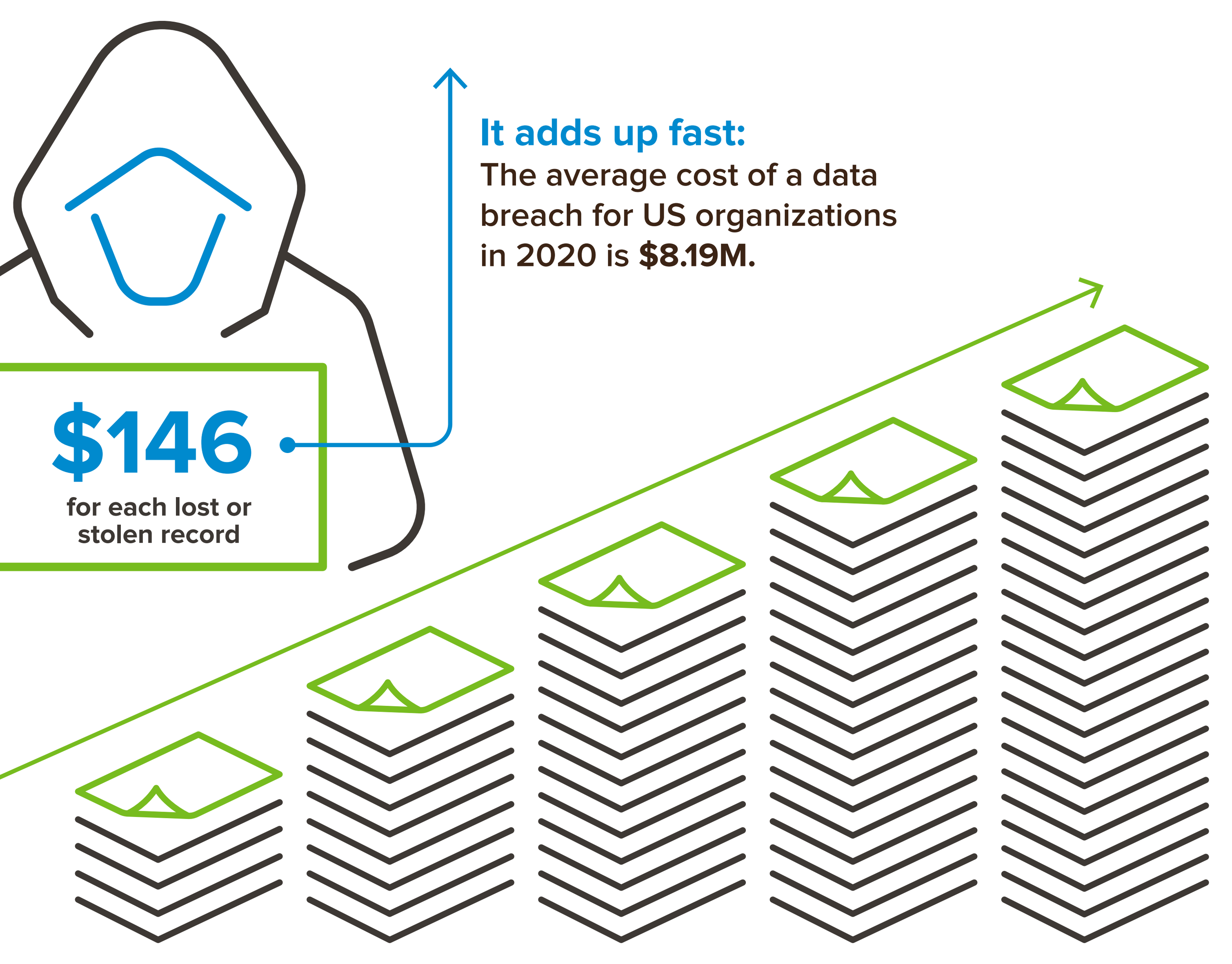
aria CYBERSECURITY SOLUTIONS

Why is Complying with Data Privacy Regulations So Hard?

Meet the Most Challenging Compliance Requirements with ARIA Cybersecurity

Data Breaches Continue to Rise

Billions of PII records are lost, stolen, or compromised each year – numbers that increase each and every year.



As a result, more and more data privacy regulations are being created to protect consumers' rights.

A Complex Landscape Makes Compliance Difficult

Each year, more data privacy regulations are passed at the state, national, and international level. Even worse, each regulation has its own requirements, many of which could conflict with other regulations.

International Regulations Spotlight: GDPR Sets the Stage

Gives EU citizens more control over their **personal data** and the rights to bring civil suits against organizations.

Requires breach notification within **72 hours**, including the exact records affected.

Failure to comply can lead to fines of **4% in revenue or €20M**.

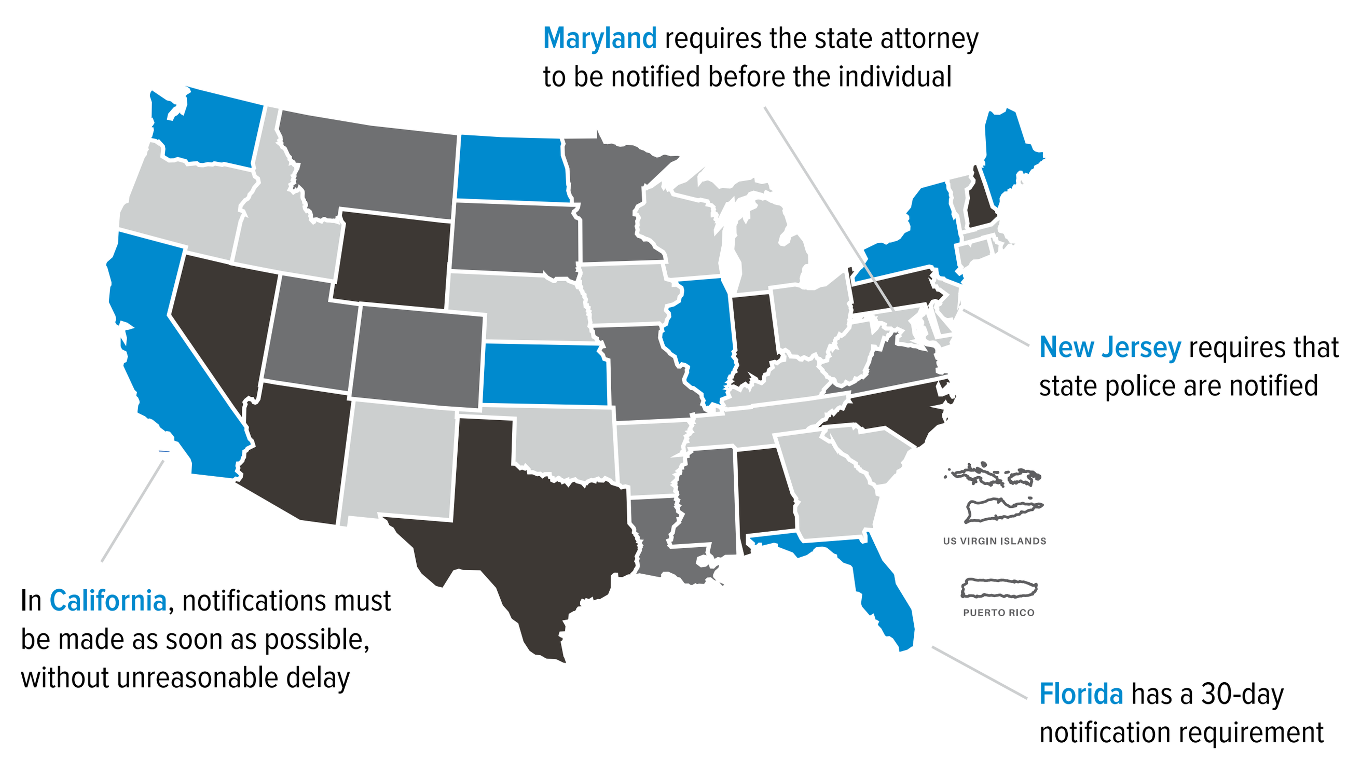
Federal Laws to Consider: CMMC

The Department of Defense recently introduced its Cybersecurity Maturity Model Certificate (CMMC) certification to improve the protection of controlled unclassified information (CUI) within the defense industrial base.

Yet with five different levels requiring a total of **171 different security practices**, CMMC can be hard to understand — and hard to comply with.

State Laws Add to the Confusion

All 50 states (plus the District of Columbia, Puerto Rico, and the U.S. Virgin Islands) have data privacy laws in place.



Industry Regulations are the Final Nail in the Coffin

Companies in highly regulated industries must comply with additional regulations. These include (but are not limited to):

HIPAA
Seeks to protect the privacy and security of PHI.

PCI DSS
12 specific regulations to reduce fraud and protect credit card information.

NYDFS/23 NYCRR 500
Requires financial institutions to establish and maintain a "risk-based, holistic, and robust security program" to protect consumers' data.

NIST
Provides a catalog of security controls for all U.S. federal information systems except those related to national security.

Organizations Struggle to Meet Compliance with Existing Threat Detection and Response Approaches

The main problem is that traditional security solutions such as SIEMs, IDS/IPS tools, Threat Intel tools, EDRs, NDA, and SOARS aren't effective.

What's driving this?

An organization's threat surface is growing with public cloud, IoT, BYOD and WFH, giving hackers more vulnerable access points.

Existing security tools generate too much alert noise – more than 5,000 a day – making it impossible to investigate all of them.

Network-borne threats are missed due to lack of visibility and monitoring of internal network traffic, particularly east-west.

A Better Approach Means No Data Loss and No Compliance Fines, Ever.

aria ADR
Automated, AI-driven threat detection and response: six security tools in one for complete coverage at a fraction of the cost.

aria PACKET INTELLIGENCE
Provides visibility into all network traffic, for full network monitoring, resulting in improved detection and containment effectiveness of security tools, including SIEMs, IDS/IPS, and forensic packet recorders.

aria KEY MANAGEMENT SERVER
Automatically generate and manage lifecycle requirements for encryption key management.

ARIA Cybersecurity Solutions enable organizations to:

- Provide complete visibility into the internal network, including east-west traffic
- Improve and automate the detection and response of network-borne threats
- Gain auditable compliance reporting to meet even the most challenging data privacy regulation
- Contain threats surgically, without, without taking devices offline

DOWNLOAD OUR COMPLIANCE EBOOK

Better Security, Better Compliance

To learn how our security solutions help organizations comply with even the most challenging data privacy regulations, visit ariacybersecurity.com today.

aria CYBERSECURITY SOLUTIONS

REV2.0-InfoG-12-20-DataPriv