience and reliability — and that not all aspects of security can be shifted left. We must also understand that prevention and detection are not mutually exclusive; rather, they are intertwined and mutually reinforcing. Every failure in prevention must be identified and addressed through detection. In the end, security is an integral part of the DevOps cycle, and it's essential to ensure that it's properly implemented throughout the entire DevOps workflow.

3. RISE OF CLOUD-NATIVE APPLICATIONS

The COVID-19 pandemic accelerated digital transformation initiatives for many businesses. For many, this entailed embracing Cloud-Native Application Protection Platform (CNAPP) to enable rapid deployment of software. The downside? Increased security risks across cloud environments.

Cloud-native applications are designed to take advantage of the scalability and flexibility of cloud computing environments.

While cloud-native applications offer many benefits, they also pose unique security challenges. These applications require a different approach to security, as they are often distributed across multiple cloud environments and may involve third-party libraries and frameworks.

The proliferation of microservices, the increasing use of third-party libraries and frameworks, and the complexity of application architectures are all increasing. This complexity can make it difficult to secure applications effectively. The global CNAPP market is projected to grow from an estimated $7.8b in 2022 to $19.3b in 2027 with a compound annual growth rate (CAGR) of 19.9%.

4. THE EFFECTS OF SECURITY DEBT ARE CATCHING UP

The aggregate build-up of security debt is dragging companies behind. A large contributor to these vulnerabilities comes from open-source software. Companies have shifted to purchasing commercial off-the-shelf (COTS) products. According to CVE.icu, there were 25,087 Common Vulnerabilities and Exposures (CVEs) documented in 2022 — an increase of 20% from 2021 — and this number has been increasing drastically year over year.

The backlog of unresolved vulnerabilities within an organization's application creates friction that slows down the release of new applications, ultimately slowing down innovation.

The discovery of a new vulnerability can cause a ripple effect of activity across the enterprise, from investigation and patching to remediation and follow-up. As a result, security team members often find themselves in a reactive mode, reacting to new vulnerabilities as they are discovered rather than proactively securing their networks. Snyk's State of Open Source Security Report 2022 states that it takes up to 148 days to remediate a critical vulnerability in a .NET application, while it can take 118 days for a JavaScript application.

While security teams keep up with the speed of DevOps, one way to mitigate against open vulnerabilities is to protect against them using Runtime Application Self-Protection (RASP).

RASP is a useful tool for protecting against open-source software because it can detect and block malicious activity in real time, even if the application contains vulnerabilities. This is especially important when dealing with unknown, untested and difficult-to-patch code.

5. GREATER EMPHASIS ON COMPLIANCE

Governments worldwide are taking increased action to safeguard citizens' data privacy. Gartner forecasts that by 2023, 65% of the world's population will have their personal data protected under modern privacy regulations, up from 10% in 2020. One thing that we learned in 2022: The cost of data breaches can break an organization.

The push toward compliance is driven by the following three main factors:

1. President Biden's administration is prioritizing cybersecurity and has issued several executive orders aimed at modernizing cyber defenses and enhancing the nation's ability to respond quickly and efficiently to threats. One of the orders seeks to promote the rapid sharing of threat information by removing existing barriers. This has resulted in IT and OT service providers updating their contracts and standardizing processes to clarify their information-sharing responsibilities. Other measures include enhancing the federal government's visibility into threats while ensuring the privacy of companies and citizens, and modernizing through the implementation of Zero Trust Architecture, secure cloud services and personnel training.

2. The Office of Management and Budget (OMB) issued Memorandum M-22-18 mandating that all federal agencies and their software suppliers comply with the NIST Secure Software Development Framework (SSDF) NIST SP 800-218 and the NIST Software Supply Chain Security Guidance whenever third-party software is used on government information systems or otherwise affects government information.

3. The Securities and Exchange Commission (SEC) has proposed a new regulation titled Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. The regulation would increase SEC scrutiny of public businesses' cybersecurity-related activities, decision-making processes and the board's role in cybersecurity oversight. The proposal highlights the SEC's growing focus on cybersecurity and introduces more stringent guidelines for companies to follow when disclosing and supplementing material cybersecurity events. One key requirement is for public company boards to oversee and participate in the evaluation, assessment and implementation of cybersecurity policies and procedures.

Increased compliance requirements present a significant challenge to organizations in staying up-to-date with ease. Choosing the right tools and technologies can help them ensure their applications comply with relevant regulations and standards.

The road ahead to overcome adversities

To overcome these challenges, organizations can leverage products like Contrast Assess, Contrast Protect and Contrast SCA to enhance their security posture.

Contrast Assess helps address the increased security risks associated with cloud-native applications by integrating security early in the development cycle, allowing developers to eliminate vulnerabilities as they are being produced. This tool not only reduces the need for traditional security experts but also improves the accuracy and efficiency of existing security methods.

Contrast Protect, a RASP solution, can be invaluable in protecting against open-source software vulnerabilities. It can detect and block malicious activity in real time, ensuring application security even in the presence of unknown, untested or difficult-to-patch code.

Lastly, Contrast SCA can aid businesses in managing their security debt and staying compliant with ever-evolving regulations. By providing insights into open-source software risks, it allows organizations to remediate vulnerabilities and maintain compliance with regulations such as the NIST SSDF and the SEC's Cybersecurity Risk Management guidelines.

Contrast Security provides the industry's most modern and comprehensive Application Security Platform, removing security roadblocks inefficiencies and empowering enterprises to write and release secure application code faster. Embedding code analysis and attack prevention directly into software with instrumentation, the Contrast platform automatically detects vulnerabilities while developers write code, eliminates false positives, and provides context-specific how-to-fix guidance for easy and fast vulnerability remediation. Doing so enables application and development teams to collaborate more effectively and to innovate faster while accelerating digital transformation initiatives. This is why a growing number of the world's largest private and public sector organizations rely on Contrast to secure their applications in development and extend protection in production.

240 3rd Street
2nd Floor
Los Altos, CA 94022
Phone: 888.371.1333

Contrast SECURITY

contrastsecurity.com