GIGAOM

GIGAOM CxO BRIEF

COMMISSIONED BY:

ZIMPERIUM®

The Imperative of Mobile Application Security Platforms

SECURITY & RISK

GIGA
OM

GigaOm CxO Decision Brief:

The Imperative of Mobile Application Security Platforms

Solution Overview

Mobile app security is crucial, often outweighing functionality in importance. Zimperium’s Mobile Application Security (MAPS) offering provides an essential, integrated suite covering pre-release testing, app hardening, run-time protection, and cryptographic key protection, streamlining the security lifecycle for CTOs prioritizing robust defense in today’s threat-laden digital landscape.

Benefits

Mobile application security ensures early vulnerability detection, enhancing app resilience and compliance, especially in sensitive data sectors. It offers real-time threat monitoring with remediation, protecting against evolving threats, reverse engineering, and data theft. Finally, intellectual property protection and safeguarding source code and in-app data is a cornerstone, addressing key attack vectors.

Urgency

The surge in mobile apps has heightened their risk for cyber threats, compelling CTOs to emphasize client-side security to prevent data breaches, uphold compliance, and safeguard their reputation. Zimperium’s MAPS emerges as a pivotal solution in fortifying app defenses.

Impact

Implementing MAPS can shift an organization toward a security-first mindset in mobile app development, enhancing its security posture. Zimperium’s continuous testing tool allows for ongoing remediation, optimizing the time spent on mobile pen testing.

Risk

Ignoring mobile app security risks data breaches and erodes trust. Regaining trust is too costly to be worth the risk when the tools exist to mitigate the issue.

01 Solution Value

Commissioned by Zimperium

IN TODAY'S DIGITAL LANDSCAPE, where mobile applications are vital for business operations, the importance of mobile application security cannot be overstated. It's essential for CTOs to acknowledge that ensuring the security of mobile applications is as crucial as their functionality and performance and, in some cases, even more critical. We live in a world where the economic impact of a sluggish mobile application is far less damaging than an insecure one. In this context, platforms like Zimperium's Mobile Application Protection Suite (MAPS) offer an integrated solution, demonstrating the effectiveness of dedicated mobile app security tools.

Mobile application security involves several distinct stages to provide a holistic security framework. The pre-release testing stage is most critical because the more security issues we can resolve before release, the better the application will survive in the wild, and the better the application team will approach security as a whole (it is fundamental to the DevSecOps lifecycle). Once the application is published, your responsibilities do not end. We are not lucky enough to live in a world where all vulnerabilities align with our development and release cycles, so run-time protection is vital. Run-time protection can be divided into subcategories, where one focuses on protecting the application and the other on protecting the intellectual property within the application. Finally, we have cryptographic key protection, which is designed to protect sensitive data against specific device attacks seen in the wild.

IT organizations can struggle to apply disparate tooling that meets the maturity and capability requirements of the business. It is not uncommon for organizations to go from no mobile application security tools to a full lifecycle protection solution, often leading to the adoption of multiple tools that do not integrate well (or at all). Zimperium supports a full range of customers by providing a distinct offering at each stage that communicates and integrates with a centralized management and reporting console. These purpose-built tools address the needs of each stage (and the teams that manage those stages) while giving you the integrated management and reporting capabilities of a monolithic platform.

02 Urgency & Risk

WIDESPREAD PROLIFERATION OF MOBILE DEVICES and applications pose a challenge to enterprises, which must secure these assets or risk significant consequences.

Urgency

The proliferation of mobile applications has made these devices prime targets for cyber threats. CTOs must prioritize mobile app security to protect against data breaches, ensure compliance, and maintain their organization’s reputation. Advanced solutions like Zimperium’s MAPS can be a game-changer in this regard.

As a SaaS offering, mobile application security needs to be available where you need it most, so we recommend looking at a provider that can match your needs. Zimperium has a global server availability across multiple regions, ensuring reliable service and seamless performance, as shown in Figure 1, with plans to integrate new regions every quarter.

Risk

Neglecting mobile application security needs before and after release can lead to dire consequences, including data breaches, legal penalties, and loss of customer trust. While integrating solutions to address these challenges, CTOs should be aware of the complexities involved and plan for effective implementation. Zimperium MAPS seeks to mitigate this risk through a unified platform approach that addresses the entire lifecycle of mobile application security.

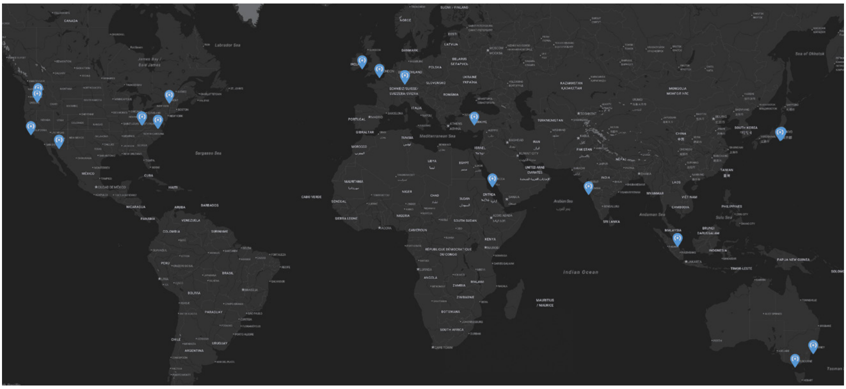
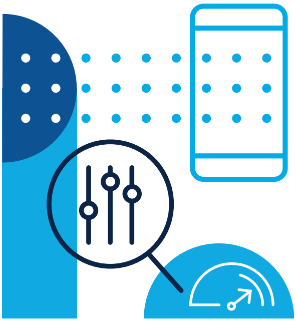


Figure 1. Zimperium’s Global SaaS Infrastructure Reach

03 Benefits

ZIMPERIUM MAPS PROVIDES an integrated suite that secures mobile applications against attack. Capabilities like early vulnerability detection and real-time threat monitoring enhance app resilience and compliance, especially in sensitive data sectors.

- **Early vulnerability detection:** Identifying security risks during development and pre-release testing saves time and resources.
- **Enhanced compliance:** Maintaining regulatory standards is crucial, particularly in sectors handling sensitive data.
- **App resilience:** Protecting apps against reverse engineering and data theft is vital in safeguarding intellectual property and customer trust. The MAPS platform does this while optimizing for app performance and size.
- **Real-time threat monitoring and remediation:** Continuous monitoring and on-device protection are key in a landscape where threats evolve rapidly. Better tools provide for protection and remediation as part of the platform. Monitoring without remediation is not an ideal solution. The Zimperium MAPS platform does both.
- **Intellectual property protection:** Protecting the application source code and data stored (and accessed) within the application is a key component of the Zimperium MAPS platform and an attack vector you must protect against.

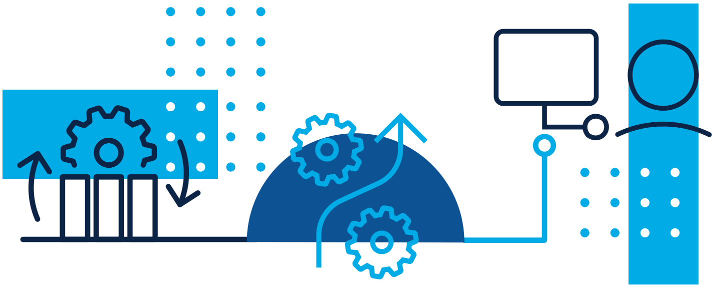


Continuous monitoring and on-device protection are key in a landscape where threats evolve rapidly.

04 Best Practices

TO GET THE MOST OUT OF ZIMPERIUM MAPS mobile application security, it's important to prioritize action and planning around available processes and resources. Among best practices to consider:

- **Crucial for business operations:** As enterprises increasingly rely on mobile apps, ensuring their security is non-negotiable.
- **Comprehensive approach:** Solutions like Zimperium's MAPS offer a holistic approach, covering the app lifecycle from development to post-release and end-user use.
- **Key to DevSecOps:** Integrating security testing into the development lifecycle is central to a robust DevSecOps strategy.
- **Evergreen security:** Tools that do not require a new application release to update the security protection are critical to maintaining a secure posture. Update cycles are driven by the mobile device owner, so you need to overcome delays in security posture that requires app releases. Zimperium MAPS uses a policy engine to constantly update protections over-the-air without requiring application updates. By using MAPS, the app receives autonomous updates on new detections to stay on top of evolving threats.



Solutions like Zimperium's MAPS offer a holistic approach, covering the app lifecycle from development to post-release and end-user use.

05 Organizational Impact

A DEDICATED MOBILE APPLICATION security suite like MAPS will enhance the overall mobile application security posture. It leads to a culture shift toward a more security-focused approach in mobile app development and operations.

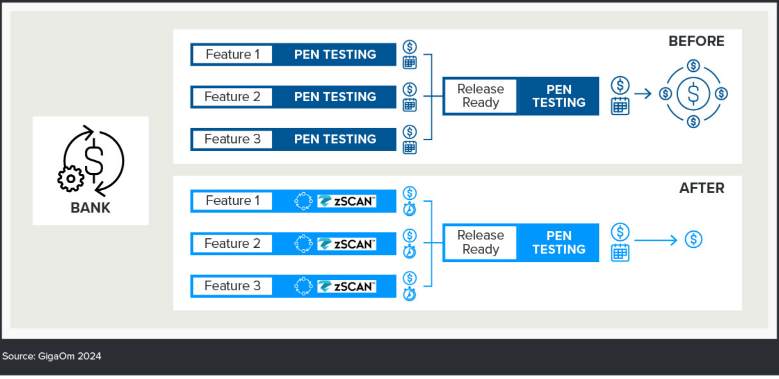
Adopting an advanced mobile application lifecycle security solution requires CTOs to drive a security-centric culture within app development teams. This move will elevate the organization's security maturity and customer trust.

There is a knock-on effect that can improve both security and speed of release. Typically, organizations make a trade-off between testing (mobile pen testing) and remediation. Zimperium allows customers to have a continual testing tool that gives developers unique insights and time to remediate. Since the average mobile pen test activity is four weeks, that time can be used to remediate and release rather than pause and wait for a report from the pen test teams.

Figures 2 and 3 show a pair of different scenarios where Zimperium's zScan automated pen testing saves money and time. In the first example, a bank exchanges manual pen testing, done in parallel, for zScan automated testing features, which speeds testing and lowers cost.

GIGAOM

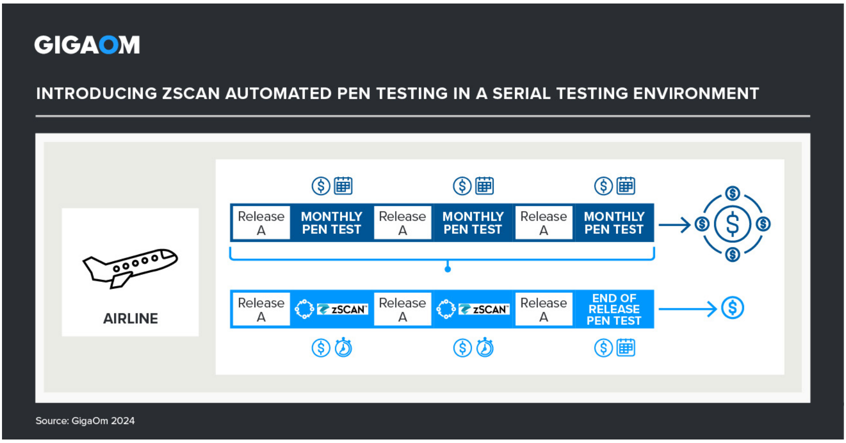
INTRODUCING ZSCAN AUTOMATED PEN TESTING IN A PARALLEL TESTING ENVIRONMENT



Source: GigaOm 2024

Figure 2. Updating a Parallel Testing Process with Automated zScan Pen Testing

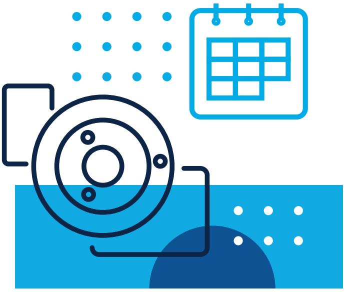
In the second scenario (Figure 3), an airline that conducts testing in a serial fashion deploys zScan to save time and money.


GIGAOM

INTRODUCING ZSCAN AUTOMATED PEN TESTING IN A SERIAL TESTING ENVIRONMENT

Source: GigaOm 2024

Figure 3. Updating a Serial Testing Process with Automated zScan Pen Testing



Since the average mobile pen test activity is four weeks, that time can be used to remediate and release rather than pause and wait for a report from the pen test teams.

In both scenarios, the time savings can be used to provide remediation of discovered issues without the impact on timelines that a traditional pen test would produce.

This allows your organization to gain significant value and deliver more secure applications—protecting your business and reputation and making you a good custodian of your customers' trust.

People Impact

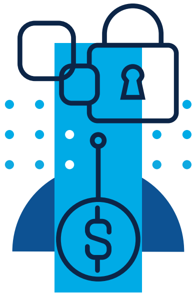
Mobile application security solutions involve two or three parts of the larger technology organization. Development teams need to integrate continuous security testing and application shielding into their workflows. Security and IT teams need to integrate and manage the real-time protection tools into theirs. A unified central reporting tool eases the requirements around communication and collaboration. Among the required motions are:

- Upskill IT staff in advanced security testing tools.
- Encourage a proactive security mindset across development teams.
- Foster continuous learning to keep pace with evolving cyber threats.
- Change operational workflows to leverage the capabilities of the platform efficiently.

Investment Outlook

Investing in a comprehensive mobile application security platform is a strategic decision. While initial costs might seem significant, the long-term benefits in risk mitigation and regulatory compliance are substantial.

The high cost of a full lifecycle platform investment can be offset by licensing only the tools your organization is prepared for and building the investment (both people and tools) over time. We also recommend understanding your scope and licensing requirements by using a method and license type that best fits your organization's needs. Since these tools are delivered as a service, you can change licensing easily as your organization evolves and needs change.



Investing in a comprehensive mobile application security platform is a strategic decision. While initial costs might seem significant, the long-term benefits in risk mitigation and regulatory compliance are substantial.

06 Solution Timeline

DEVSECOPS CAN BE HARD TO IMPLEMENT in meaningful ways. Here we provide guidance on adoption and future planning around mobile application security platforms.

Plan, Test, Deploy

As with any new technology, we recommend customers run a proof of concept with an existing code release. This will allow you to use the existing release as a baseline and measure the value the platform delivers without also impacting existing schedules and code work. This allows you to measure the points of impact and document the changes required for integration in the teams.

Plan

Integrate mobile-specific security testing early in the development lifecycle to gain visibility into app risk posture.

Test

Use comprehensive tools like MAPS for in-depth vulnerability assessments and in-app protection.

Deploy

Ensure continuous monitoring and dynamic threat response post-deployment.

Future Considerations

CTOs should anticipate and plan for evolving security challenges, considering advancements in threat landscapes and regulatory requirements.

CTOs should work with their peers in IT and security to leverage a cohesive platform that allows all members of the development and support teams to communicate using a single record of authority.

This allows everyone to see the same information and avoid delays in communication and resolution, improving team morale and cross-team collaboration.

07 Analyst’s Take

FROM AN ANALYST’S PERSPECTIVE, the demand for mobile application security is driven by the rapid evolution of cyber threats and the expanding role of mobile applications in business processes. In this context, Zimperium’s MAPS emerges as a robust solution that effectively bridges the gap between agile mobile app development and stringent security requirements. Analysts view this integration of security into the app development lifecycle as essential, aligning with market trends and regulatory demands. Zimperium’s approach, combining AI-driven threat detection with a comprehensive suite of protection tools, is seen as well-aligned with the current and future needs of businesses that prioritize mobile security.

Why Zimperium?

While focusing on the broader need for mobile application security, Zimperium stands out as a quality vendor. Its MAPS solution provides:

- **Centralized security management:** With a unified platform for threat visibility and in-app protection.
- **Proactive threat defense:** Leveraging AI and machine learning for real-time threat detection.
- **User-device-focused protection:** Offering security solutions tailored for diverse end-user environments.
- **Keep security current:** Teams can keep up with evolving threats without having to constantly publish updated versions.
- **Solutions that fit your business needs today and as you evolve:** The MAPS platform integrates four Zimperium tools in one console, but you can start with the tool, or tools, that make the most sense for you today, adding others as your capabilities change over time.

08 About Howard Holton

HOWARD HOLTON IS AN ANALYST AT GIGAOM. He has worked in IT for three decades, the last half in executive leadership, as a CIO and CTO. He has been an engineer, an architect, and a leader in telecom, health care, automotive, retail, legal, and technology.

In the last decade, Howard focused on cloud technology and economics, data analytics, and digital transformation. As CTO of Hitachi Vantara, he spent his time developing digital transformation, IT, and data strategies for Fortune 1000 companies and global governments.

His years at Rheem Manufacturing, Hitachi Vantara, and others provided the experience that helped him develop a mind for leadership—the successful execution of vision and culture to inspire. Successful leadership is all about maximizing your team's potential, as Howard has demonstrated over the course of his career.

Howard is also a technologist at heart; passionate about how data science and new technologies can be used to accelerate time-to-market and better serve the customer, now and in the future. Howard has been a trusted advisor and agent of change to a number of organizations, bringing vision and successful execution to internal and external customers alike.

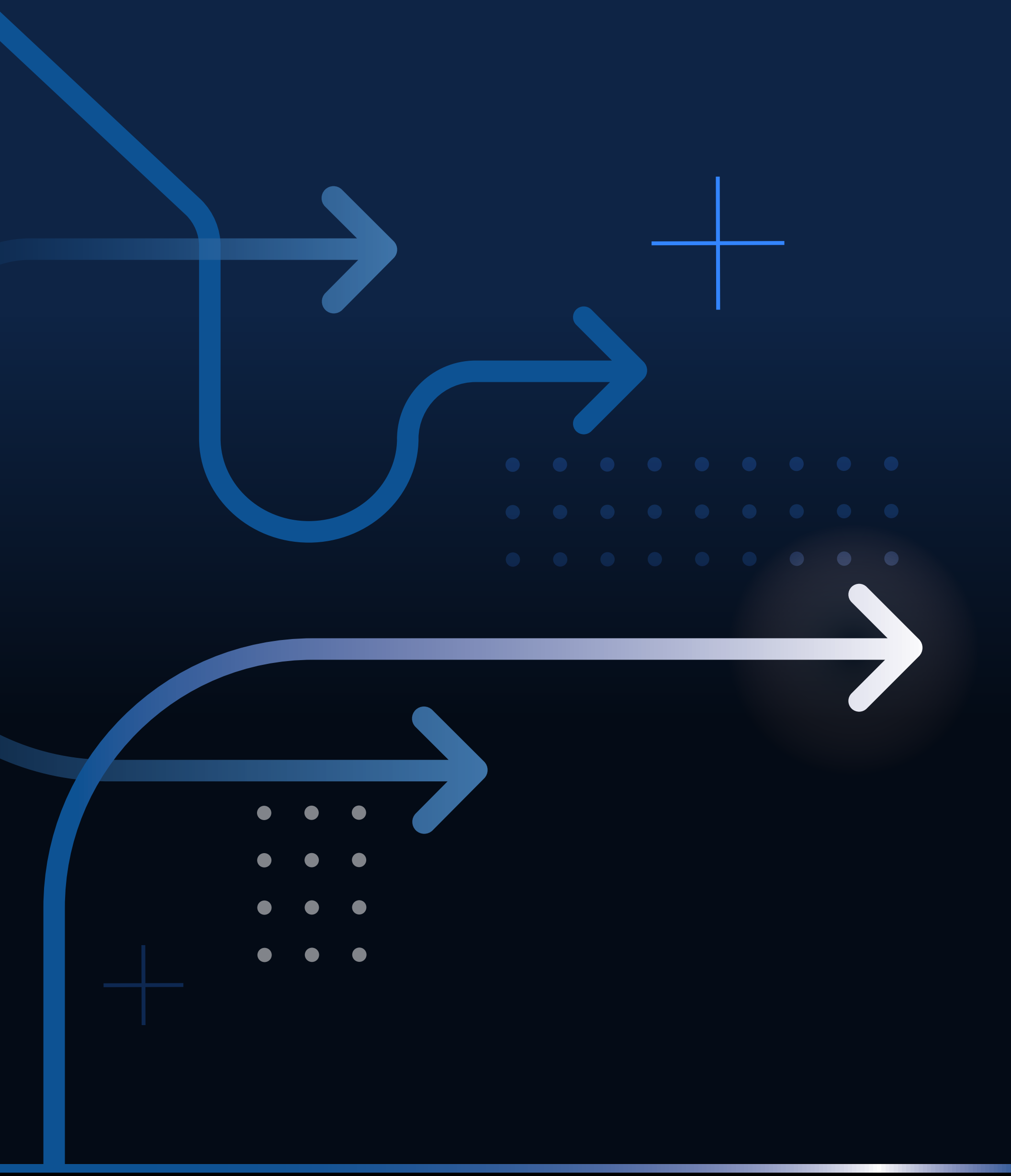
GIGAOM

About GigaOm

GigaOm provides technical, operational, and business advice for IT's strategic digital enterprise and business initiatives. Enterprise business leaders, CIOs, and technology organizations partner with GigaOm for practical, actionable, strategic, and visionary advice for modernizing and transforming their business. GigaOm's advice empowers enterprises to successfully compete in an increasingly complicated business atmosphere that requires a solid understanding of constantly changing customer demands.

GigaOm works directly with enterprises both inside and outside of the IT organization to apply proven research and methodologies designed to avoid pitfalls and roadblocks while balancing risk and innovation. Research methodologies include but are not limited to adoption and benchmarking surveys, use cases, interviews, ROI/TCO, market landscapes, strategic trends, and technical benchmarks. Our analysts possess 20+ years of experience advising a spectrum of clients from early adopters to mainstream enterprises.

GigaOm's perspective is that of the unbiased enterprise practitioner. Through this perspective, GigaOm connects with engaged and loyal subscribers on a deep and meaningful level.



GIGAOM

GigaOm democratizes access to strategic, engineering-led technology research. We enable businesses to innovate at the speed of the market by helping them to grasp new technologies, upskill teams, and anticipate opportunities and challenges. The GigaOm platform changes the game, by unlocking deep technical insight and making it accessible to all.