SECURECON 2019 | DALLAS, TEXAS

MOVE FAST & SECURE THINGS

ARMOR AND PALO ALTO NETWORKS

STAN GOLUBCHIK
Head of Alliances,
Armor

BERRET TERRY
Prisma Public Cloud Technical
Marketing

AGENDA

1. The Challenges of the Modern Cloud CISO
2. 5 Steps: Public Cloud & Good Security Hygiene
3. 3 Major Takeaways
4. Q & A

STAN GOLUBCHIK

HEAD OF ALLIANCES, ARMOR

Contact me at:
stan.golubchik@armor.com

BERRET TERRY

PRISMA PUBLIC CLOUD TECHNICAL MARKETING

Contact me at:
bterry@paloaltonetworks.com

CHALLENGES OF THE MODERN CLOUD CISO

PROBLEMS THAT KEEP A CISO AWAKE AT NIGHT

Lack a holistic strategy to minimize the impact of a breach

Require a cloud security readiness plan

Expanded attack surface driven by digital transformation initiatives

Risk management and cost reduction/avoidance

CYBERSECURITY STRATEGY BUSINESS DRIVERS

77%

Lack Consistent
Incident & Response Plan

80%

Risk Mitigation with
One Command Line

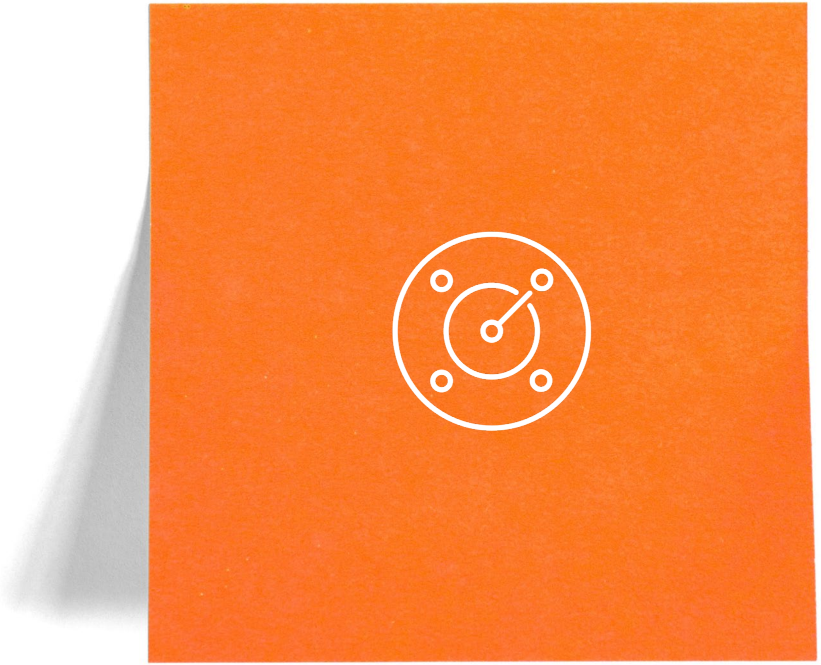
90%

Self-Inflicted Breaches

5 STEPS:
COMBAT CONCERNS

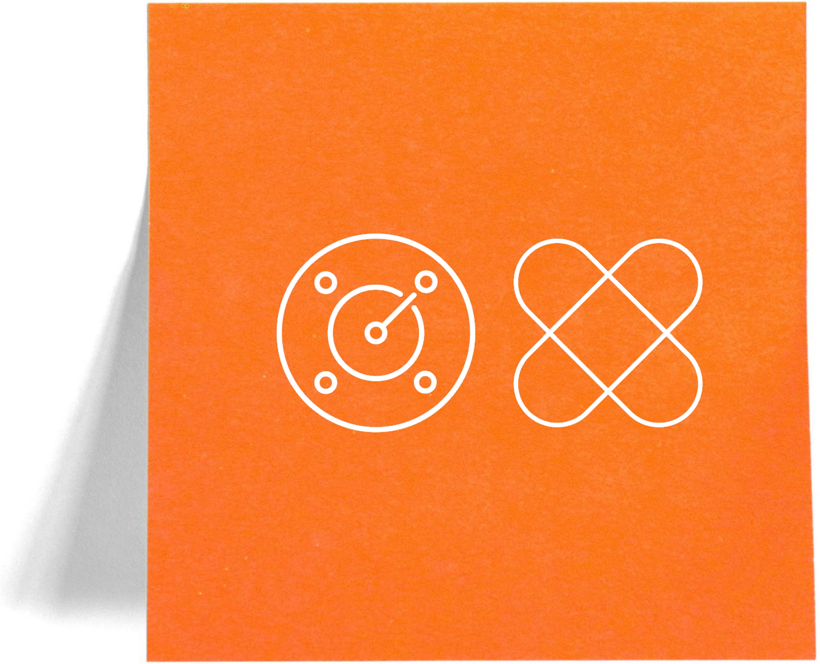
PATCH MONITORING

- Consistent patching is a cornerstone to maintaining a strong security posture
- Visibility into environment to identify critical OS-level patches for resolution
- Secure 3rd party cloud environments includin AWS, Azure, Google Cloud etc., through OS hardening, **patch monitoring**, managed malware protection, file integrity monitoring, log & event management and external vulnerability scans.



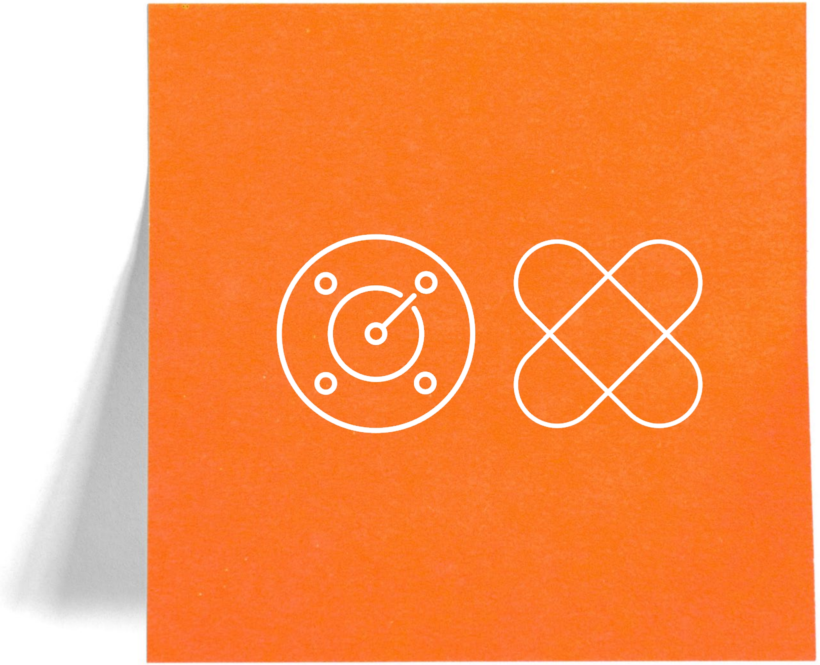
VULNERABILITY SCANNING + PATCH MONITORING

- Continuous vulnerability scanning places the customer’s hands on the wheel of their network
- Armor’s service scans internal and external networks for technical vulnerabilities, patching, and compliance issues
  - Provides clients with ability to mitigate risk; ensure compliance
- Complete visibility through the Armor Management Portal (AMP)
  - View weekly scan reports
  - Review past incidents
  - Continually monitor compliance results



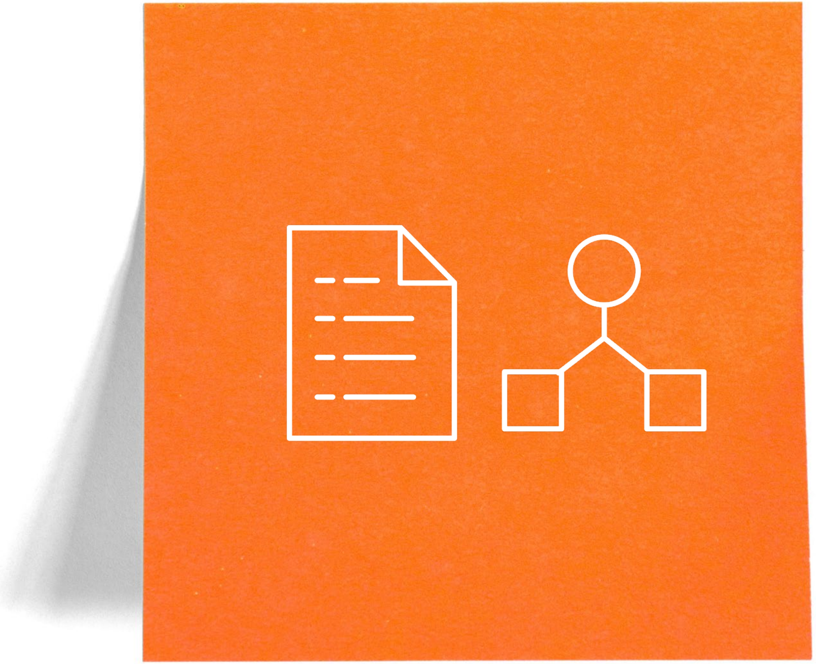
VULNERABILITY SCANNING + PATCH MONITORING

- Consistent patching is a cornerstone to maintaining a strong security posture
- Visibility into environment to identify critical OS-level patches for resolution
- Secure 3rd party cloud environments includin AWS, Azure, Google Cloud etc., through OS hardening, patch monitoring, managed malware protection, file integrity monitoring, log & event management and external vulnerability scans.



LOG MANAGEMENT AND LOG RELAY

- Data retention is important for audits – provides greater context of your environment to identify potential threats
- Armor's Log and Data Management service brings environment data to your team:
  - □ Storage for audit readiness
  - □ Correlation for potential threat identification
- Armor's Log Relay service extends the integration to public cloud environments
  - □ AWS: GuardDuty, VPC Flow Logs, CloudTrail and WAF
  - □ Cisco: ASA and ISR
  - □ Juniper: SRX
  - □ Fortinet FortiGate Firewall
  - □ More to come…



THE ERROR IS HUMAN, BUT COSTLY

⚠ MISCONFIGURATIONS, "HONEST MISTAKES," AND CARELESSNESS IS FUELING "ACCIDENTAL" CYBER RISK ACROSS ORGANIZATIONS.

14 Enterprise organizations have an average of 14 misconfigured IaaS/ PaaS instances running at one time.*

920M Thirteen major accidental (no threat actor involved) data exposures since 2017 exposed nearly one billion records.**

5.5% 5.5% of AWS S3 buckets have world read permissions, making them open to the public.*

8/13 The number of incidents where data was exposed by an affiliate, partner, or customer of a larger organization.**

*Source: "Cloud Adoption and Risk Report," McAfee – 2019. **Source: "Naked Data," Armor - 2019

THE COST OF A CLOUD MISCONFIGURATION

COSTS ASSOCIATED WITH RISKS: $148 PER EXPOSED RECORD, UPWARD OF A COMBINED $57B.

DETECTION & ESCALATION

Detecting and reporting a breach to the appropriate personnel in a timely manner.

Forensic and investigative activities, audit services, crisis management, and communications teams

NOTIFICATION COSTS

Properly notifying data subjects whose information has been compromised.

Hard costs of paper, equipment, labor, communications with regulators and outside experts.

POST DATA BREACH RESPONSE

Helping individuals affected by the breach to communicate with the company.

Help desk activities, credit report monitoring and identity protection services, issuing new accounts or credentials, legal expenses, product discounts, and regulatory fines.

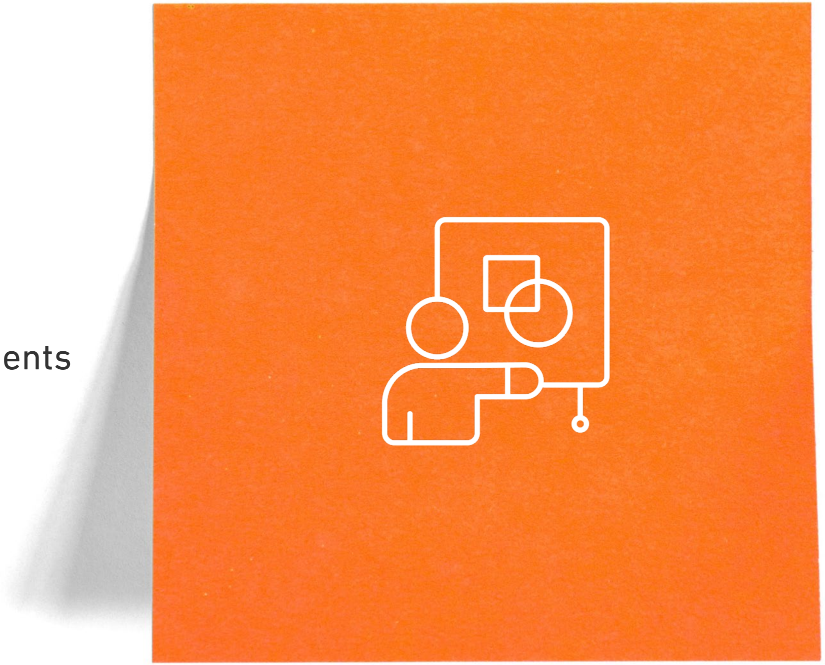
LOSS OF BUSINESS COST

Overall cost to the business.

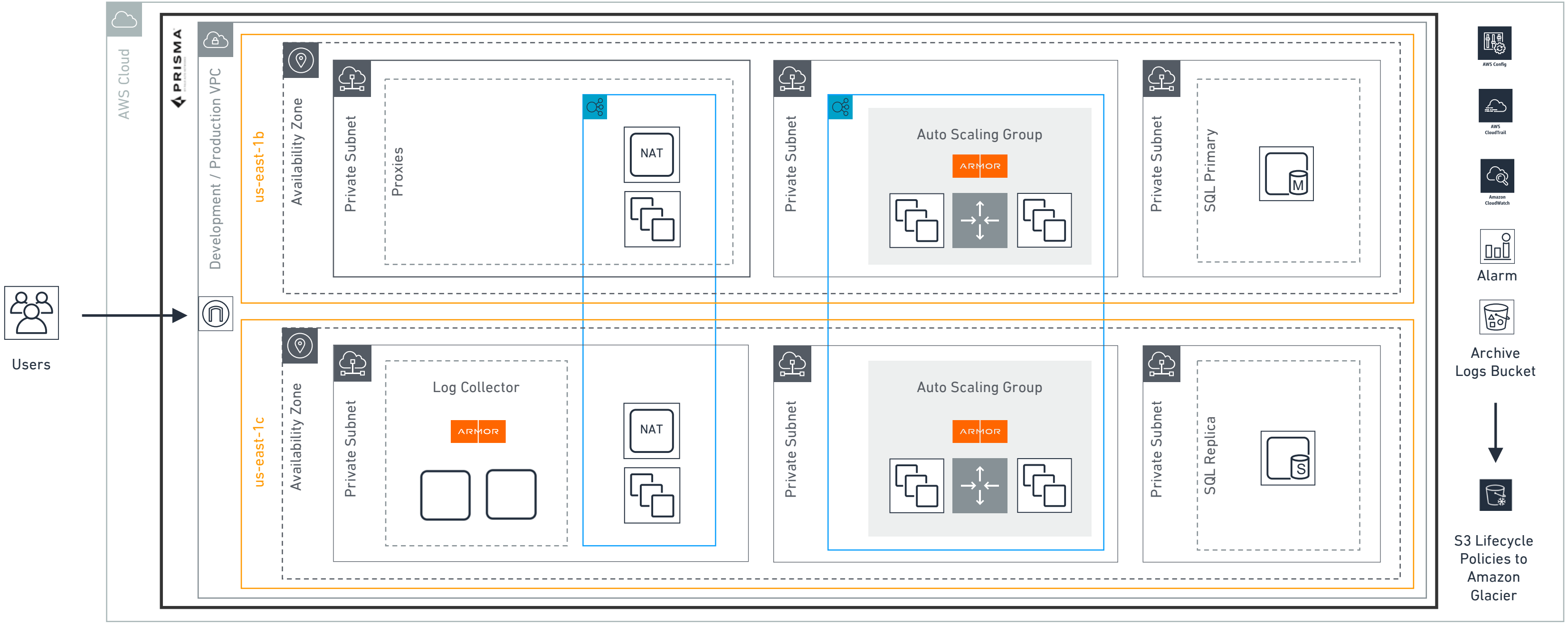
Accounts for losing customers, system downtime, business disruption, and reputation damage.

TRAINING FOR YOUR ORGANIZATION

- Maintain security guardrails for your public cloud infrastructure
- Develop and implement security guardrails for your public cloud
- Maintain compliance standards of your public cloud deployments
- Analyze & investigate public cloud security incidents
- Integrate third-party security platforms



ARMOR AND PRISMA PUBLIC CLOUD AUTOMATED COMPLIANCE



3 MAJOR TAKEAWAYS

THE BIG 3

1

Cloud has changed everything – we must secure our workloads against accidental and intentional threats

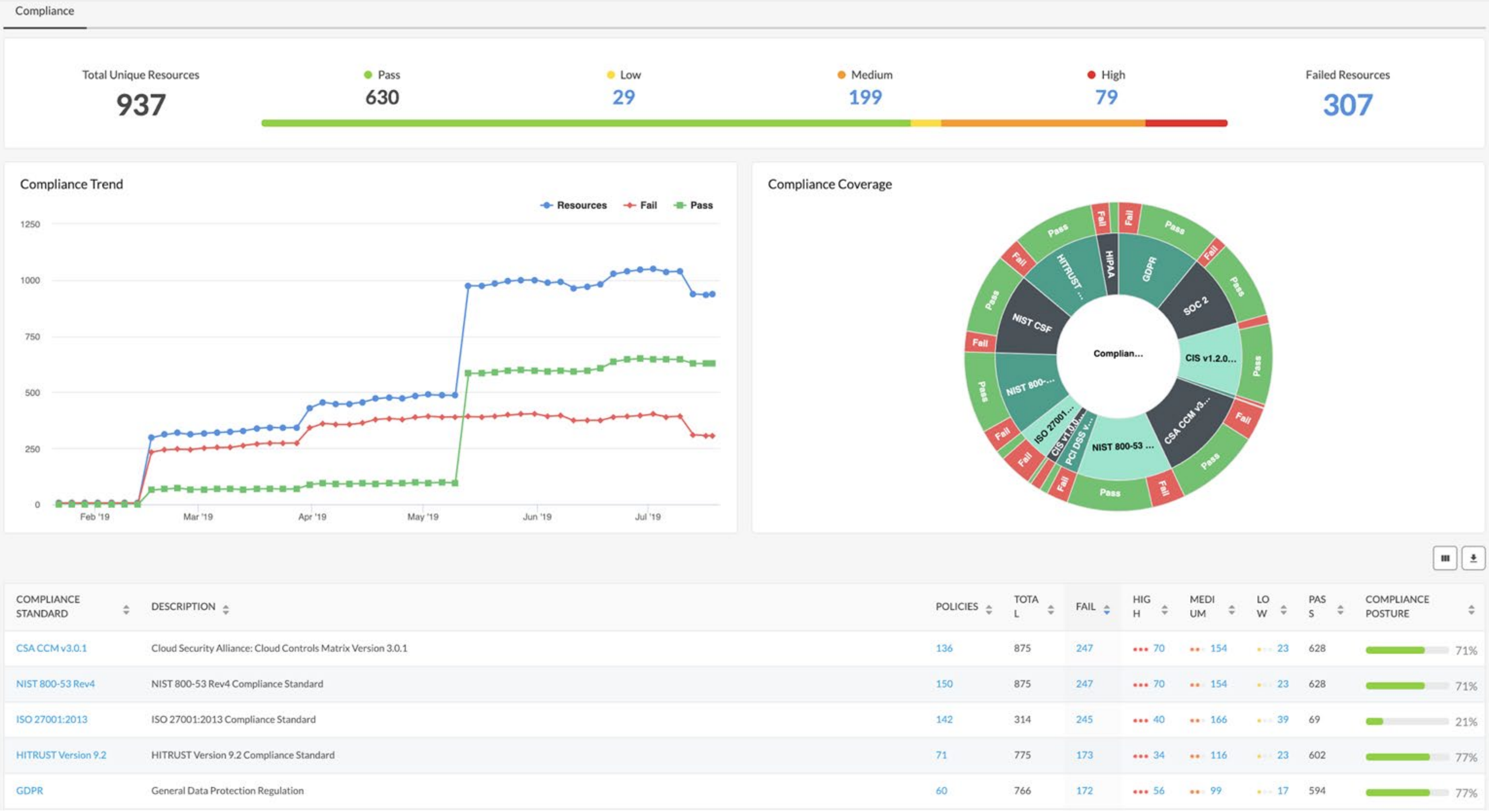
2

Hard part of security is it's an operations problem

3

Having a cloud security readiness plan will lower your risk and breach costs

DEMO



Compliance

Total Unique Resources	● Pass	● Low	● Medium	● High	Failed Resources
937	630	29	199	79	307

Compliance Trend

Compliance Coverage

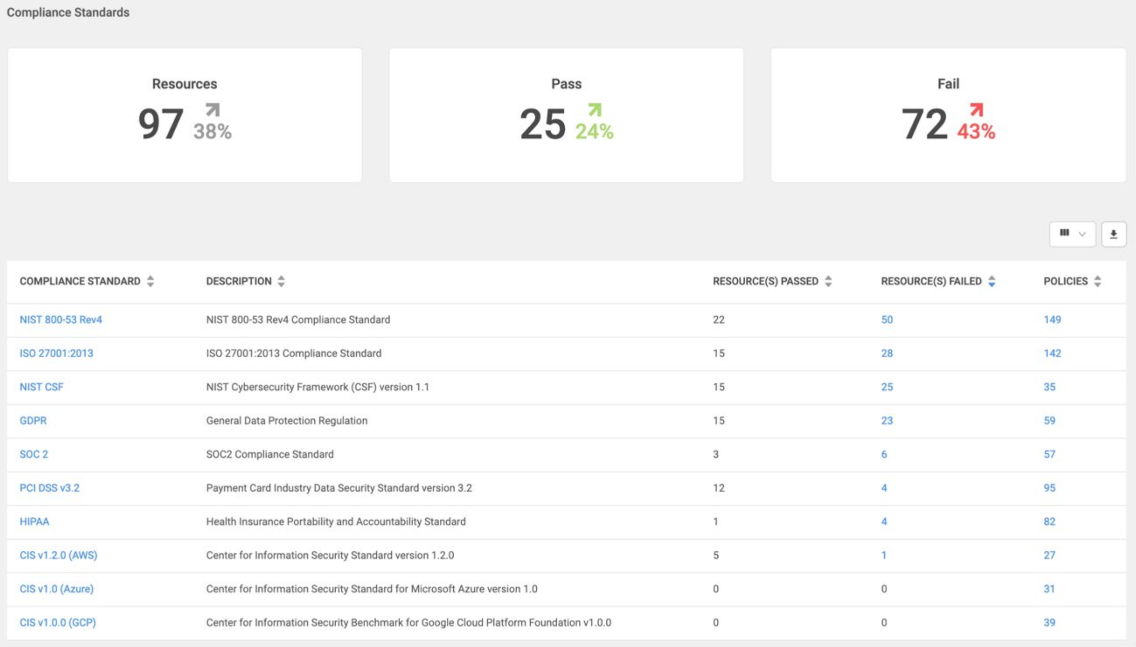
COMPLIANCE STANDARD	DESCRIPTION	POLICIES	TOTAL	FAIL	HIGH	MEDIUM	LOW	PASS	COMPLIANCE POSTURE
CSA CCM v3.0.1	Cloud Security Alliance: Cloud Controls Matrix Version 3.0.1	136	875	247	70	154	23	628	71%
NIST 800-53 Rev4	NIST 800-53 Rev4 Compliance Standard	150	875	247	70	154	23	628	71%
ISO 27001:2013	ISO 27001:2013 Compliance Standard	142	314	245	40	166	39	69	21%
HITRUST Version 9.2	HITRUST Version 9.2 Compliance Standard	71	775	173	34	116	23	602	77%
GDPR	General Data Protection Regulation	60	766	172	56	99	17	594	77%

SECURITY AND COMPLIANCE POSTURE

PRISMA
BY PALO ALTO NETWORKS

Easily quantify and assess your cloud security and compliance posture

Armor's Cloud Security Assessment boosts the security of your public clouds and improves your compliance posture by monitoring against industry standards, regulatory mandates and best practices to prevent issues like misconfigurations, unwarranted access, and non-standard deployments.



Compliance Standards

Resources
97 ↗ 38%

Pass
25 ↗ 24%

Fail
72 ↗ 43%

COMPLIANCE STANDARD	DESCRIPTION	RESOURCE(S) PASSED	RESOURCE(S) FAILED	POLICIES
NIST 800-53 Rev4	NIST 800-53 Rev4 Compliance Standard	22	50	149
ISO 27001:2013	ISO 27001:2013 Compliance Standard	15	28	142
NIST CSF	NIST Cybersecurity Framework (CSF) version 1.1	15	25	35
GDPR	General Data Protection Regulation	15	23	59
SOC 2	SOC2 Compliance Standard	3	6	57
PCI DSS v3.2	Payment Card Industry Data Security Standard version 3.2	12	4	95
HIPAA	Health Insurance Portability and Accountability Standard	1	4	82
CIS v1.2.0 (AWS)	Center for Information Security Standard version 1.2.0	5	1	27
CIS v1.0 (Azure)	Center for Information Security Standard for Microsoft Azure version 1.0	0	0	31
CIS v1.0.0 (GCP)	Center for Information Security Benchmark for Google Cloud Platform Foundation v1.0.0	0	0	39

Q & A

STAN GOLUBCHIK

Head of Alliances,
Armor

BERRET TERRY

Prisma Public Cloud Technical
Marketing

ARMOR | paloalto NETWORKS | SECURECON 2019 | DALLAS, TEXAS

THANK YOU.

WWW.ARMOR.COM

WWW.PALOALTONETWORKS.COM