HashiCorp

From Best Practice to Mandate

The Rising Stakes of Data Protection in Australia

Jamie Wright
Staff Solutions Engineer

What is the real impact of security incidents?

Josh [redacted] <[redacted]>

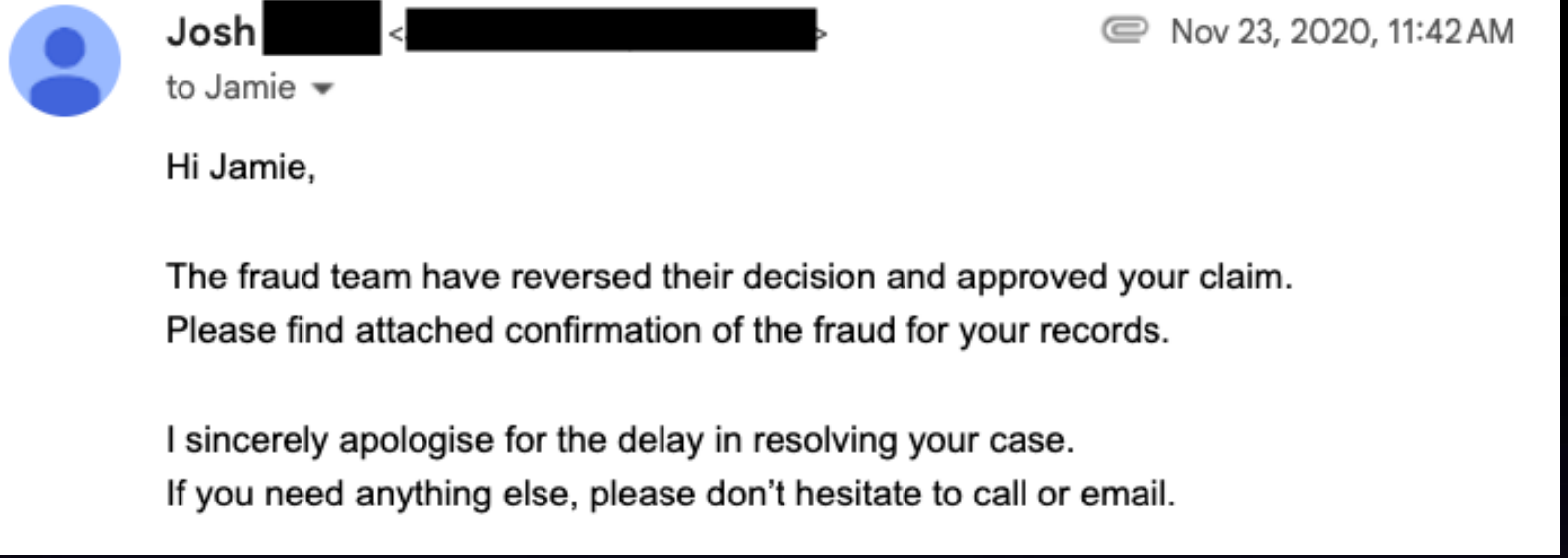
Aug 26, 2020, 4:59 PM

to Jamie

Hi Jamie,

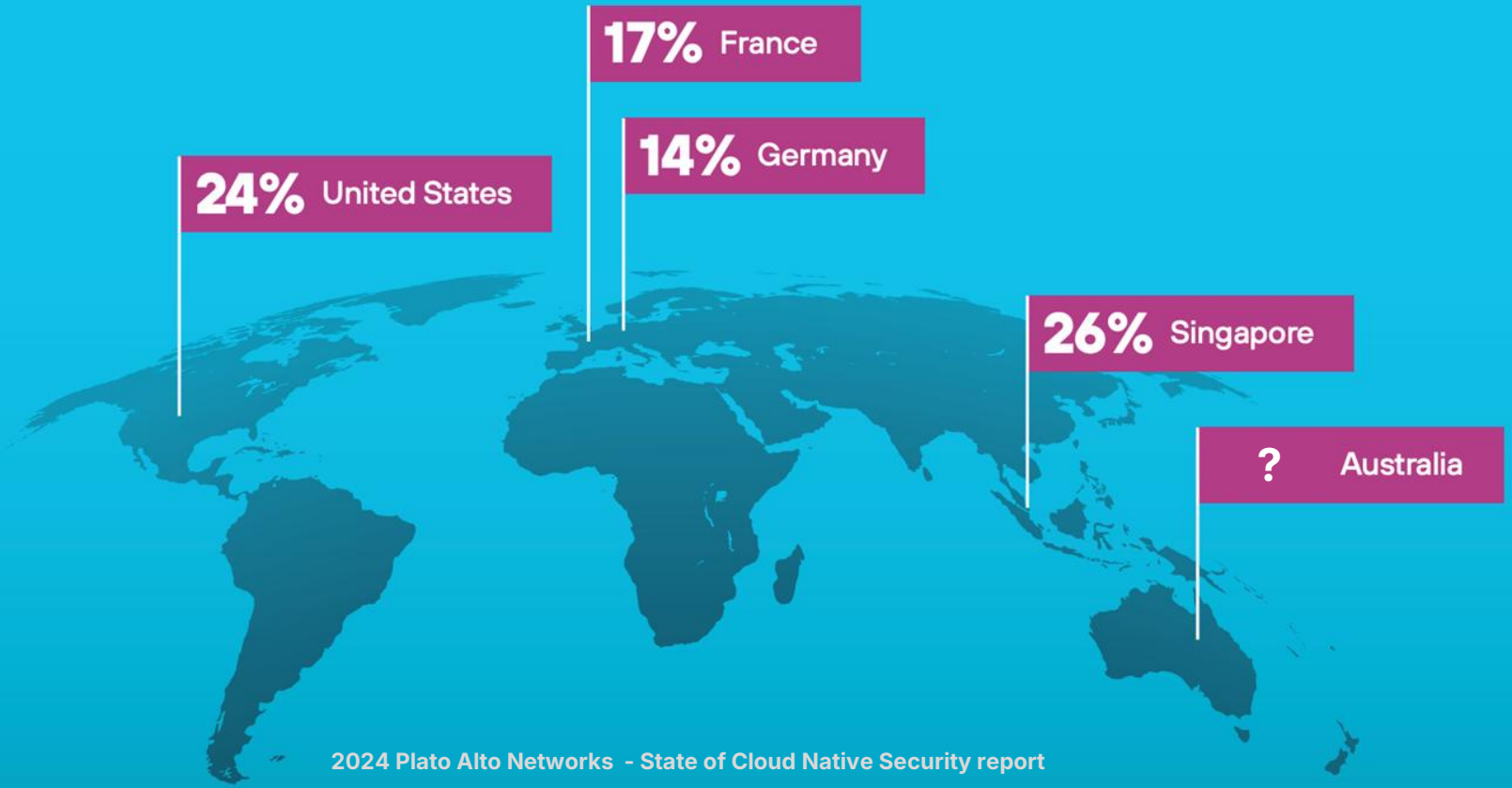
Unfortunately I am emailing to report that the fraud claim was denied on three points:

- Your correct details have been entered in our system,
- The phone was delivered to your address, and
- You accepted delivery of the phone.



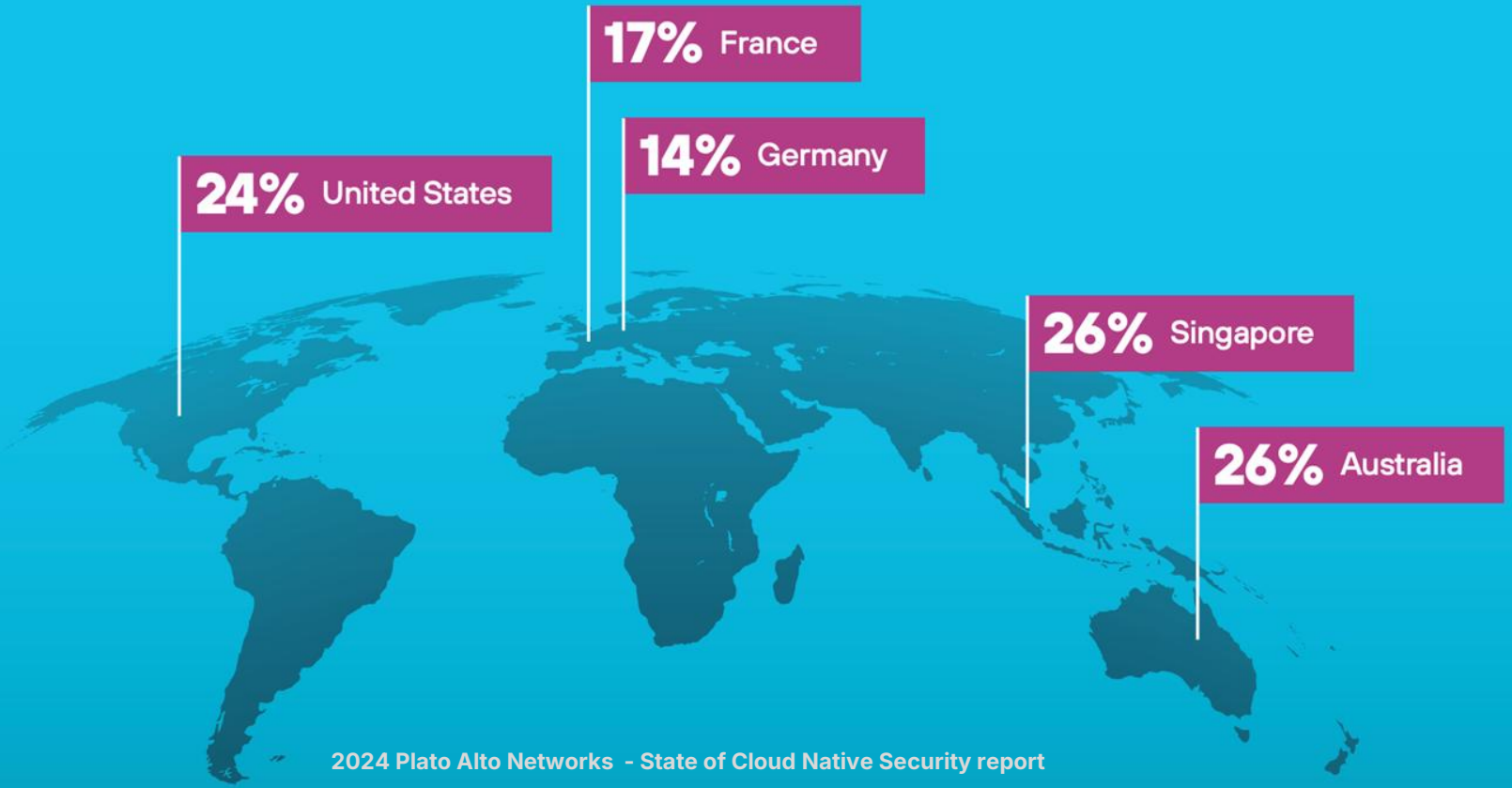
Ask yourself, what motivates you to do your best work?

Percentage of companies running 100% in the public cloud



2024 Plato Alto Networks - State of Cloud Native Security report

Percentage of companies running 100% in the public cloud



2024 Plato Alto Networks - State of Cloud Native Security report

Cloud Identity Statistics

1%

percentage of permissions used by identities [1]

80%

of workload identities are inactive, double the percentage reported in 2021 [1]

[1] 2023 Microsoft state of cloud permissions risks report

Motivators For Regulations

Reliability/Availability of systems

Modern applications are sometimes required to be available to consumers as close to 100% as possible.

Confidentiality of Data

Personally Identifiable Information in the wrong hands can have massive downside effects on privacy, health or financial well being of consumers.

Accuracy of Information

Systems like banking and health care need accuracy for the safety and well being of the consumer.

To Protect and Prove

1 Controls

The objectives of the standard for the certification. E.g. Must encrypt data in transit. Preventative, Corrective, Detective.

2 Processes

The implementation of the Controls. E.g. Create PKI certificates with Vault and distribute to applications via secure agents.

3 Auditing

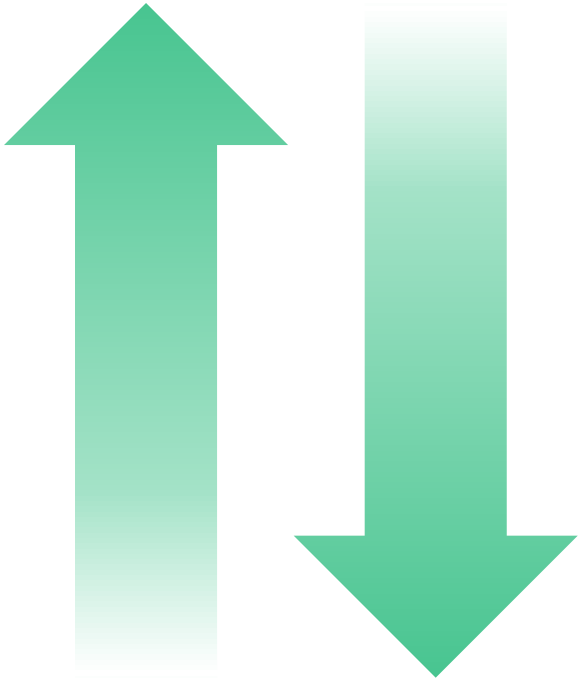
Prove that controls and processes are implemented to standards. E.g. Create documentation of architecture and logs of of process working.

4 Reporting

Give auditors detailed information on conforming to standards though auditing mechanisms. E.g. Show access control lists, authentication procedures, system logs to prove Controls are being met.

What motivates us to change?

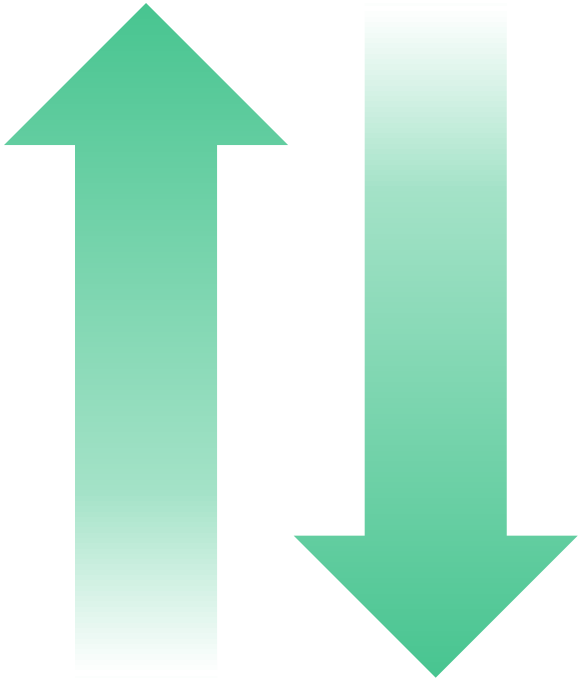
- Profits
- Revenue
- Quality
- User Satisfaction
- Security
- Compliance
- Productivity
- Velocity
- Talent Retention



- Costs
- Risk
- Variance
- Error Rates
- Time to Market
- Toil

What motivates us to change?

- Profits
- Revenue
- Quality
- User Satisfaction
- Security
- Compliance
- Productivity
- Velocity
- Talent Retention



- Costs
- Risk
- Variance
- Error Rates
- Time to Market
- Toil

Best Practice to Mandate

New requirements in PCI-DSS v4.0. Effective 31st March 2025

Payment Card Industry Data Security Standard: Requirements and Testing Procedures, v4.0.1

Best Practice to Mandate

New requirements in PCI-DSS v4.0. Effective 31st March 2025

Least privilege

7.2.5.1 All access by application and system accounts and related access privileges are reviewed as follows.

- The application/system access remains appropriate for the function being performed

Payment Card Industry Data Security Standard: Requirements and Testing Procedures, v4.0.1

Best Practice to Mandate

New requirements in PCI-DSS v4.0. Effective 31st March 2025

Least privilege

7.2.5.1 All access by application and system accounts and related access privileges are reviewed as follows.

- The application/system access remains appropriate for the function being performed

Key inventory

4.2.1.1 An inventory of the entity's trusted keys and certificates used to protect PAN during transmission is maintained.

Payment Card Industry Data Security Standard: Requirements and Testing Procedures, v4.0.1

Best Practice to Mandate

New requirements in PCI-DSS v4.0. Effective 31st March 2025

Least privilege

7.2.5.1 All access by application and system accounts and related access privileges are reviewed as follows.

- The application/system access remains appropriate for the function being performed

Key inventory

4.2.1.1 An inventory of the entity's trusted keys and certificates used to protect PAN during transmission is maintained.

Field-level encryption

3.5.1.2 While disk or partition encryption may still be present on these types of devices, it cannot be the only mechanism used to protect PAN stored on those systems.
... for example, through truncation or a data-level encryption mechanism.

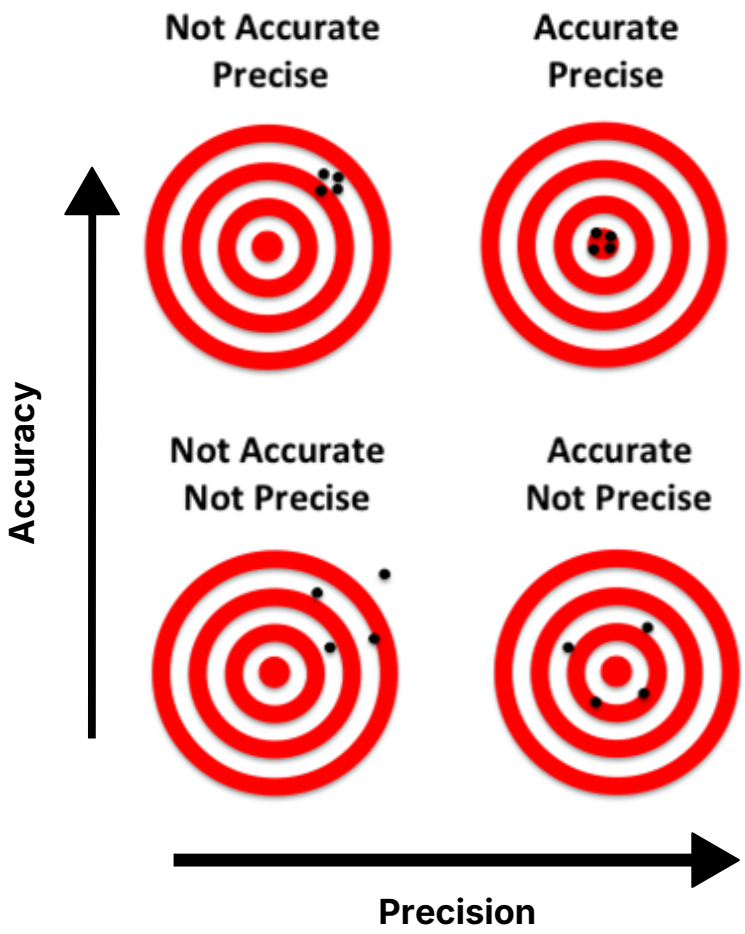
Full disk encryption helps to protect data in the event of physical loss of a disk and therefore its use is appropriate only for removable electronic media storage devices.

Payment Card Industry Data Security Standard: Requirements and Testing Procedures, v4.0.1

Regulations are there to establish a minimum standard

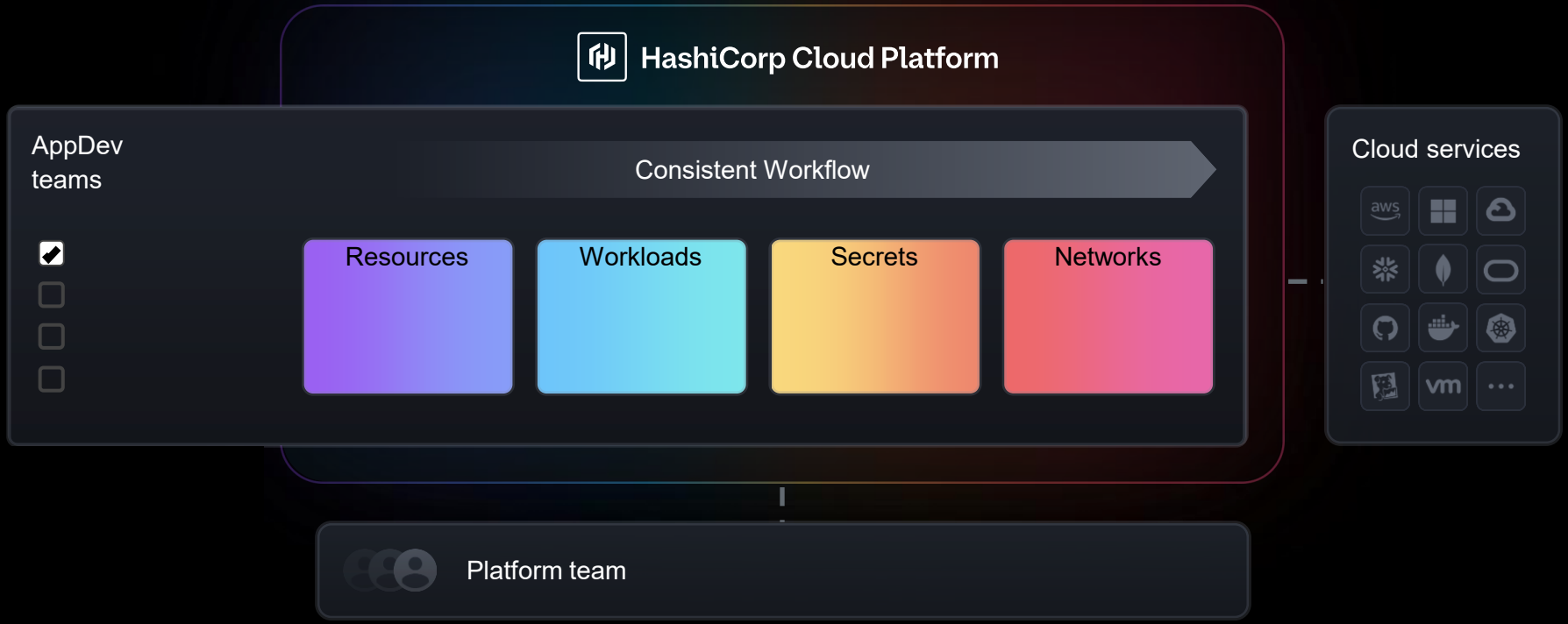
Compliance to regulation is not the same thing as being secure

Aim for being competitive, not just compliant.



Unified platform approach

The Infrastructure Cloud



Do cloud right