Securing Your Data in the Cloud: Threats and Mitigation

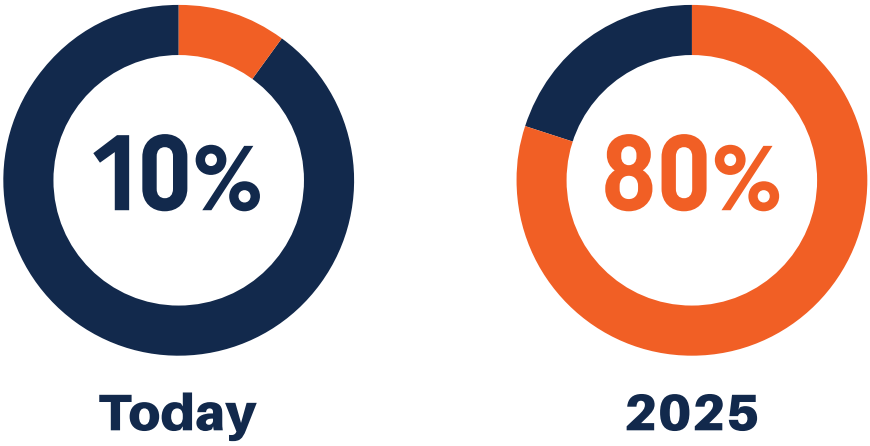
Security Compass

Organizations of all sizes are moving applications to the cloud to leverage shared services, for rapid and elastic scaling, and data security. Gartner expects that 80 percent of organizations will shutter their proprietary data centers by 2025. This is not a new initiative. The U.S. Federal Government has been consolidating and closing data centers for ten years and had closed over 6,200 through August 2018.

Cloud environments are not inherently less (or more) secure than internal data centers. However, moving applications and infrastructure to the cloud requires security teams to consider new threats and risks, including policies, technical risks, and privacy and security regulations.

Enterprises that will close their traditional data centers

Percentages of respondents



How SD Elements helps with cloud security

SD Elements automates threat modeling and secure development by anticipating threats and risks and ensuring that those are addressed throughout the development lifecycle. SD Elements uses a brief survey to characterize an application's business value, technology stack, deployment environment, the cloud providers' shared responsibility model, and applicable regulatory standards. From this, it generates a comprehensive list of threats to the application, applicable secure coding guidelines, and actionable tasks that are assigned to developers, security, and operations.

SD Elements secures cloud deployments

Building secure applications for deployment in the cloud adds new threats. The shared responsibility model requires development, security, and operations to understand exactly who has responsibility for each risk and control. SD Elements' content library of threats, controls, guidelines, and regulatory standards covers cloud risks including:

Cloud services configurations

Improperly configured service settings have resulted in dozens of breaches exposing sensitive data. Each service in a cloud deployment, installation, and maintenance requires specific configurations to minimize risk. SD Elements anticipates these threats, provides mitigation controls, and assigns controls and test validation plans to developers. Some of the services covered by SD Elements are: Identify and Access Management (IAM), Storage Services, Domain Name Services (DNS), Notification Services, Key Management Services, Load Balancing Services, Database Services, and more.

SD Elements Supporting Services		
AWS Services	**Azure Services**	**Google Cloud Services**
AMI Aurora Auto Scaling CloudFront CloudWatch Config DynamoDB EBS EC2 ECS ELB IAM KMS Lambda RDS Route53 S3 SNS SQS VPC	Active Directory Azure Functions Key Vault Monitor Multi-Factor Authentication Network Watcher Resource Manager Security Center SQL Database Storage Virtual Machines Virtual Network	Cloud IAM Compute Engine Virtual Private Cloud (VPC) Cloud DNS Cloud Storage Cloud SQL Cloud Audit Logs Stackdriver Cloud Key Management Service Kubernetes Engine

Mapping to regulatory standards

Organizations are subject to rapidly expanding sets of regulatory standards covering privacy and security, and understanding which controls are required by each standard is critical. To ensure compliance and simplify audits, SD Elements' content library includes standards and controls for over 50 industry and regulatory standards, and translates these requirements into actionable tasks, including code samples and test plans.

Support for cloud frameworks

SD Elements supports security frameworks and standards, including the Cloud Security Association's (CSA) Cloud Controls Matrix (CCM). The CCM is a security framework that provides over 130 cybersecurity controls for cloud computing across 16 domains, including application and API security, audit assurance, encryption and key management, and data security and information lifecycle management.

Cloud-specific risks

Moving to the cloud introduces risks unique to its deployment model. These are articulated well by the European Network and Information Security Agency (ENISA) in its publication, "Cloud computing benefits, risks and recommendations for information security." SD Elements incorporates the ENISA risks and corresponding controls for all three ENISA categories: policy and organizational (governance and operation policies); technical (provider planning and multi-tenancy risks); and legal (compliance and privacy regulations).

FedRAMP reporting

The Federal Risk and Authorization Management Program (FedRAMP) provides a standardized approach to security assessments for cloud products and services purchased and used by the U.S. Federal Government. Any cloud services or applications that process or store federal data must be FedRAMP compliant and authorized. SD Elements translates FedRAMP requirements into specific tasks and validation tests.

Go Fast. Stay Safe.

Cloud deployments require you to think differently about security. SD Elements ensures that cloud-specific risks, organizational policies, and regulatory standards are met and validated. It anticipates threats and provides development, security, and operations teams with actionable tasks to mitigate risk. This means that security testing is validating that prescribed controls were implemented correctly for cloud security. You wouldn't have to rely on testing as a primary vulnerability discovery activity.

The result is a balance between speed and security. SD Elements allows companies to build products nearly as fast as if they were being built without any security or compliance at all and as safely as if it were built under the guidance of human experts.

SecurityCompass

Security Compass, a leading provider of cybersecurity solutions and advisory services, enables organizations to adopt balanced development automation for rapid and secure application development. 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.

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

CALIFORNIA
995 Market Street
2nd Floor
San Francisco, CA
USA 94103

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

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

1.888.777.2211
info@securitycompass.com
www.securitycompass.com

@SECURITYCOMPASS
SECURITY COMPASS