WHITEPAPER

How Automated Threat Modeling Can Support Your Move to the Cloud

Security Compass

It sometimes seems like everyone and everything is moving to the cloud. A move to the cloud can free up internal resources and be more cost effective than purchasing hardware and staffing a dedicated data center. Cloud deployments allow organizations to scale up and down quickly, without the need to determine peak demand in advance.

A recent study by Flexera found

- 90 percent of enterprises expect cloud usage to exceed prior plans due to COVID-19
- 92 percent of enterprises have a multi-cloud strategy, and 82 percent have a hybrid cloud strategy
- On average, respondents use 2.6 public and 2.7 private clouds
- 59 percent of companies plan to migrate more workloads to the cloud
- 42 percent plan to expand the use of containers

Organizations contemplating a move to the cloud quickly realize that security in a cloud deployment is not automatically made more efficient. Many organizations struggle to understand and implement a cloud deployment that meets all their security requirements. Cloud security considerations are different from traditional networks and on-premises applications, and understanding the potential security threats in such infrastructures in advance makes development, security, and operations teams more effective and efficient.

Much of the confusion arises from the shared security model used in cloud deployments. Unlike on-premises application deployments where in-house resources manage all assets, security activities vary by cloud service provider, the deployment model, and the specifics of the cloud services contract. This can present challenges to security teams when identifying threats and mitigations, and especially when attempting to validate whether a mitigation is effective.

"While cloud companies have to publicly disclose copious amounts of security design and operational information, it can be impossible for [cloud] consumers to understand which threats the cloud services are taking into account, and how. This lack of understanding makes it hard to assess a cloud service's overall security."

Bruce Schneier,
American security technologist

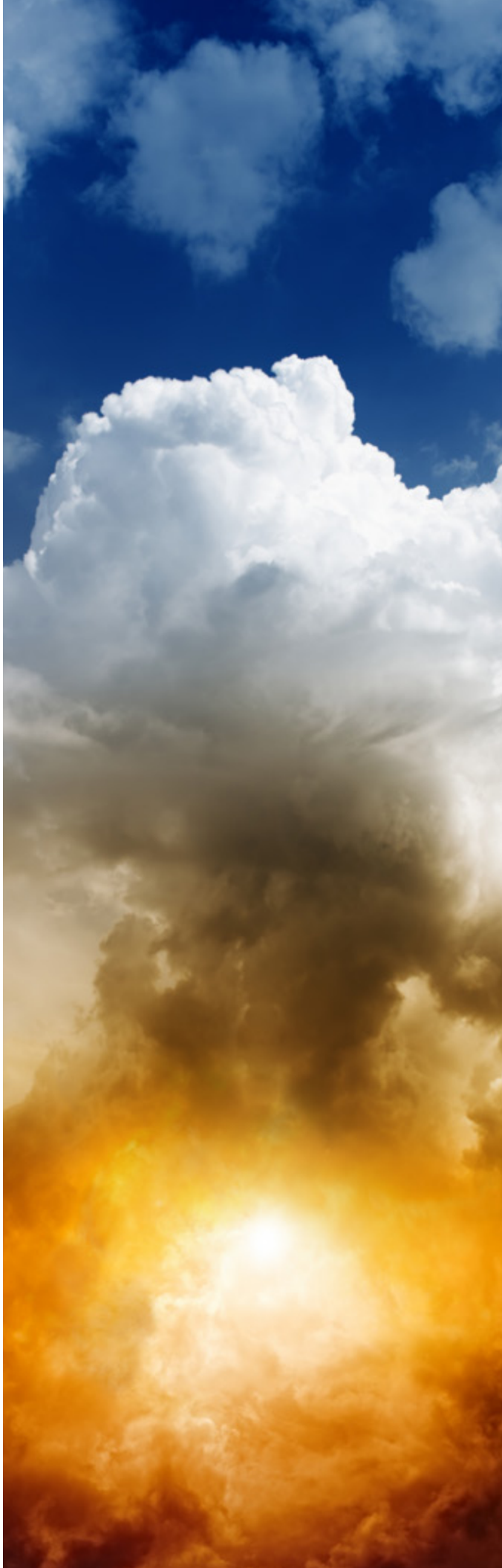
Perhaps, then, it is not surprising to learn that 73 percent of companies using AWS have at least one critical security misconfiguration. Another study showed that over 40 percent of cloud hosts were found to have high or critical vulnerabilities.

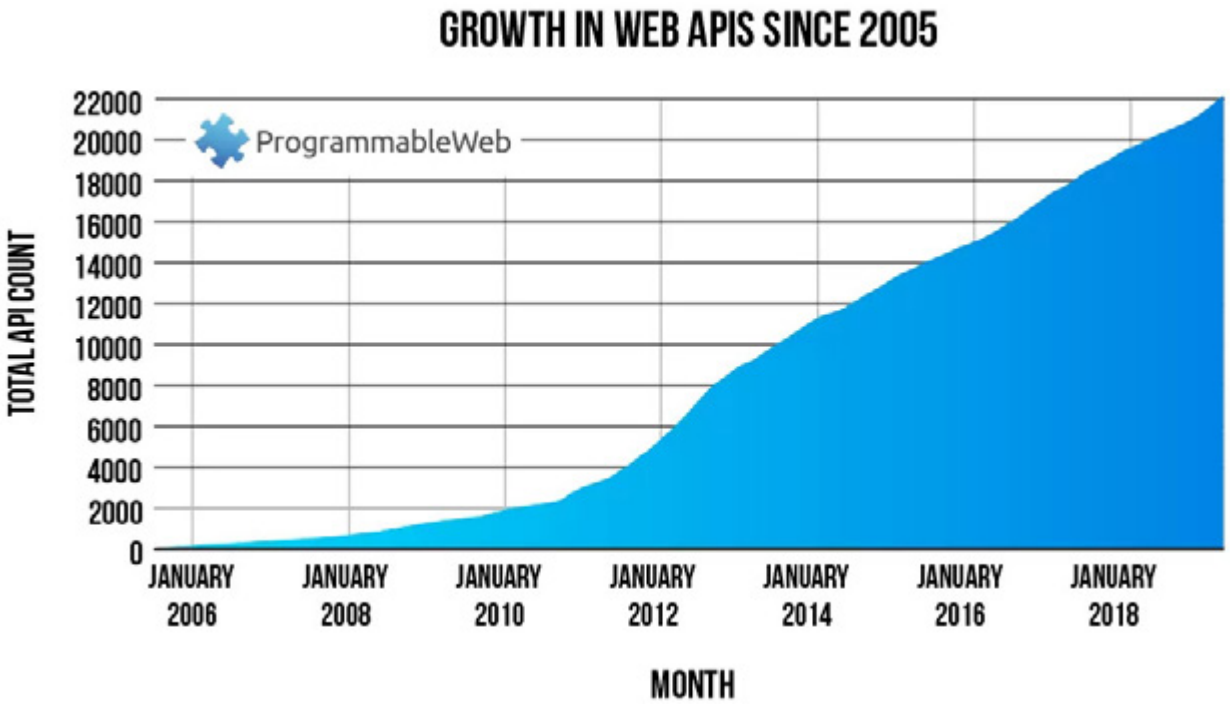
Threats to cloud applications are complex

Cloud applications cannot be easily protected. Multi-tenancy and shared services open new attack vectors such as isolation failure, malicious insiders at the cloud provider, management interface compromises, and insecure or ineffective deletion of data stored in the cloud. In short, you need to worry about your security practices, those of the cloud provider, and those of the provider's other customers.

APIs introduce additional complexity

Using a cloud service provider means organizations must rely on the application programming interfaces (APIs) used to provision, orchestrate, manage, and interact with cloud services. Unlike management APIs for on-premises deployments, these APIs are exposed publicly, which greatly increases an application's attack surface. This, coupled with the shift from monolithic applications to microservices, has greatly increased the number of APIs in the average organization. According to a study by Ping Identity, 25 percent of the companies surveyed have over 1,000 APIs, while 35 percent report having between 400–1,000 APIs. More worrisome, 51 percent are unsure if their security team has visibility into all the APIs used in their organization.





Graphic source: programmableweb.com

Identifying security controls for threats to cloud deployments

In a cloud deployment, teams need to consider not just their own software, but the deployment environment and controls for each cloud service provider. Many organizations conduct threat models and develop corresponding security controls for their applications. In a traditional threat model, software architects, developers, and security teams analyze an application's design to identify weaknesses an attacker can exploit. In highly critical environments, teams may even examine the tools, techniques, and procedures used by a specific adversary.

There are also resources to help DevSecOps teams identify threats to cloud applications. To address threats arising from the adoption of APIs, the Cloud Security Alliance has published "Security Guidelines for Providing and Consuming APIs". It lists nine "risk areas" and over 30 mitigations across the Secure Development Lifecycle—from Threat Modeling and Countermeasures all the way through Documentation. Similarly, SAFECode publishes Best Practices for Secure Development of Cloud Applications that includes identifying threats to cloud-based applications, and the Software Engineering Institute publishes information on cloud-unique threats and risks.

Good policies are not enough

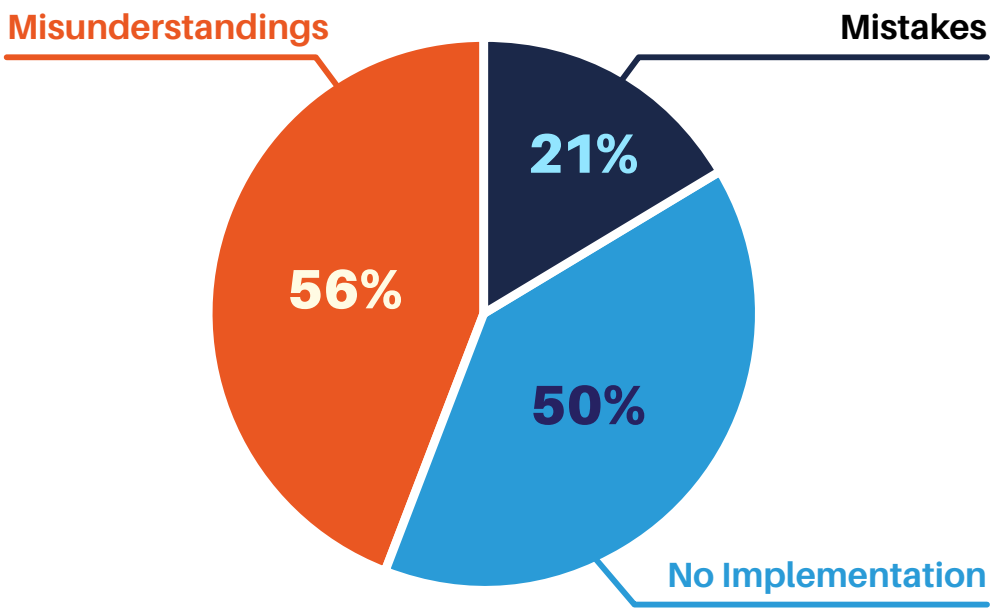
Despite the availability of valuable resources, significant vulnerabilities may remain. Traditional threat modeling practices can be arduous and take weeks to complete. Most organizations lack sufficient senior resources to scale threat modeling beyond their most critical applications. In addition, development teams need to understand the best practices and controls for each identified threat.

Training development teams for secure coding best practices, and providing secure coding policies are good initial steps, but do not guarantee a positive outcome. Developers are under constant pressure to quickly deliver software that meets functional specifications.

Remembering all the security policies that apply in all situations is impossible.

Research by USENIX analyzed 94 projects submitted by teams—many of whom had just completed a four-course program on secure development in the Build It, Break It, Fix It (BIBIFI) secure coding competition series. They classified errors as (a) simple mistakes made when implementing a solution, (b) failures to attempt to implement a necessary security mechanism (e.g., neglecting to use encryption or integrity checks), and (c) conceptual misunderstandings of the security mechanism (e.g., using a weak algorithm or insufficient randomness). While mistakes made up only 21 percent of the errors, vulnerabilities that resulted from misunderstanding or failure to implement security controls appeared in 78 percent of the projects.

USENIX analysis of programming vulnerabilities



The solution: SD Elements

Development teams need to receive accurate information about security controls as part of their workflow if they are to build more secure applications. That means understanding the threats associated with each application and cloud service provider model, and translating those threats into actionable, enforceable development and testing tasks.

Scalable threat modeling

Traditional threat modeling methods take time and expertise. Enumerating the threats and corresponding controls can take weeks. Diagramming architecture and generating attack trees and data-flow diagrams require days of discussion. While such time investment may be justified for critical projects, it may not be possible when scaling threat modeling across all applications in a cloud deployment.

Automated threat modeling scales easily and saves valuable time.

Up to 90 percent of the threats to an application are inherent to its development stack, including programming languages, frameworks, and deployment environment. Instead of weeks, automated threat modeling requires less than an hour to complete a short survey that categorizes the application and identifies in-scope secure coding policies and regulatory requirements.

Translate threats into actionable controls

A primary concern with cloud deployments is understanding which controls are required for each potential threat, and whether the cloud service provider or DevSecOps team is responsible for the controls to mitigate each threat. SD Elements identifies the threats and maps each threat to a security control that can be implemented by Development, Security, Operations, or the cloud service provider. This ensures a comprehensive and clear process for application maintenance, and compliance with internal security policies and regulatory standards. To make threat mitigation actionable by the appropriate party, you need specific implementation information, including, when appropriate, code examples and test plans.

Integration with DevSecOps workflow

DevSecOps teams need a single source of information for applications intended for the cloud. As demonstrated in the USENIX research, even security-aware developers struggle to remember every policy and use case when facing the pressure of pushing multiple releases to production each week (or day).

SD Elements makes security controls part of the normal development and testing workflow. Through integrations with popular project management tools like Jira, controls are assigned directly to the individuals responsible for implementing and verifying each control.

Use application security testing for confirmation, not bug hunting

By anticipating threats and implementing controls as part of the normal development lifecycle, security testing is simplified. Instead of using static and dynamic analysis or penetration testing as the primary method for identifying security vulnerabilities, SD Elements allows you

to verify that each control is in place, reducing the number of issues teams must address late in the development lifecycle.

Stay informed

SD Elements provides a centralized, auditable reporting platform for all applications. Consistent, repeatable, and verifiable reporting shows the status of each set of applications – whether hosted in the cloud or in house – and quickly provides an accurate understanding of the organization's risk posture.

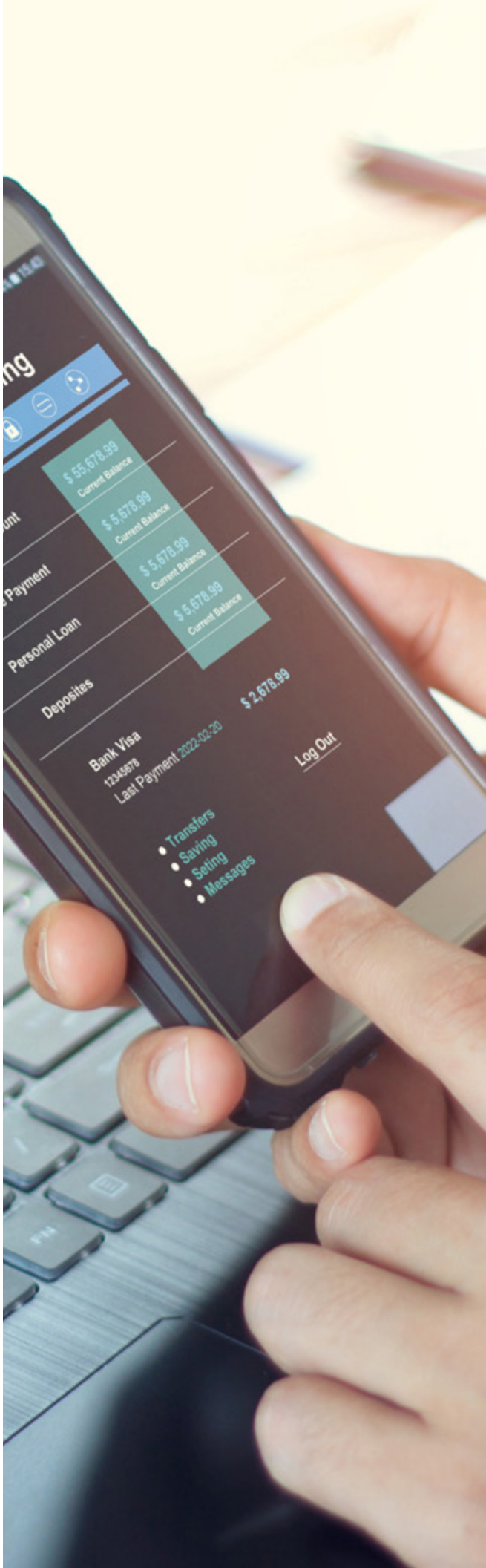
Lather, rinse, repeat

Threat modeling cannot be a one-time event. Over time, applications change, cloud environments are updated, and features and components are added and removed. Any of these changes can invalidate a previous threat model. Few organizations can reassign senior resources for the weeks required to redo traditional threat models several times each year.

Modifying a threat model with SD Elements is as easy as updating the survey so new threat reports can be generated, translated into controls, and assigned to the appropriate individuals or teams.

Go Fast. Stay Safe.

Building secure software is not a secret. Resources exist to identify threats and apply secure coding practices to minimize risk. SD Elements brings consistency, scalability, and auditability to threat modeling and secure development. This allows organizations to build and deploy cloud applications with all the necessary security controls in place nearly as fast as if they were developed without worrying about security or compliance.



Security Compass

Security Compass

Go Fast. Stay Safe.

Security Compass, a leading provider of cybersecurity solutions and advisory services, enables organizations to build more secure software faster. With their flagship product, SD Elements, the company helps automate significant portions of proactive manual processes for security and compliance that improves time to market for new technology. In addition, they offer advisory services on how organizations can embrace emerging technologies like cloud to strengthen their security posture. Security Compass is the trusted solution provider to leading financial organizations, technology enablers, and renowned global brands. The company is headquartered in Toronto, with offices in the U.S. and India. Follow Security Compass on Twitter @securitycompass or visit them at securitycompass.com to learn more

1.888.777.2211
info@securitycompass.com
www.securitycompass.com

@SECURITYCOMPASS
SECURITY COMPASS

OFFICES

GLOBAL HEADQUARTERS
1 Yonge Street
Suite 1801
Toronto, Ontario
Canada M5E 1W7

TORONTO
390 Queens Quay W
2nd Floor
Toronto, Ontario
Canada M5V 3A6

NEW JERSEY
621 Shrewsbury Avenue
Suite 215
Shrewsbury, New Jersey
USA 07702

CALIFORNIA
600 California Street
San Francisco, California
USA 94108

INDIA
#4.07
4th Floor, Statesman House
Barakhamba Road, New Delhi
India 110001