VALTIX

# HOW LOG4SHELL CHANGED CLOUD SECURITY

New research shows how IT leaders are changing the way they secure cloud workloads in the aftermath of Log4Shell

VALTIX

It’s an obscure piece of software that was exploited to shake the entire global cybersecurity apparatus. Log4J is used to record all manner of digital activities that hum under the hood of millions of computers, and once hackers discovered it was vulnerable to attack, it opened up a dangerous vulnerability for IT teams across every industry.

Log4J was a “wake up call” for IT leaders. But this humble piece of internet infrastructure became the worry of not just IT teams, but executives and boards as they scrambled to protect their most valuable data, systems, and platforms.

Valtix, a multi-cloud security company, wanted to understand how Log4J changed how IT teams secure their future.

Valtix surveyed 200 Cloud Security Leaders to better understand how they protect every app across every cloud in the aftermath of Log4J. The study was conducted in March 2022 with a random sample of screened IT managers and executives in the US. The margin of error for this study is +/- 6.9% at the 95% confidence level.

## Survey Methodology

A random sample of US-based respondents was recruited to respond to our survey using a variety of digital communication channels including permission-based in-app messaging, email, social media and SMS. All responses were collected using an online questionnaire. Respondents were profiled, vetted and screened prior to taking the survey, and all respondents were provided financial incentives for their participation.

## What you will learn in this research report

- **How IT leaders have altered their security strategy in the wake of Log4J**
- **The most common responses to Log4J**
- **How Log4J has affected security confidence with IT teams**
- **The degree to which IT teams are still dealing with Log4J**
- **The key trends, tools and tactics IT leaders are using to protect from cloud security threats**
- **The top challenges to deploying new security technology within organizations**
- **How IT leaders see Defense in Depth as a security approach**
- **The perceived security strength of Platform as a Service (PaaS)**

## Who is this research for?

- **Security and Privacy leaders who want to prepare for the next unexpected security development**
- **Executives who want to better support IT teams cleaning up after Log4J**
- **Cloud and PaaS leaders who want to see how their peers are dealing with security vulnerabilities**

## Respondent Breakout

**100%** of respondents are IT and cybersecurity leaders

**100%** of respondents work directly with cloud security issues

**36%** are C-level or higher

**43%** are VP level or higher

**77%** are director level or higher

**100%** are manager level or higher

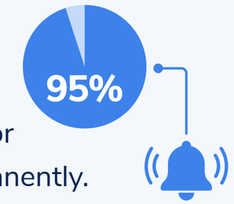
**Top industries represented:**

Computer hardware | Computer software | Financial services | Manufacturing

# STUDY INSIGHTS
## The Fallout from Log4J

### Log4J set off alarm bells.

95% of IT leaders say Log4J / Log4SHELL was a wake up call for cloud security - changing it permanently.



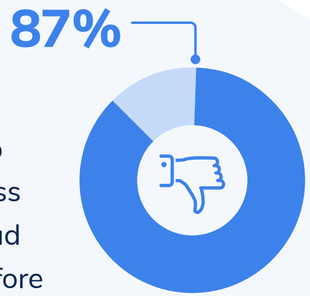

### Log4J taught IT leaders the status quo isn't good enough.

Why does Log4J / Log4SHELL change the game of cloud security:

- **The security protections in place now are insufficient**
- **Other high severity open source vulnerabilities will emerge**
- **Cloud service providers themselves might have vulnerabilities that could impact their teams**

### Log4J ate into confidence.

As a result of Log4J, 87% of security leaders feel less confident about their cloud security than they did before




### The Log4J impacts businesses.

83% of IT leaders say that the response to Log4J has impacted their ability to address business needs

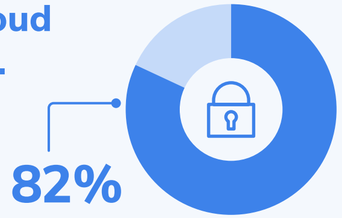
✓ Log4J impacted not only the security posture for organizations across the globe, but the very way IT leaders think about security. Log4J is ubiquitous with enterprise apps and cloud services, and when it was exposed, it set off an "all hands on deck" effort in IT teams across the globe to patch it up.

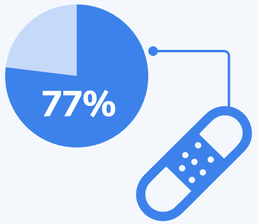
# The Fallout from Log4J

CONTINUED

## Log4J shuffled cloud security priorities.

82% of IT leaders say their priorities have changed due to Log4J




## A vulnerable Log4J is still with us.

77% of leaders are still dealing with Log4J patching

## Log4J revealed a need for new tools and processes.

As a result of Log4J, security leaders are prioritizing additional


## Financial services industry has shuffled its priorities.

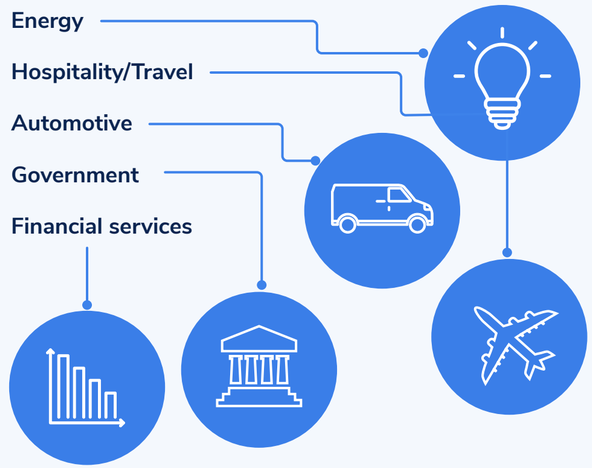
The top industries that have reprioritized their cloud security initiatives after Log4J:

1. Financial services
2. Pharmaceutical
3. Automotive
4. Consumer products
5. Manufacturing

*Industry data is directional

## Energy industry has low confidence due to Log4J.

The top industries where confidence is still negatively impacted due to Log4J:




*Industry data is directional

# Exploring Beyond Legacy Security

## On-prem is easier than public cloud.

**86%**

86% of IT leaders agree it's more challenging to secure workloads in a public cloud than in an on-prem datacenter

## Leaders recognize that there's no such thing as an invulnerable cloud workload and defense in depth is needed.

97% of IT leaders view Defense in Depth as essential in the cloud

**97%**

## Budget constraints slow tech adoption.

Top reason IT teams don't frequently deploy new tech to protect their workloads


✓ 96% of enterprises say their cloud security threats grow more complex every year. New players, threats, tools, business models and requirements keep IT teams more relevant than ever. Here's what's next for IT leaders.

# Exploring Beyond Legacy Security

CONTINUED

## Agent-based security is a challenge.

79% of IT leaders agree that agent-based security solutions are difficult to operationalize in the cloud

## Public clouds are still considered somewhat secure.


52% of IT leaders believe they have sufficient security of their Platform as a Service (PaaS) cloud services (AWS S3, AWS RDS, Azure SQL etc)

## Security simplicity varies by public cloud.

Do cloud services make advanced security easy?

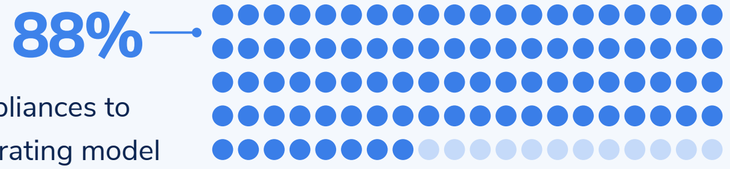

**52%** of IT leaders say AWS makes advanced security easy

**14%** of IT leaders say GCP makes advanced security easy

**32%** of IT leaders say Azure makes advanced security easy

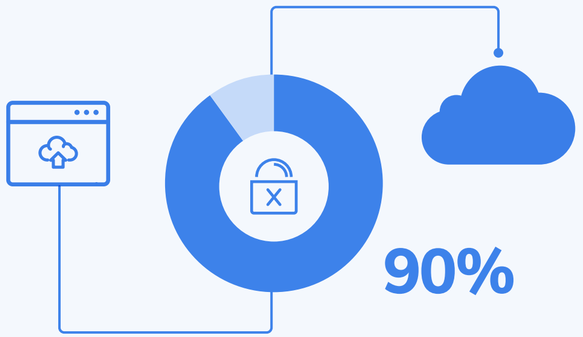
## Firewall appliances in the cloud upends the cloud computing model.

88% of IT leaders say bringing network security appliances to the cloud is challenging to the cloud computing operating model




## Additional risks confirmed to be created by open network paths.

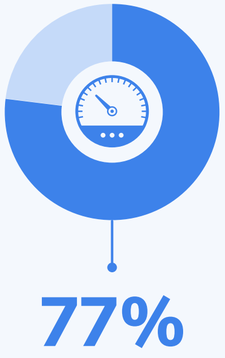
90% of IT leaders say open network paths to cloud workloads from the public internet can create security risk



# Slow Security Slows Business

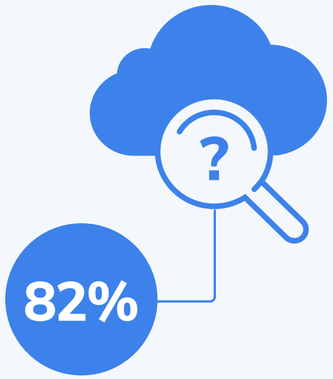
## Slow security implementation slows business.

77% of businesses are slowed because securing new cloud workloads adds time to deployment cycles




## Low security visibility is common.

82% of IT leaders say visibility into active security threats in the cloud is usually obscured

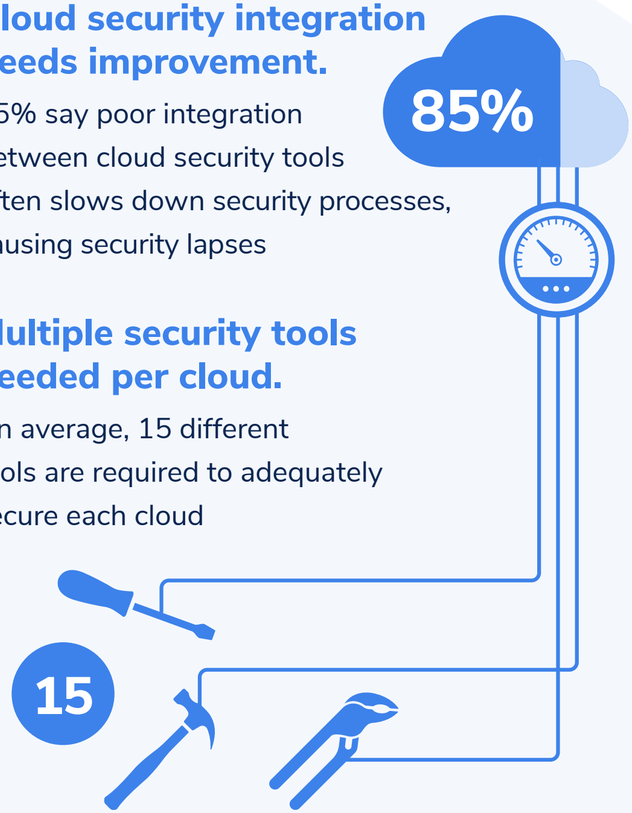



## Cloud security integration needs improvement.

85% say poor integration between cloud security tools often slows down security processes, causing security lapses

## Multiple security tools needed per cloud.

On average, 15 different tools are required to adequately secure each cloud

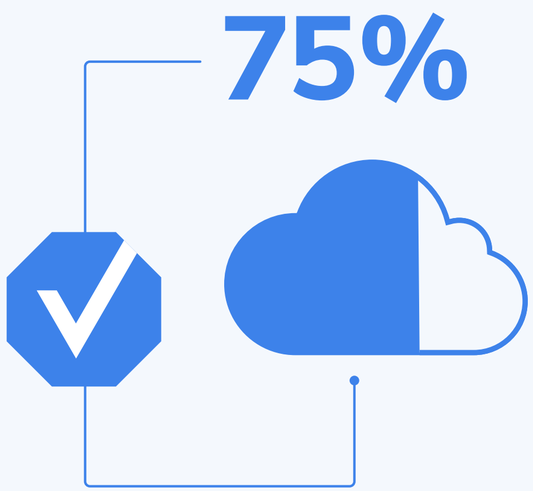



Product, marketing, finance and executive teams are asking more from IT than ever before. When development cycles slow or block business momentum, the entire organization suffers. To avoid this, IT leaders are constantly seeking out ways to both speed up and stand up new solutions to keep the business competitive.

# Current State Reflects Lack of Confidence

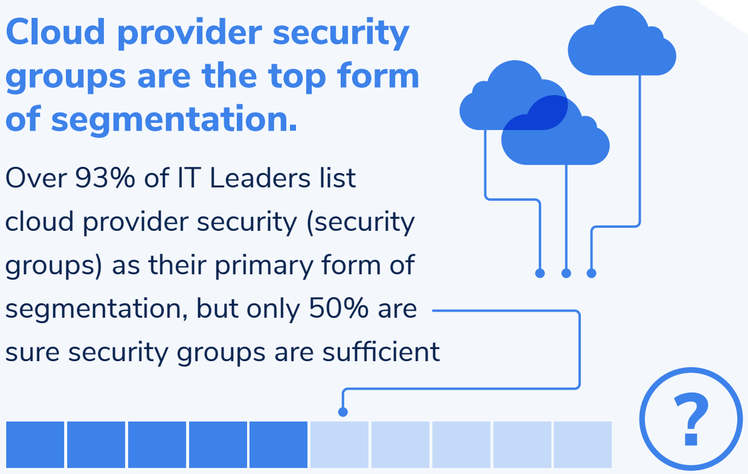
### Low confidence in separation from the public internet.

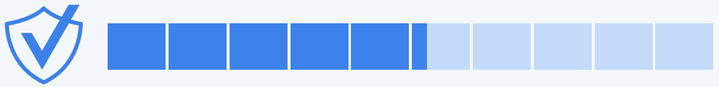
Less than 75% are confident that all of their cloud workloads are fully segmented from the public internet




### Cloud provider security groups are the top form of segmentation.

Over 93% of IT Leaders list cloud provider security (security groups) as their primary form of segmentation, but only 50% are sure security groups are sufficient



### IT leaders don't feel fully protected.

Only 53% feel confident that all of their public cloud workloads and APIs are fully secured against attacks from the internet

Effective cloud security creates resilient organizations.

As more businesses today are "cloud first," IT leaders must constantly discover new ways to access data, prevent threats, and facilitate transactions in ways that go far beyond the default security settings of public clouds.

## Summary Log4J Redefined and Re-prioritized Cloud Security

Log4J woke up the IT world, making leaders aware of just how brittle their defenses actually are in the cloud. While public clouds offer new opportunities to modernize and transform organizations, many organizations have struggled to find a cloud security operating model built for a more dynamic, distributed, and exposed environment than their legacy datacenter. IT and security leaders are in a precarious state as they continue dealing with Log4J while at the same time looking to invest in cloud security technology that will help them be ready for the next incident.

**https://valtix.com**

Valtix is on a mission to protect every workload, every app architecture, across every cloud. The first multi-cloud network security platform delivered as a service, Valtix was built to combine robust security with cloud-first simplicity and on-demand scale. Powered by a cloud-native architecture, Valtix provides an innovative approach to multi-cloud security that is deployable in just 5 minutes and adapts to changes in seconds. The result: security that is more effective and aligned to cloud agility requirements. With Valtix, organizations don't have to compromise in the cloud. They can meet critical security and compliance requirements without inhibiting the speed of the business.

Join 4 of the top 10 pharmaceuticals and leaders across every industry and sign up free in minutes.