IDC

Overcoming Security Challenges to Adopting Public Cloud

WRITTEN BY:

Amita Potnis
Director, Future of Trust Global Practice, IDC

FUTURE OF TRUST PARTNERSHIP OVERVIEW
PARTNER: FORTINET

CHALLENGES AND OPPORTUNITIES:
Obstacles to engendering trust include sophisticated cyberattacks, managing complex regulations, and fragmented IT and security infrastructure. Security is the #1 area that improves the market's perception of an organization as a trusted entity, according to IDC.

PARTNER SOLUTION:
Google Cloud and Fortinet's partnership focuses on bringing disparate workloads and deployment environments together into a single-policy framework to securely manage far-flung infrastructure by utilizing a platform-based unified security approach.

BUSINESS OUTCOMES:
A unified security-first model enables cloud adoption and improves an organization's risk posture and trust perception.

Introduction

Trust is the new metric to measure an organization's ability to enable security, privacy, and regulatory compliance. It is an important measure since the heart of any digital-first business is data, which may include sensitive information such as protected personal information (PPI). Customers must be able to trust that a business can secure data and maintain its confidentiality and integrity. Trust is thus critical to driving innovation at lightning speed.

Cloud is an enabler for innovation. Public cloud in particular enables rapid elasticity, scalability, and metered service that allows resources to be consumed as needed. However, cloud's multitenancy and shared resources can be a serious concern for businesses when it comes to securing data and maintaining confidentiality, privacy, and integrity. These concerns are amplified for highly regulated industries such as finance, healthcare, and life sciences as well as the public sector.

Organizations seeking to engender trust while leveraging public cloud must deal with challenges that include the expansion of threat vectors, skilled staff shortages, and complex regulations that protect sensitive data. A company's ability to leverage the right controls, products, or services in the public cloud to protect its digital assets is critical. Businesses are investing in several approaches for overcoming the barriers around security and compliance (see **Figure 1**).

FIGURE 1

Security Investment Areas 2021

Q. What are the top security-related investment areas for 2021?

n = 507, Source: IDC's *Future of Trust Survey,* February 2021

They are also seeking specialized capabilities to protect against cyber-risks and ensure regulatory compliance. In the public cloud, these capabilities come in the form of partnerships with the ecosystem of technology providers.

Challenges

According to *IDC's Future of Trust Survey 2021*, 47% of respondents call reputational damage their greatest concern as it erodes trust, hurts brand reputation, and impacts business activity. Respondents also say that IT security risk management is the most strategic challenge followed by data privacy management.

The survey identifies the top three challenges to building trust as:

- Sophisticated cybersecurity attacks
- Complex regulations
- Fragmented IT and security infrastructure

Having a robust security posture allows organizations to maintain compliance with legal regulations, mitigate cybersecurity risks, protect against financial risk, and respond to external threats. A well-planned strategy using a unified security-first approach will enable organizations to build a strong security posture and safeguard against potential cyberthreats.

Strategy

To successfully embrace public cloud and build trust, businesses should consider the following tactics.

Improve security. Building a good brand and reputation and creating trust is top of mind for most C-level leaders today. Aligning security spend to ROI metrics such as time to market and improved brand value enables leaders to contextualize security spend to long-term gains.

Buttress compliance. Adherence to complex regulations can be improved by finding a partner that enables a company to prove its compliance to industry and regional regulations.

Seek strategic help from third parties. Organizations may require the support of skilled resources to defend against sophisticated cyberattacks. Third-party organizations including ISVs and outsourcers can support strategic planning and ideation, offer advice on tactics, and help develop security policies and processes.

Consider platforms versus products. Extended detection and response (XDR) is a technology platform that brings together cybersecurity platforms such as endpoint detection response (EDR), log management, user behavioral analytics, and web and email security threat intelligence onto a single dashboard with a single SKU. It helps companies gain the benefits of endpoint detection, including evidence of memory corruption. XDR also correlates alike use cases over many machines and personas to find the single version of truth and offer the most direct remediation processes.

Attract, retain, and upskill staff. A company needs to retain its talented employees and develop a program of continuing education to ensure workers can leverage AI and analytics-based tools to protect against security vulnerabilities.

Business Outcomes

Organizations must think about security early on to implement a more agile cloud environment. Fortinet enables customers to leverage automated security, threat intelligence, and enrichment in the information and data sets that are used to determine if an anomaly is benign or malicious in real time. Automation has the potential to unlock the agility that the cloud can offer at enterprise scale.

With a unified security-first approach, leveraging Google Cloud/Fortinet solutions, organizations can protect against financial losses due to a sensitive data breach, avoid reputational damage caused by a cybersecurity incident, retain and expand their customer base, and equip security staff with AI and analytics solutions to utilize time and data efficiently, among other benefits.

PARTNER PROFILE:

Fortinet's broad security portfolio and investments in cross-product integration (Fortinet Security Fabric) and XDR (FortiXDR) help it to meet customer objectives around vendor consolidation and in maturing from EDR to XDR. FortiEDR is integrated with FortiGate and FortiNAC and a host of third-party vendors in support of intelligence sharing and coordinated responses, with FortiSandbox for real-time file assessment and FortiSIEM in support of security operations. FortiEDR's features and capabilities are comparable with those of larger modern endpoint security vendors.

GOOGLE CLOUD AND PARTNER RELATIONSHIP:

Google Cloud's partnership with Fortinet is strategically positioned to address the challenges and strategy discussed previously.

Fortinet brings a broad and differentiated portfolio with offerings that operate uniformly whether implemented on premises or in a public cloud, hybrid cloud, or multicloud environment. This is helpful when organizations migrate to Google Cloud Platform, where the two companies provide a highly integrated and extensive portfolio that addresses public cloud security and compliance requirements.

This partnership also allows businesses to insert services at any point in a unified manner across all environments. As an example, Google's GKE or Kubernetes engine running on Anthos must be secured in the same way as Google Cloud. Fortinet's capabilities can secure data generated or accessed from IoT devices in a SCADA environment where the end user could be working from home, school, or any remote location. Google Cloud and Fortinet's partnership is focused on bringing the security of disparate workloads and environments together into a single policy framework to manage far-flung infrastructure—a hard reality facing organizations today.

About the Analyst

Amita Potnis
Director, Future of Trust Global Practice, IDC

Amita Potnis is the global lead of IDC's Future of Trust research practice. In this role, Amita is responsible for leading the development of IDC's global thought leadership research around the growing influence of security, privacy, GRC, social responsibility, and ethics that contribute to organizational trust. Her research focuses on global trends that can measure, enhance, and amplify trust.

More about Amita Potnis

Message from the Partner

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet's Security Fabric architecture addresses the most critical security challenges, whether in networked, application, Google Cloud workloads, or mobile environments. Fortinet ranks #1 in the most hardware and virtual based security appliances shipped worldwide.

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.

IDC @idc @idc idc.com