The fundamental shift in cloud security: from point products to platforms

LACEWORK®

Introduction

The digital economy is no longer distinguished from the regular economy. Just about every type of business-to-business and business-to-consumer communication, transaction, or other engagement happens as a result of software applications and resources processing information and delivering solutions through digital formats. It's a shift that has been years in the making, but has accelerated at an increasingly rapid pace in the past few years. Innovative organizations continue to look to digital means to provide competitive advantages, as well as new and faster routes to market.

This transformation is happening on the back of public clouds, which have touted large promises: move fast, reduce human capital costs, improve integration—and deliver as advertised. As a result, businesses of all sizes and types are more agile, dynamic, and scalable than ever before. But this change is not simply about reformatting business in a digital format. The fundamental aspects of the cloud are enabling an entirely new way of conducting business.

Move fast, reduce human capital costs, improve integration

What we're seeing now is that, much as Marc Andreessen predicted when he said, "software is eating the world." IT is both driving this change and making adaptations through the effective use and deployment of cloud software.

The burden of enabling this shift falls to IT and security teams who recognize that for this new pace of business to be sustainable, security has to keep pace with the speed and agility of the cloud. This duality of purposes—risk management and speed—is forcing a shift in their approach to cloud security. The modern approach to cloud security now must combine the protection and visibility of data and workloads with operational capabilities that support rapid development and delivery of digital products and services. In other words, make it safe but don't slow it down.

The burden of enabling this shift falls to IT and security teams who recognize that for this new pace of business to be sustainable, security has to keep pace with the speed and agility of the cloud. This duality of purposes—risk management and speed—is forcing a shift in their approach to cloud security. The modern approach to cloud security now must combine the protection and visibility of data and workloads with operational capabilities that support rapid development and delivery "of digital products and services. In other words, make it safe but don't slow it down.

Security solutions have evolved incrementally since the cloud first took shape. The current market is a mix of legacy point products trying to adapt to the needs of the cloud, narrowly defined tools that address specific use cases, or mash-ups of point products that try to imitate a unified solution.

These security solutions have been delivered to the market incrementally as cloud adoption has grown. Because the pace of growth has been so fast, many teams have not had time to build a comprehensive approach. Rather, they add products that appear to fit specific needs. That means they're sitting with a host of point products that address different parts of their dynamic cloud environment, though they lack a unified approach. Managing and maintaining these point products gets more complex with each new solution, and addressing that complexity can risk the speed at which companies must operate.

Modern organizations prefer a more effective cloud security posture, which they can achieve with a comprehensive approach to cloud security that addresses the specific demands of cloud environments, while supporting the need for business agility and scale.

How can you tell when security tooling isn't aligned with cloud changes?

Lack of visibility

Slow deal cycles and customer loss

High operational costs

Long and manual audits

Missed product deadlines

Deploy vulnerable cloud infrastructure

Developers deploy services faster than security can keep up

Wasteful cycles between security and devops

Talent shortages

Point products no longer work in the cloud

The rate of cloud adoption has been in hyperdrive over the past few years, and it's not hard to see why. As companies see the implications and advantages of digital transformation, the cloud has provided a gateway to rapidly initiate and take advantage of those efforts.

Chief among the cloud's advantages is the speed it enables for both IT and product teams, which is core to their digital goals. Right off the bat, data integration among applications that used to require long-term projects can now get done with the execution of an API and a basic set of requirements. Development of applications that deliver a company's digital services can be improved and delivered back to users through the process of continuous innovation. As a result, business goals have changed because organizations can demand more of their digital infrastructure.

The speed of this change has become self-perpetuating; more can be done, so more is being done. For business, this has created huge advantages. However, as speed becomes dogma, the corresponding need to secure the data, workloads, and assets being used in these complex cloud environments often lags behind, causing security gaps. What's worse, many organizations aren't equipped to identify where those gaps actually exist, leaving prolific blind spots across their cloud environments, creating an undue amount of vulnerabilities.

Coming to the aid are an endless array of tools that purport to address the issue of cloud security in various forms. These solutions typically just address specific parts of the cloud stack: application security, front-end client security, bot detection, intrusion detection, email security, encryption, data loss prevention, content governance...the list is seemingly endless.

Organizations can demand more of their digital infrastructure

We've likely all seen the architecture diagrams that illustrate multiple products addressing security needs. In some cases, they're doing duplicative work. Others are no longer useful. The problem for cloud users is that most solutions are point products that cannot achieve true cloud security because of certain limitations, which include:

Point products are narrow in scope

Most cloud security point products were developed for narrowly defined goals, and they cannot achieve true cloud security because they can only do one thing.

More tools = more blind spots

Each new security product requires additional resources to integrate and manage, and that progression eventually creates gaps that lead to blind spots where activity is not identified. This is where threats hide.

Rules-based approaches aren't cloud-optimized

Most solutions calculate risk and identify threats through rules analysis. But threats can enter an environment without breaking rules.

Not all security is the same

Many cloud security vendors are not born-in-the-cloud. In fact, many of the larger players started as hardware vendors, selling commoditized routers and VPN boxes for razor-thin margins. The cloud looked profitable, and they've looked to make a fast transition. Their skill set, however, doesn't always translate, and it shows in the lightweight applicability of their products.

Multiple toolscreate friction

Trying to unify multiple tools is a manual, never-ending series of tasks, and ultimately it eliminates the advantages of speed that the cloud is built for. Container development and operating a continuous innovation/ continuous delivery (CI/CD) pipeline is impossible in this type of IT scenario.

An approach that relies on multiple products that serve different needs across the cloud environment is now simply untenable.

The cloud footprint is simply too vast, with data residing in various repositories, and users collaborating with different platforms spread across various geographies.

Yet, while the cloud thrives in complexity, it can only be safe with a security approach that seeks not to tame that complexity, but to understand and address it in its entirety and as it changes and adapts.

Almost every problem that a modern organization faces today has a software-based solution applied to it, and IT is tasked with the development and delivery of that. New models to address this (think IaaS, Paas, SaaS) function as a type of IT-as-Code which are built to serve macro trends that mature companies are responding to as well, like accelerated business operations, the increasing pace of change, and a real-time approach to security and compliance that treats risk as an always-on possibility that should not slow you down.

The corresponding security approach is one that's predicated upon three basic principles, all of which are critical to aligning business goals with security demands:

Innovate fast or die

This has become a cardinal principle that drives almost everything an organization does, or tries to achieve, in the cloud. To drive innovation, you must keep up with constant cloud changes.

If you can't see it, you can't secure it

You need to see changes across cloud stacks from app behavior through cloud service configs.

When there is too much to see, where do you focus?

If you can make sense of cloud changes at scale, you can run a secure business.

Consider how different these principles differ from the goals that security teams had even five years ago, when restricting access and identifying vulnerabilities at the edge of networks constituted a security strategy. Today, the emphasis is essentially about grocking the entirety of a cloud environment's activities, analyzing it, and making sense of actual threats across billions of events without impeding the pace of business.

Change is the natural state of the cloud. How can security adapt?

The Greek philosopher Heraclitus said, “No man ever steps in the same river twice, for it’s not the same river and he’s not the same man.” Surprisingly, he was not a cloud architect, but he probably spent considerable time gazing into the heavens, and it provided him with the insight that parallels the nature of the cloud we use today.

Think of it this way: every cloud environment becomes a slate of exponential expansion from the moment it’s spun up. There is no specific state for the cloud. It is continuously changing, and anyone looking to understand change need only look at a typical cloud environment. Every log-in to a network brings a new user—that’s a fundamentally different environment than was present before that user joined. Every application that gets integrated, every new AWS S3 bucket that’s created, every container configuration change, every time an employee accesses from a public WiFi network on their mobile phone—these are all activities that reshape the cloud environment. As a result, they also change the threat potential.

As an example, consider the documents in your Google Drive. Now, give ten people access and editing rights. Multiply that by say, 3 billion. That’s roughly the scale and rate of change happening in a mid-sized company’s cloud environment in a given month. And that number grows with every new document, application, user, log-on…you get the picture.

The fact that all this data is available to be used and consumed is good news, but the bad news is that trends like infrastructure-as-code mean that a single developer’s script can kick off tens of thousands of changes across the environment. Every action, therefore, has to be understood in the context of security, and it reframes the issue of security posture. For each event, does it, or does it not carry risk? And if it does, how are you going to address a threat or protect against the potential for risk in the future?

Security that supports speed and continuous innovation

This rate and level of change has also become a business necessity, which is why product teams use CI/CD principles to apply innovation as a competitive advantage. Product changes are integrated into continuous release cycles, but they must adhere to security and compliance guidelines. Point products slow this process to the point that product teams either lose the advantage of digital speed, or they will simply choose to ignore security and push products out anyway. Either way, the company is vulnerable.

What’s the recourse for product and IT teams that thrive on innovation and change, but must operate according to their own security requirements and compliance frameworks? The only corrective measure is to rely on a platform-based approach that will:

- Reduce the attack surface and meet configuration compliance requirements
- Detect breaches, threats, malware, and anomalous behaviors
- Investigate, discover, and remediate known issues

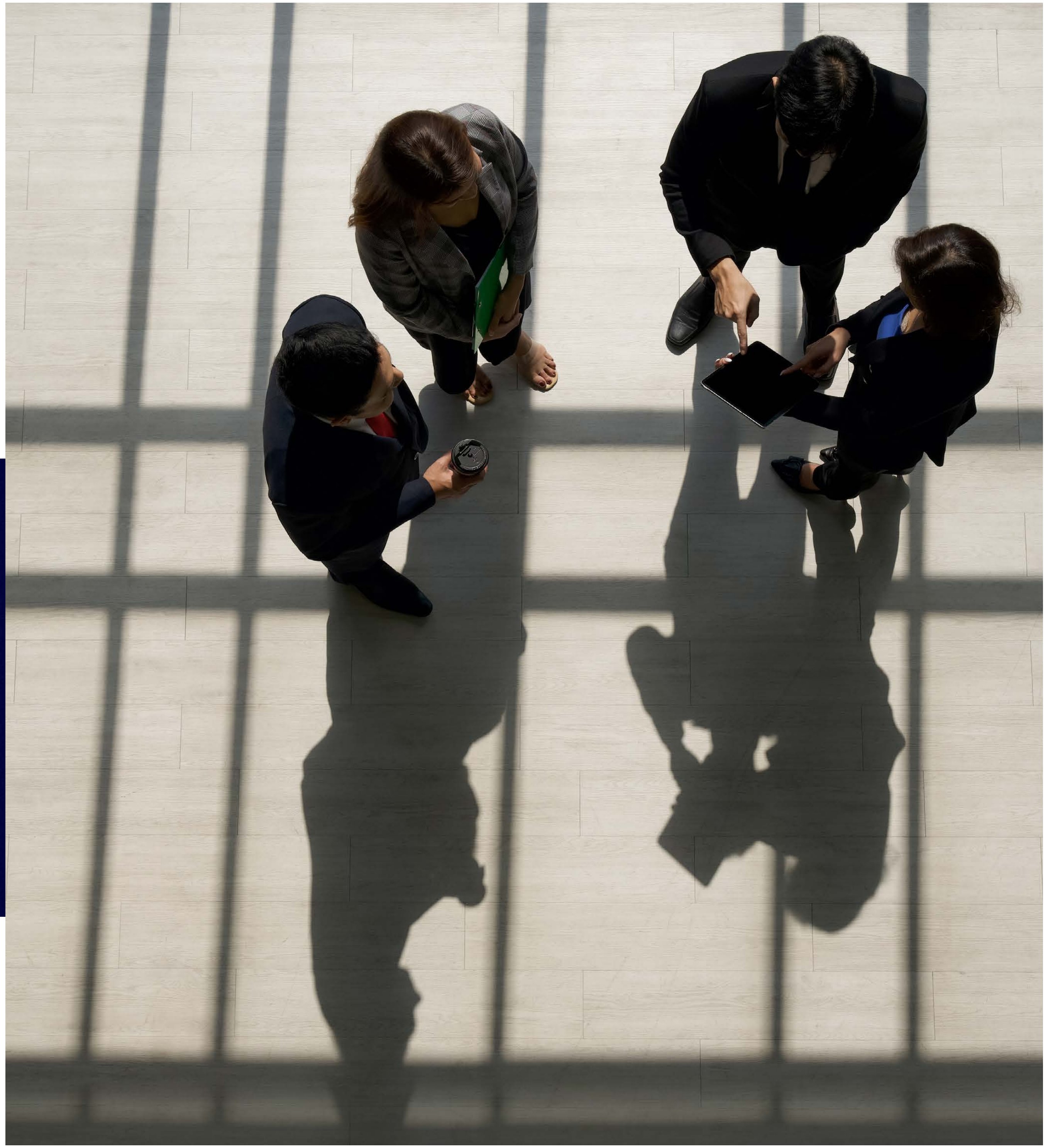
An effective solution, therefore, does not look just for specific rules that have been violated, because that can deliver false positives and it typically doesn’t come with meaningful context. A solution purpose-built for the cloud, looks at the entirety of a customer’s cloud and container environments: all users, all applications and resources, all behaviors, the whole spread—and identifies anomalies (e.g., certain behaviors that are not consistent with normal behavior, and situations that fall outside of normal operations). Remember, that’s across the ENTIRE cloud environment—anything that touches the customer’s cloud environment(s) is viewed, assessed, and analyzed by one, unified platform, not through triage to multiple point products.

A unified cloud security platform eliminates visibility gaps

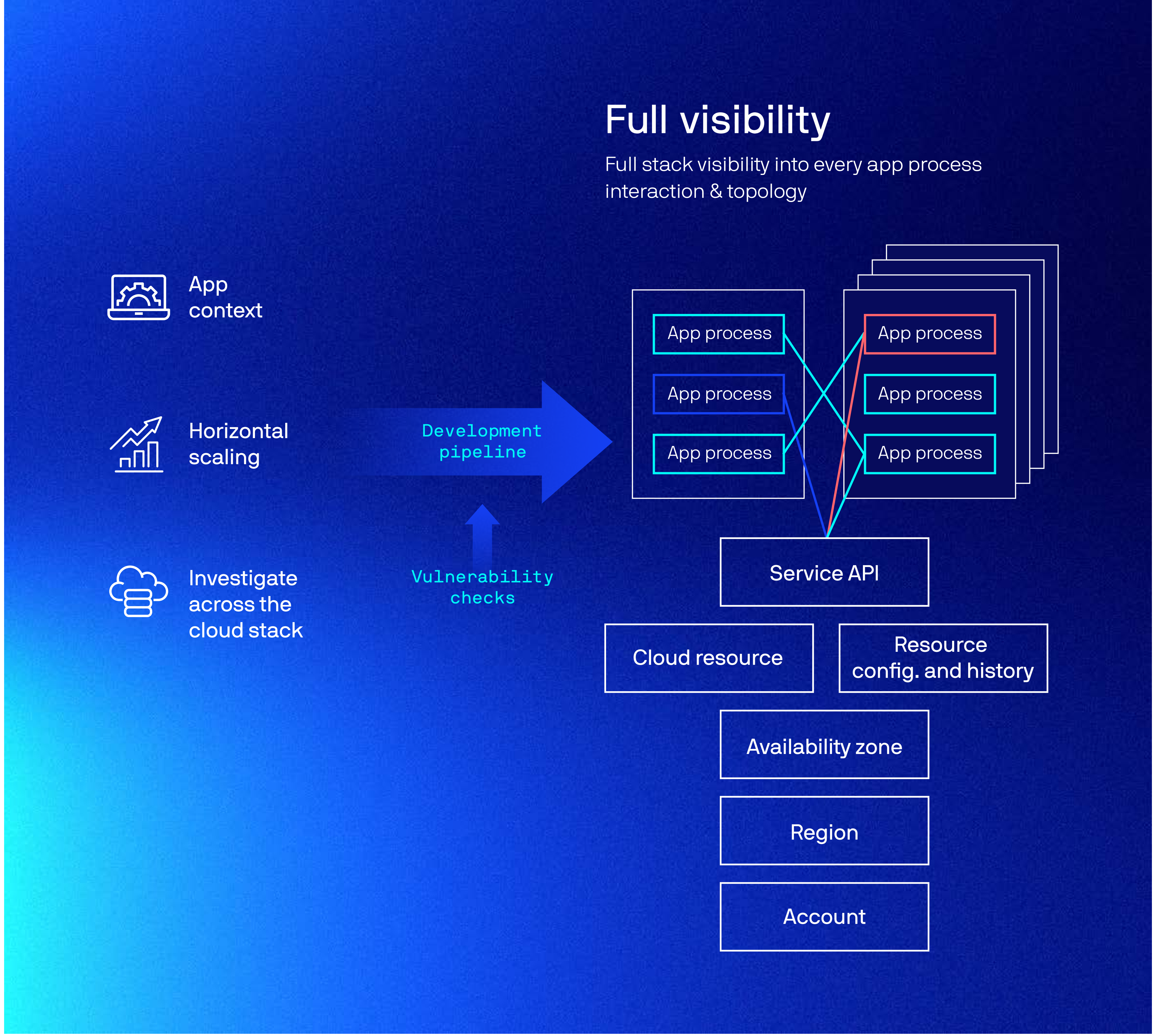
As organizations move more and more workloads to the cloud, their security visibility gap increases. This is only exacerbated by applying multiple point products to the task of addressing specific security issues. IT and security teams are constantly trying to make sense of cloud activity, assess risk, and do it in cloud, container, multicloud, and hybrid environments. This creates a complex landscape to maintain, and it leads to blind spots among and between these different tools.

This is not simply opinion. Even the NIST Cybersecurity Framework (NIST CSF) underscores the importance of visibility when it states:

> "Organizations must develop an understanding of their environment to manage cybersecurity risk to systems, assets, data and capabilities. To comply with this function, it is essential to have full visibility into your digital and physical assets, their interconnections, and defined roles and responsibilities, as well as to understand your current risks and exposure and put policies and procedures into place to manage those risks."
>
> -NIST CYBERSECURITY FRAMEWORK (NIST CSF)



An effective cloud and container security solution has to be able to ingest all activities, understand them, and baseline them against normalized behaviors. It must collect data at the application process layer so it can classify horizontally scaled applications. Without the ability to classify and differentiate application driven infrastructure changes resulting from anomalous behaviors, it's nearly impossible to understand the difference between a normal scaling event and a threat at scale.



Adding to the confusion is when IT and security teams try to repurpose existing tools in their security stack, or native cloud solutions, to protect individual applications or repositories. Security and compliance policies and configurations have to be managed for each resource, each of which will change (as we have seen) in continuous fashion. And all of that has to be done while maintaining awareness and protection over always-changing internal and external threat landscapes. AWS CloudTrail for e xample, is not equipped to perform this. Container security solutions that don't consider non-application activities cannot do this.

This continuous variation and change creates isolated, myopic views into the security posture across the various tools being used, but it doesn't capture everything happening. This fragmented view creates gaps in visibility and enforcement, and cyberattackers seek these gaps. The work required to identify threats, isolate them, and kick-off remediation efforts further slows down delivery efforts because so much manual effort has to go into uncovering these gaps and unwrapping issues after they've caused damage.

Ultimately, without a unified view and a comprehensive approach, no organization is capable of moving at the speed, or with the efficacy, that modern, digital businesses require.

Advantages Of A Platform Approach

Lacework looks at this challenge from an end-to-end perspective, and in doing so, threat detection and risk assessment happen across the entire scope of cloud and containerized environments. This gives users an all-encompassing view into cloud configurations, account activities, workload/runtime analysis, and automated anomaly and threat detection. The advantages over distributed solutions include:

Runtime visibility

Security issues must be addressed in real-time and at the point of being discovered. A unified solution provides visibility on activities and events happening at runtime, and without having to adhere to specific rules.

Machine learning

Security rules become obsolete as soon as they're deployed, and attacks thrive on this lag time. Machine learning relies not on rules, but on analysis of behaviors. And this approach begins to learn behaviors immediately, and gets more intelligent as it continuously analyzes cloud and container activity.

Accurate alerts

Rules-based security systems deliver many false positives which leads to alert fatigue within organizations. Alerts should only flag what is new and anomalous.

Simplified approach

Cloud platforms have native applications that store event log data, which is recalled when there is an indication of a threat. But at that point, it's effectively too late. Automated threat defense techniques are able to apply visibility, insight, and analysis capabilities to this log data at runtime, so users get both a continuous and automated view into their environment. Runtime analysis coupled with a review of historical event data provides enterprises with intelligence about threats sourced from internal resources, or during interactions with third-party data and applications. Dead accounts, inappropriate data exfiltration, and other aspects of misuse within a cloud or container environment are some of the indicators of potentially malicious events.

Behavioral anomaly detection

A major differentiator for security solutions is their level of accuracy in detecting anomalies. When events are analyzed against normalized behavior, only those issues that are truly problematic are surfaced. In this approach, instead of investigating every machine, user, and application individually, behavior baselining clusters these together based on historical behavior analysis, and alerts when behavior is abnormal. Rather than being alerted multiple times for activities on multiple machines that all operate according to the same behaviors, alerts are generated only for those few issues that deviate from the norm.

Power Of automation

The cloud enables organizations to deploy, scale, and configure their IT infrastructure at great speed and efficiency. But runtime threat detection involves analysis of the massive volume of events at fast rates. That's possible by automating threat detection. Traditional security approaches are hard to automate. Runtime threat detection based on behavior baselining and machine techniques pave the way to automate the entire workflow and to provide security teams with investigative insights.

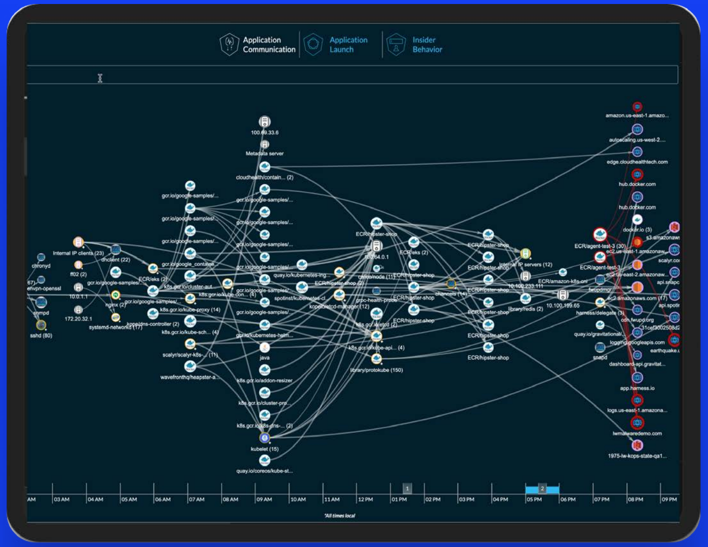
Too many companies think they must choose between speed and security. They also have existing security tools they are trying to maximize. While these realities are certainly understandable, they have to be removed from the equation when planning for a digital future.

New security tools designed to deeply monitor cloud infrastructure and analyze workload and account activity in real time make it possible to deploy and scale without compromising security. When operating in the cloud, businesses need to know that their infrastructure remains secure as it scales. They need assurance that they can deploy services that are not compromising compliance or introducing new risk. This can only happen with new tools designed specifically for highly dynamic cloud environments, tools that provide continuous, real-time monitoring, analysis, and alerting.

The task may appear daunting, but using a platform approach means that organizations can apply not just the concepts of security throughout the development and delivery lifecycle, but now have a foundation on which all activity can operate because it is continuously looking for any and all behavioral abnormalities, irrespective of where they live, to identify issues.

With a complete, modern security platform that has been designed specifically to meet the challenges of public cloud environments in both build-time and run-time operations, organizations can take advantage of a security-first model that enables continuous visibility, automation, and the ability to move fast. This will not only strengthen security, it will provide IT and product teams with the tools and processes they need to successfully meet the requirements of the cloud era.

Tools that provide continuous, real-time monitoring, analysis, and alerting



Ready to chat?

Request a demo

Lacework delivers security and compliance for the cloud generation. The Polygraph® Data Platform is cloud-native and offered as-a-Service, delivering build-time to run-time threat detection, behavioral anomaly detection, and cloud compliance across multi-cloud environments, workloads, containers, and Kubernetes. Trusted by enterprise customers worldwide, Lacework significantly drives down costs and risk, while removing the burden of unnecessary toil, rule writing, and inaccurate alerts. Lacework is based in San Jose, California, and backed by Sutter Hill Ventures, Liberty Global Ventures, Spike Ventures, the Webb Investment Network (WIN), and AME Cloud Ventures.

Get started at www.lacework.com

LACEWORK®