Don’t Fortify, Amplify: The New Cloud Security Stack

A Cloud Security Framework Built for the New Pace of Business

GlobalDots

Security at the Speed of Scale

Balancing security with speed is a classic problem for organizations; protections often seem to lag behind innovations. And, as organizations accelerate their digital transformation to invest in cloud migration, those security needs are more pronounced than ever.

We've seen this conflict pivot play out in real time. Synergy Research Group reported cloud spending rose 37% to $29 billion during the first quarter in 2020, and, according to Canalys, cloud infrastructure spending in the U.S. grew 29% in the first quarter of 2021 to $18.6 billion.

COVID-19 certainly served as a catalyst for expediting digital transformation plans to accommodate the new distributed workforce. But the rapid adoption of cloud technologies brought with it a variety of new requirements and challenges which all too often are not met with updated security protections.

For example, just as our ways of working have changed, compliance standards have evolved along with them. This has introduced new guidelines for organizations that previously may not have thought about industry compliance.

These forces of migration, adoption and transformation make the cloud more important than ever for businesses to address. Yet the same opportunities that make the cloud vital for business are the same that make it attractive to malicious threat actors. According to the (ISC)2 2021 Cloud Security Report, 96% of cybersecurity professionals state they are at least moderately concerned about public cloud security. And it's for good reason; 80% of organizations experienced a cloud data breach in the last 18 months.

To balance the requirements of both speed and protection, there is a need for a security framework that can keep up with—and support—the rapid iteration required of businesses.

The new cloud security stack.

{ 96% of cybersecurity professionals are moderately concerned about public cloud security }

In this eBook, you'll learn more about the new cloud security stack and how it can empower an organization's growth within the cloud.

Understanding the Cloud Security Need

The decentralization of work as a result of the COVID-19 pandemic marked the beginning of a significant shift. Prior to the pandemic, only 6% of U.S. workers performed their jobs remotely, compared to more than 40% today. And with 96% of workers responding favorably to some amount of remote work, that trend is expected to continue.

Remote work diversifies connectivity, meaning new threats are more easily introduced. Organizations need tools to not only help navigate the shift, but to also increase protection against the growing list of risks. These risks include:

Excessive Permissions to Cloud Environments

Every unnecessary permission an account holder is given over time can just as easily be accessed and leveraged by a bad actor. Maybe your intern wouldn't delete your data, but a hacker with excessive permissions might. That's why 75% IT leaders recently listed excessive permissions as one of their top security concerns.

Misconfiguration of Cloud Resources

A cloud misconfiguration is often a benign human error that is essentially invisible because it's often hard to detect with traditional security solutions. For that reason, it becomes a convenient threat surface for a bad actor to steal cloud data. Solidifying just how much of a concern this is, 92% of IT professionals worry cloud misconfigurations make them vulnerable to a data breach.

Open Source Vulnerabilities

Software development has become far more collaborative than ever. While this process can allow speedy iteration and progress, currently 70% of all open source applications contain at least one security flaw. Without parsing or auditing that open source code, companies may be unknowingly bringing in new risks.

Outdated Perimeter Security

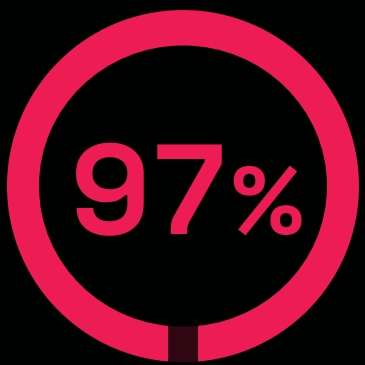
As a result of the distributed workforce, the traditional perimeter has essentially dissolved. 97% of organizations use at least one public cloud, and the increasing use of the supply chain has introduced a variety of new endpoints. Traditional perimeter-based security practices, like internal firewalls, cannot protect an organization's resources as they once did.

Authenticating Employee Identity

With more than 60% of security breaches caused by leveraged credentials, it's even more critical to ensure an organization's users are who they say they are. By granting every employee access to core material, a bad actor only needs to successfully impersonate an employee to gain access to as much data as that employee can reach.

It's clear that today's connected cloud environment presents many diverse risks, but applying patchwork solutions is an inefficient, reactive approach. To reap the benefits of the cloud in a secure way, there needs to be a new holistic security framework that can grow along with an organization.

What's Leading to the Creation of a New Cloud Security Stack?



97% of Organizations Use Public Cloud

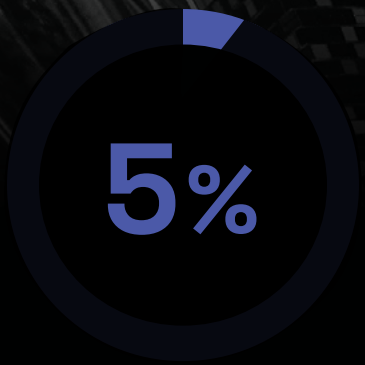
It should come as no surprise that the cloud now dominates enterprise IT strategies. As referenced above, 97% of organizations use at least one public cloud, 92% report having a multi-cloud strategy, and 82% have a hybrid approach that combines public and private clouds.

This increased cloud adoption supported the shift to remote work and decentralized employees. In fact, 90% of IT leaders report that cloud usage during the pandemic was higher than anticipated. Yet many organizations realized that the rapid shift to cloud-based tools and solutions increased the threat surface, and they did not have a solid security strategy in place.

Increased cloud traffic empowers businesses, just as it attracts bad actors. Managing that flow is the way to avoid collisions between an organization's scale and risk.

90% of IT Leaders Rely on Open Source Software Development

Just as our ways of working have changed, the work itself has followed. As most organizations know, open source software comes with many advantages: it saves time, money and can be used to better adapt to customer needs. But open source software can't be an open door. That's why an organization needs rigorous clarity on who it's letting in--and who it's keeping out.



5% of Total Revenue Spent on Compliance

Compliance costs more than just headaches. In 2020, more than 29% of organizations reported that their compliance costs were as much as 5% of their total revenues, and another 32% were entirely unsure of what it actually cost them.

With new and evolving regulatory standards, compliance regulations are more rigorous and complicated than ever. And an increasing part of compliance regulations includes reporting requirements around data security.

Take, for example, GDPR. While these data and privacy laws are specific to the European Union, they can affect your business anywhere. In fact, under Article 3 of the GDPR, your company has to weigh GDPR compliance for any data collected of EU citizens, regardless of where you're based.

With most companies holding and collecting some amount of data under the scope of GDPR, the risks (and expenses) of a data breach or hack are higher than ever, including fines that go up to 4% of a company's revenue. To combat this, companies of all sizes need to be prepared to meet different compliance standards that shift over time.

The Solution

The New Cloud Security Stack

5 Components of the New Cloud Security Stack

The security stack is built to handle the current market needs, so the stack needs to evolve alongside new challenges and innovations. That won't be simple. As the COVID-19 pandemic disrupted companies worldwide and expedited new ways of working, safe connectivity became more important than ever.

This tipping point underscored the need for a **new cloud security stack** capable of meeting these new needs. The cloud security stack is comprised of five components: Identity & Access Management, Zero Trust Network Access, Open Source Security, Cloud Workload Protection, and Compliance Automation. With each of these components in place, organizations can more effectively avoid security breaches, data leaks, and targeted attacks while maintaining the benefits of cloud operations.

01
Identity & Access Management

Integrate multi-factor authentication and single sign-on for employees' remote access workflows.

02
Zero Trust Network Access

Enforce authorization and authentication with the least-privilege principle.

03
Open Source Security

Monitor and detect open source dependency with smart alerting.

04
Cloud Workload Protection

Minimize permissions and detect misconfigurations in public clouds.

05
Compliance Automation

Enable automation of multiple compliance tasks to reduce regulatory burdens.

4 Traits of the New Cloud Security Stack

Security threats are consistently evolving, requiring CISOs to be flexible to ensure they can maintain a best-in-class security approach. The four traits listed below provide evaluation guidelines that ensure an organization's security solutions integrate with the new cloud security stack.

SaaS Consumption Model

The new cloud security stack offers the SaaS model's inherent agility and scalability with automatic updates to ensure best-in-class security can evolve. Each iteration receives feature updates instantaneously without affecting operations. Furthermore, SaaS-based pay models enable organizations to scale usage up or down to pay for what is used. This ensures an organization can more efficiently manage its needs in real-time.

Frictionless DevOps

The new cloud security stack integrates seamlessly with critical tools and components throughout the organization's DevOps environments. Collaboration apps, administration, and reporting can be accessed and configured from a single hub. This model allows integration for the most popular enterprise apps in a cloud-native environment, removing the need for UI-only solutions.

Reduced Noise

The new cloud security stack eliminates alert fatigue because AI and ML are continually learning the organization's exposure patterns. This ensures security teams only see alerts for highly suspicious, true-positive activities that require intervention. And, with inherent and integrated auto-remediation capabilities, your team can save time and effort while maintaining best-in-class protection.

Effortless Evidence

The new stack provides one-click reporting, letting you produce the evidence needed for compliance audits for common security standards, such as GDPR, PCI-DSS, ISO-27001, and SOC2, among others, with ease and clarity. This increases your visibility and reduces liability to better position your organization to manage diverse and changing compliance standards.

01. Identity & Access Management

Establish Unified Access Governance for All Business Applications

IAM solutions help organizations overcome the employee identification challenge with efficient multi-factor authentication (MFA) and single-sign on (SSO) access policies. With IAM, remote and on-site employees are able to move freely and securely between critical business applications.

Most companies experience a huge disconnect on IAM. They operate from a time when usernames and passwords were acceptable for their security needs, which is insufficient for an environment with a substantial amount of web-traffic driven by malicious bots. Meanwhile stopgap solutions, like the infamous CAPTCHA, can slow workers down without doing enough to protect organizations.

Correctly applied, IAM and SAML work together to create SSO policies which operate as a frictionless single source of truth to identify users at scale. This creates a secure and speedy working process, enabling organizations to automate role provisioning without giving excessive permissions and minimizing access for bad actors. Business growth requires more team members and more accounts, so creating a secure path to onboarding is the easiest way to ensure the organization can grow without jeopardizing cloud data.

This level of security matters because authentication methods without IAM can often be exploited by bad actors. Recently, sophisticated phishing campaigns successfully exploited authentication for a Florida Hospital, holding systems ransom and releasing sensitive data. And a hacker in California was able to remotely access a waste-treatment plant by impersonating an employee.

In both these cases, authentication was successfully spoofed without much difficulty; simple usernames and passwords can be easily accessed or stolen. Fortunately, IAM solutions prioritize security with MFA, ensuring that only those with privileges can access their accounts.

Critical features of effective IAM solutions include:

Extensive Integrations

To ensure productivity and protection, the ideal IAM solution integrates with most business applications through SAML or SWA connectivity, while offering API integrations for any ancillary applications. The ability to sync with employee directories, such as AD, LDAP, G-Suite, and Office365, supports timely permission management.

Smart MFA and SSO

Effective IAM solutions reduce authentication friction as much as possible. Smart MFA features triggered only by anomalous behavior minimize employee disruption, and SSO that pre-includes all applications used for daily work supports smooth employee engagement.

Lifecycle Automation

Lifecycle automation enables IT teams to implement workflow-like logic triggered by changes in employee directories. This will allow permission-related procedures to automatically roll out upon onboarding, role changes, or offboarding.

{ IAM solutions overcome the employee identification challenge with smart MFA and SSO }

02. Zero Trust Network Access

Authenticate Everyone and Trust No One

Zero trust means taking nothing for granted and verifying every device, network and user to minimize the attack surface. In a cloud-dominant environment where no user should be blindly trusted, 76% of security leaders agree that Zero Trust Network Access will simplify their organization's security architecture.

In comparison to outdated models that "trust, but verify" users, zero trust architecture instead requires organizations to actively monitor and validate that a user--and their device--have the right privileges before allowing connection to any enterprise or cloud assets.

This process isn't just safer, it's easier. By applying zero trust, you could create an access portal that customizes access and permissions for users. This limits user access to only what they need to do their jobs. And, by linking that portal through SSO, you can link applications to your LDAPI and have increased transparency. This ensures everyone is who they should be, doing what they should be.

That's why enforcement of zero trust policies rely on real-time visibility into user credentials and attributes. Doing so allows an organization's security plan to be both proactive and responsive to a variety of potential threats.

The principles of effective zero trust solutions include:

Identifying Users and Devices on Network

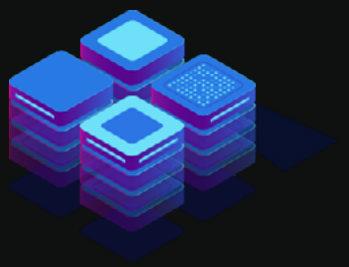
In a changing permissions world, authenticating users and devices is more important than ever. Managing and identifying specific users and devices on an organization's network can keep it protected from malicious actors seeking access.

Applying Controls to Manage Access

Maintaining limited controls and access points ensures an organization's team is empowered to do their work while mitigating the risk of an account becoming an entry point for an attacker.

Monitoring Network and Device Behavior

Vigilance and surveillance as a best practice keeps the team aware of patterns. This allows organizations to identify and respond to security anomalies quickly and effectively.



Innovating for New Threats

Zero trust solutions aren't stagnant like a firewall. Instead, they're an application of best practices with granular precision, built to adapt to a changing environment.

By implementing a zero trust architecture into the cloud security stack, an organization essentially eliminates any trust with the network. Requiring users to verify who they are (every time) enhances legitimate application access.

Zero trust enforces rigorous authorization policies through least-privilege access.

03. Open Source Security

Detect, prioritize, and remediate open source vulnerabilities

Open source software is appealing to companies for its ease-of-use and speed; it's faster and cheaper than many alternatives. And, as open source development ecosystems continue to grow, organizations are increasingly working with third-party systems.

Furthermore, numerous security reports point to hackers actively contributing to open-source projects in order to introduce backdoors to companies using such software.

Since open source work is publicly maintained, no one properly manages the work. The result is that many open source packages have dependencies, often two or three layers deep. And, despite the common misconception that the latest version of a project will work perfectly without bugs or vulnerabilities, we've seen time and time again that isn't the case.

To continue working collaboratively and nimbly in open source workflows, it's crucial to apply customized security solutions that continuously monitor and detect open source vulnerabilities. Doing so allows organizations to track a baseline for safe work while being primed for alerts on any potential problems.

For example, with open source security solutions in the cloud security stack, organizations can eliminate potential problems before they emerge by scanning Git repositories, containers, and infrastructure-as-code prior production.

Furthermore, by integrating open source security throughout the CI/CD pipeline, these scanning solutions can provide vulnerability scanning and remediation capabilities directly within developer's IDEs as they code. This offers unparalleled visibility and clarity for an organization's team, creating the ability to automatically scan code-changes as a check-gate.

This proactive measure can shift-left the entire security process before issues snowball, allowing an organization to reap the benefits of open source work and collaboration with confidence. Ultimately, it means organizations can move quickly and safely.

Some critical features of effective open source security solutions include:

Vulnerability Remediation

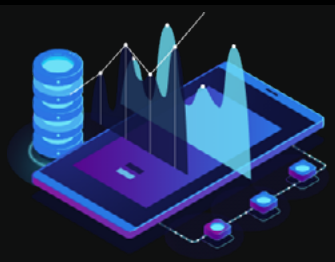
Finding and fixing vulnerabilities in an organization's code is key to reaping the time-saving benefits of open source code. Solutions that can pinpoint the risk while solving for the problem can operate as a proactive way to source action-ready information and use it to fix vulnerabilities that may otherwise go undetected.

Container Support

Third-party container technology, like Kubernetes' base images, can accidentally include dependency vulnerabilities. Because applications inherit everything that comes with third-party software--including the vulnerabilities--security solutions need to be prepared to audit an organization's dependencies, as well.

Automated Reporting

The security stack should allow an organization to track organizational trends and vulnerability fix rates across teams and companies to provide real-time insights and data. Not only does this reduce the burden of management and compliance auditing reports, but it also provides insight and data to compare against going forward. This ensures a consistent and clear security report to guide business decisions.



{ Open source security supports shift-left security, allowing an organization to reap the benefits of open source work and collaboration with confidence. }

04. Cloud Workload Protection

Secure public cloud workloads against identity and access abuse

Much like a Zero Trust approach, solutions like cloud security posture management (CSPM) and cloud workload protection platforms (CWPP) are built to minimize excessive permissions and detect misconfigurations in an organization's cloud infrastructure.

Part of this problem is the order of magnitude of complexities within a cloud environment; the amount of things that could be misconfigured are enormous. There seems to be a data breach in the news every day; resources are left with open access to the internet, most commonly S3 buckets and elastic search databases.

With a CWPP in your cloud security stack, you gain a **single unified dashboard** that provides visibility into any anomalies across the entire cloud infrastructure. This creates a reinforced security stack that replaces the need to maintain security across multiple isolated points.

Furthermore, these solutions provide AI-powered detection of any indicators of the access abuses that might precede a security breach. This is especially crucial given the continuously changing nature of the cloud; with no central visibility, it can be difficult to track changes (such as configurations and team collaboration) made by malicious users.

Running against your data against the CIS foundation global standard baseline set of rules can be tremendously helpful, as well. These rules provide a helpful baseline to help organizations take sporadic events and build them into a meaningful attack timeline with up-to-the-minute updates. Worth noting is that these rules are customizable; you can have your environment scanned based on your own rules, as well.

Automating tools to constantly monitor environments for security or policy violations offers organizations much-needed security without disrupting the rapid collaboration the cloud provides.

Critical features of effective CSPM and CWPP solutions include:

Proactive, Automated Permission Hardening

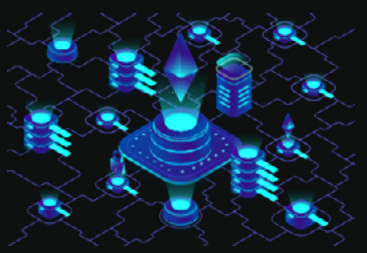
Manual permission management at scale is hardly productive. An ideal solution keeps company assets safe while considerably reducing the security workload.

Consolidated Visibility

Existing platform-specific point security products are ineffective at detecting complex attacks. A holistic solution can flag anomalies across an organization's entire cloud (or multi-cloud) infrastructure in a single dashboard.

AI-Based Anomaly Detection

Most infrastructure attacks are built over time. To outsmart them, CWPP should quietly connect the dots, surfacing suspicious patterns while limiting false positive alerts.



Policy Configuration and Agility

Differentiating policy between teams and units is a crucial cloud workload protection trait. The ability to granularly configure the CWPP decreases false alerts, prioritizes actual threats, and enables critical workflows to run uninterrupted.

Cloud workload protection minimizes excessive permissions and corrects cloud infrastructure misconfigurations.

05. Compliance Automation Platform

Maintain a compliance-ready posture

Compliance automation solutions provide CMDB and protection services for private customer information and offer features that automate compliance-ready reporting.

You can set rules inside your company until you're blue in the face; even if you say "don't leave an S3 bucket open to the public," it can still happen.

That's why compliance can no longer be something that's written as a set of rules; your compliance program needs to be automated.longer be something that's written as a set of rules; your compliance program needs to be automated.

Automating your compliance efforts means your environment is being continually scanned, cycling with active remediation capabilities. Ultimately, doing so translates to better preparedness as it relates to handling your compliance program with less resource-intensive manual work.

This is especially important as regulations and compliance standards become ubiquitous across industries and geographies. Understandably, concern is mounting around how best to manage this extensive and ever-changing landscape. In fact, 69% of executives are not confident that their current risk management practices will be enough to meet future needs.

That concern resonates in a connected world, where even local compliance shifts like GDPR can impact your company. Companies need to be prepared not just to meet compliance requirements but to earn their customers' trust.

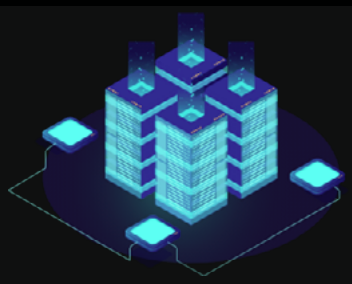
By applying an automated compliance solution in the cloud security stack, an organization can be automatically monitored for changes in relevant standards, leveraging notifications around any pertinent changes.

Implementing these features enables an organization to continue its pace of innovation knowing it can adhere to compliance regulations. This approach reduces time and costs, letting teams move quickly and securely while meeting compliance.

Critical features of effective compliance solutions:

Continuous Evidence Collection

Automatically collect protected data from enterprise systems and organize them based on the compliance standard's format. Traditional evidence collection, normally done at one point in time, is both time-consuming and inefficient; teams are forced to manually find information that could quickly become outdated or invalidated quickly. Instead, you need a continuous compliance solution that can grow and adapt alongside your company for a solution that doesn't require manual certification.



Easy Integration

As with many SaaS-based products, integration is key to achieving customer adoption. Compliance solutions should be built with human-centered design, enabling both quick implementation and out-of-the-box integrations with common data-rich applications. By safely working with existing tools and programs, your compliance solution should be a natural fit into your existing work process.

Gap Analysis

A gap analysis of existing data system practices can produce a simple roadmap to ensuring compliance with any new regulations. This significantly reduces the team's workload while providing a holistic view into the company's compliance status on a daily basis. Doing so will ensure you're always ready to find and remedy the gaps that could emerge in a changing environment.

Simple Audit Communications

Compliance can be difficult enough without endless loops of access queries for shared drives. That's why any solution should provide platform access for the auditor, granting them the ability to review all evidence and comment in one central, organized place. This allows the entire audit to be managed from a single platform without endless emails or chaotic shared drives that can leave compliance gaps.

{ Compliance platforms automate regulatory adherence and audit readiness. }

How the New Cloud Security Stack Amplifies Business

While protecting customer and proprietary data can help prevent expensive security breaches-- the average cost of which was $3.86 million in 2020-- the new cloud security stack also offers multiple benefits in four primary categories: performance, security, cost and operational.

Performance/Speed Benefits

- → IAM and ZTNA reduce security friction for employees, thus increasing productivity and satisfaction.
- → IAM, open source security, compliance automation, and CWP, automate processes to roll out immediately, with no delay, manual work, or human errors.
- → ZTNA and CWP are designed to intercept breach attempts extremely fast, with their anomaly detection and correlation capabilities.
- → Open source security speeds up the very core of the business, allowing faster product development by the automated detection of errors and risks even before they make it to the code.

Security Benefits

Enable full visibility into the predominant attack surfaces of cloud enterprises.

- → Cloud workload protection gives control and manageability over cloud infrastructures and possible misconfigurations.
- → IAM and ZTNA work as gatekeepers to prevent threats from gaining access to the enterprise network and applications.
- → Open source security applications eliminate vulnerabilities in code dependencies.

Cost Benefits

Save production resources by providing a holistic solution that secures your nimble way of working.

- → Open source security solutions immediately save production resources by providing a safer way to engage with nimble programing.
- → Cloud workload protection detects and fixes cloud misconfigurations.
- → Cloud workload protection reduces the costs of added security personnel to monitor malicious activity.
  Open source security applications eliminate vulnerabilities in code dependencies.

Additional cost benefits include saving time and resources associated with compliance audits, as well as employee onboarding/offboarding efforts.

Operational Benefits

Establish DevOps and DevSecOps by integrating solutions directly into existing workflows for tighter collaboration.

- → Shift-left security implements stringent protections early in the SDLC. This is done intentionally to ensure security isn't an afterthought of design, but rather the foundation on which those projects are built.
- → Security integrates directly into development and operations workflows, ensuring more opportunities to shift left to find and fix problems at the earlier stages when they're six times cheaper to fix.
- → Compliance solutions reduce the time and effort required across multiple teams by applying automation and continuous evidence-gathering.

Though each benefit described above is critical, the new cloud security stack provides holistic benefits to an organization, as well. These include increased focus on strategic initiatives by establishing a proactive security posture, supporting rapid development processes, and maintaining regulatory compliance for GDPR, PCI-DSS, and other regulations.

With a cloud security stack in place, organizations can move forward with confidence, knowing they are prepared for the future of work.

The Ideal State – What Great Security Looks Like

When an organization adopts the new cloud security stack, all teams, from security to development, work faster, safer and smarter at scale.

Within 3 months from implementation, we can expect six distinct benefits:

1. Confident Decisions—By relying on the new cloud security stack, the CISO will have a framework to evaluate new cloud security solutions with clarity and confidence.

2. Ease Of Use—All cloud security solutions are easily implemented with minimal efforts from the team, ensuring the security team is aligned on what matters most.

3. More Constructive Time—Cloud security solutions in the stack would save manpower hours by heavily reducing the need for monitoring, management and maintenance tasks of traditional security solutions. This will free up time for innovation and exploration.

4. Reduced Risk—Automation of security would reduce the attack surface of the organization, increase the protection level, and allow for better visibility into the overall security status of the organization.

5. Security-Focused Culture—Development, operations, IT and security teams have established an effective DevSecOps culture built on powerful integration capabilities that support their ambitious release schedules with transparent, secure and empowering solutions.

6. Compliance Ready—With the new cloud security stack, industry regulations are streamlined. This means compliance won't require significant time and resources from multiple parties in the company. It also translates to minimal business interruptions.

As cloud adoption continues to rise, the security landscape needs to evolve with it.

To be truly secure, organizations need to move beyond reactive measures in favor of proactive solutions that can meet a diverse set of threats. Fortunately, a trusted security advisor can help organizations navigate the creation and implementation of holistic security solutions that effectively meet their needs.

After all, security helps safeguard your hard-won opportunities, protecting the trust you've earned. By applying a new cloud security stack, along with expert advice, organizations can confidently meet the security needs of the business and customers alike.

Learn more about GlobalDots and their approach to navigating the cloud security stack.

Schedule a Meeting

About GlobalDots

GlobalDots has been connecting businesses with the latest cloud and web technologies for over 17 years. We consult, resell, implement and customize full-stack solutions that enable business transformation.

Our areas of expertise:

Cloud Security: Don't just fortify your organization, amplify your critical workflows and employee freedoms within their realms of permission.

Web Performance: Break the boundaries of off-the-shelf product performance and create optimal experiences within your applications.

Managed Services: Tap into the speed and agility of the cloud with robust, cost-effective, and secure cloud infrastructures customized for your ecosystem.

Web Security: Protect customer data, site availability and your brand reputation with up-to-date solutions for every critical endpoint.

Corporate IT, Hosting & Networkin: Upscale your IT with our international network of technical teams, data centers, and logistic centers all designed to deliver you optimized solutions that meet your needs.

Fusing an insatiable hunger for innovation with a diligent team of experienced, hands-on experts, GlobalDots helps our customers thrive in a changing world.

Contact us to amplify your cloud environment and your entire ecosystem.

Trusted By