HOW-TO GUIDE

Successful Data Privacy Compliance

Automate Threat Detection and Response and Meet the Most Challenging Compliance Requirements

aria CYBERSECURITY SOLUTIONS

Industry compliance challenges call for new security solutions

With breaches now an inevitability, it is important for organizations to understand and comply with an increasingly complex landscape of data privacy regulations.

This is an absolute necessity in order to mitigate, even eliminate, compliance fines and other negative consequences of a data breach.

This ebook will present an overview of the most important data privacy regulations, demonstrate why current security tools don't work, and describe ARIA's new approach to automated threat detection, response and containment for overcoming today's security and data privacy challenges.

CONTENTS

Why is it so hard to comply with data regulations?

Governments, both internationally and domestically, and industry associations, are developing data privacy regulations to not only attempt to protect consumers' PII/ePHI data, but to force transparency and accountability on what data was accessed, when and how, and what is being done to mitigate the damage.

Yet the security tools available for complying with these data privacy regulations are difficult, time-consuming, and generally ineffective.

This is true for three different reasons:

1 There are many industry, state, and international regulations. Not only are they different, but many are in conflict with each other and all have aggressive time requirements.

+

2 Traditional threat detection and prevention security tools don't work, in part because they can't provide full visibility into the network, especially east-west traffic.

+

3 The explosion of IoT devices present many new security vulnerabilities since IoT devices can't use agents or EDR solutions.

All of this adds up to unacceptable levels of security risk. And when it comes to compliance, these challenges make it extremely difficult to meet data privacy regulations – if not impossible.

How did we get here?

No company is safe, no matter what industry it is in or where it is located. The damage breaches are causing is devastating to organizations and consumers alike. In 2019, the chance of experiencing a data breach jumped to 29.6%, up from 27% in 2018.

Unfortunately, attacks like these recent examples are becoming too common:

RETAIL

Target

Attackers captured the full names, phone numbers, email addresses, payment card numbers, credit card verification codes, and other sensitive data of **more than 41 million consumers.**

HEALTHCARE

Anthem Blue Cross

A successful cyber attack stole the patient records of **78.8 million people**, including names, social security numbers, home addresses, and dates of birth.

CREDIT RISK ASSESSMENT

Equifax

The high-profile Equifax breach was caused by a missed patch on an open source application, **even though there were 172 security professionals** on staff at the time.

Yet when you consider the consequences of non-compliance – fines, bad press, a tarnished reputation, financial damage, and the loss of customers – one thing is clear: failure is not an option.

Moody's

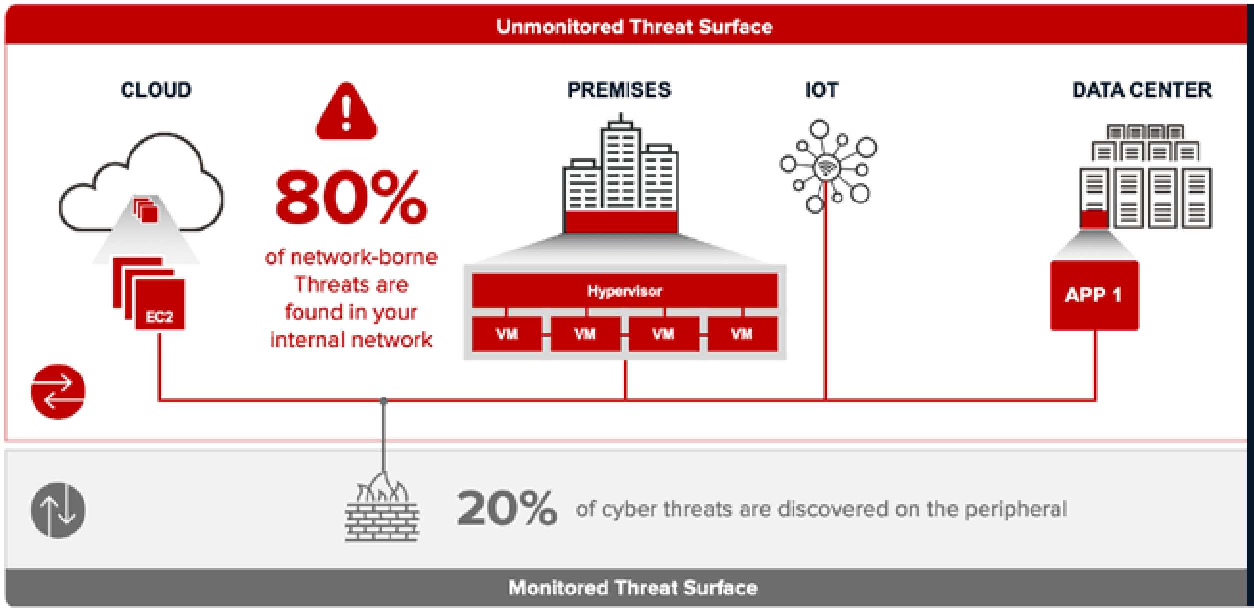
In response to the Equifax breach, Moody's downgraded the company's rating from stable to negative. More companies will be affected as Moody's now includes cyber-risk in its credit ratings.

Security teams lack complete visibility into all their network traffic

Most of the worst data data breaches resulted from missed network-borne threats that spread laterally through internal networks, including those located on-premises, private data center and public cloud. Unfortunately, these missed threats led to extensive amounts of exfiltrated data over long periods of time.

Why is this still happening? For the simple reason that traditional security tools don't provide the full visibility needed to detect and stop network-borne threats. Firewalls and other solutions tend to focus on north-south traffic only, which means that they miss 80% of all traffic – a significant threat surface.

Solutions that can help visualize, monitor, and classify all network flows, including east-west traffic, provide the visibility needed to detect and stop threats that would normally be missed faster and more effectively.


Unmonitored Threat Surface
CLOUD
EC2
80%
of network-borne Threats are found in your internal network
PREMISES
Hypervisor
VM
VM
VM
VM
IOT
DATA CENTER
APP 1
20%
of cyber threats are discovered on the peripheral
Monitored Threat Surface

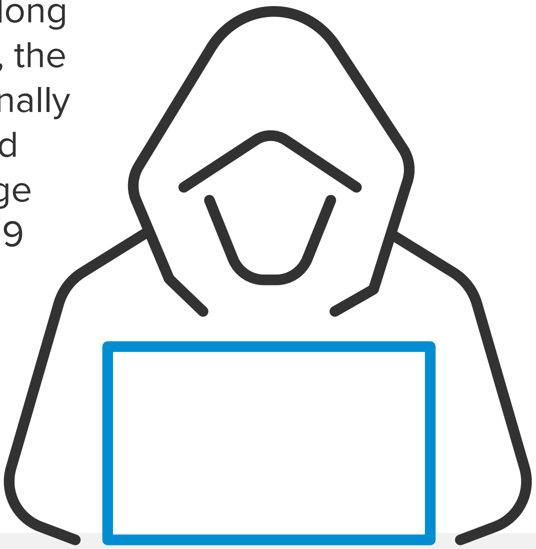
90% of the security budget is spent on perimeter measures, yet only 20% of the threats are found this way.

The other 80% of threats appear on the internal network, but are often missed or typically found too late due to significant gaps in detection and investigative response processes.

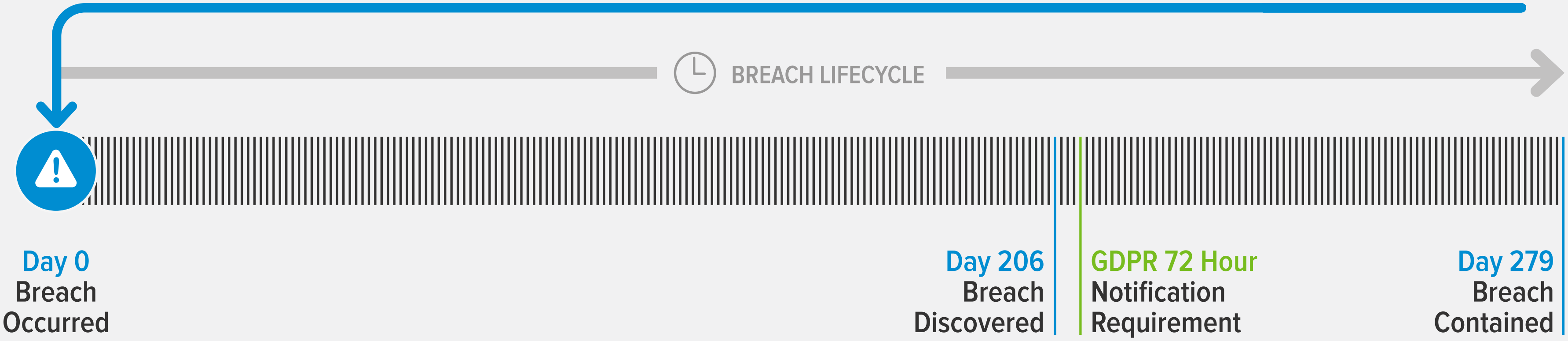
Forrester and ZK Research

Finding hackers takes too long — leading to excessive data exfiltration and additional compliance issues

Sadly the data shows that hackers are able to lurk in a network for a surprisingly long time before they are detected. According to the 2019 Ponemon Research Report, the time between when a data breach incident occurred and when the breach was finally contained (also known as the breach lifecycle) grew noticeably between 2018 and 2019. The average time to identify a breach in 2019 was 206 days and the average time to contain a breach was 73 days, for a total of 279 days. This represents a 4.9 percent increase over the 2018 breach lifecycle of 266 days.



When you factor in that GDPR demands notification within 72 hours of discovery with definitive details on origin, exact records impacted and remediation plans 73 days to containment falls short.



The rise of data privacy regulations

New data privacy regulations are being developed at the state, national, and international level to combat the fact that breaches really can't be stopped – and the perception that companies aren't doing all they can to protect consumers' PII/ePHI data.

Many companies already struggle with how to truly secure their infrastructure and safeguard data. But now, they must also navigate a complex, confusing landscape of data privacy regulations.

Worse, each one may have its own requirements, many of which could conflict with other regulations. For example, the U.S. currently has a patchwork system of state laws and regulations that can dovetail, overlap, or even contradict one another.

In addition, there are many guidelines, developed by international and government agencies and industry groups, that do not have the force of law. However, they are part of self-regulatory guidelines and frameworks that are considered best practices and are increasingly being used as an enforcement tool by regulators.

The federal government makes data security mandatory for future work

Department of Defense (DoD) created the Cybersecurity Maturity Model Certification (CMMC) as a means to protect controlled unclassified information (CUI) within the entirety of the defense industrial base (DIB) of vendors.

The CMMC framework is a mix of practices, processes, and approaches that are intended to standardize the assessment of a DIB vendors' cybersecurity capabilities.

CUI is defined as any information the government creates or possesses, or that another entity creates or possesses on its behalf. This can include things such as infrastructure, export controls, or financial, intelligence, legal, or other information and data.

Clear demonstration of CMMC compliance will be mandatory for any newly awarded contracts to any DIB vendor, including primary vendors as well as subcontractors (this means any organization that handles CUI that on behalf of the primary vendor including infrastructure, export controls, or financial, intelligence, legal, or other information and data).

aria

CMMC 3.0 Compliance Checklist

How DIB Vendors Can Achieve Compliance with ARIA ADR

DOWNLOAD OUR CMMC CHECKLIST

International regulations and GDPR

The EU's General Data Protection Regulation (GDPR) now gives EU citizens more control over their personal data. In addition to stiff fines, a critical component of GDPR is that EU citizens can bring civil suits against companies to hold them accountable for lost data.

Under GDPR, not only do any organization that collects personal data on EU citizens have to ensure it is gathered legally and under proper conditions, but they are obligated to protect it from misuse and exploitation, as well as to respect the rights of data owners – or face steep penalties.

GDPR applies to any organization operating within the EU, as well as any organizations outside of the EU that offer goods or services to customers or businesses in the EU. That ultimately means that every corporation in the world is impacted by GDPR.

One thing is clear: there will be more international regulations. Many view GDPR as the first regulation to fall in a global domino effect, where companies are watching to see how GDPR expands outside of the EU – and how similar regulations could affect them.

British Airways is the latest to feel the financial impact of GDPR: a **$230 million fine** in response to the company's 2018 data breach.

GDPR requires breach notification within 72 hours, including the exact records affected

Failure to comply with GDPR can lead to fines of 4% in revenue or €20M (whichever is higher)

State laws add to the confusion

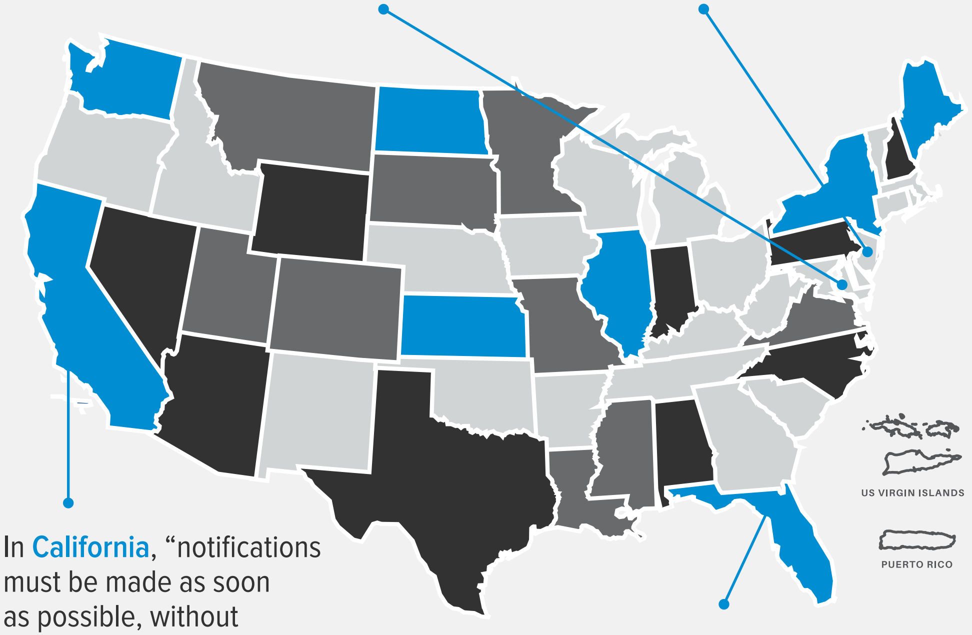
All 50 states as well as the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have passed laws that require individuals to be notified if their information is compromised.

The challenge is that these laws have different and sometimes incompatible provisions regarding what categories and types of personal information warrant protection, which entities are covered, and even what constitutes a breach.

Notification requirements also vary: New Jersey requires that the state police cybercrime unit be notified, while Maryland requires that the state attorney general be notified before any affected individual is. Florida has a 30-day notification requirement, while California stipulates that "notifications must be made as soon as possible, without unreasonable delay."

Maryland requires the "state attorney is notified before the individual"

New Jersey requires that "state police are notified"



In California, "notifications must be made as soon as possible, without unreasonable delay"

Florida has a "30-day notification requirement"

Different Laws Complicate Compliance Efforts

When it comes to reporting a breach, each state has its own requirements, creating additional complexity and confusion related to compliance. (Note: These compliance requirements are just a select few. Each state has its own law.)

The final straw: industry regulations impose further restrictions

Companies in highly-regulated industries, such as healthcare or financial, must also comply with still more regulations. These industry-specific laws are intended to give consumers extra protection over their PII/ePHI data.

The following are just a sample of today's industry regulations:

The Healthcare Insurance Portability and Accountability Act (HIPAA)

HIPAA provides data privacy and security provisions for safeguarding medical information.

Fines for non-compliance can be severe: MD Anderson Cancer Center was forced to pay a **$4.3M penalty** for three data breach violations.

The Payment Card Industry Data Security Standard (PCI DSS)

This is a set of 12 regulations designed to reduce fraud and protect customer credit card information.

Failure to comply can lead to fines ranging from **$5,000 to $100,000 per month.**

23 NYCRR 500

This New York law requires supervised financial services and insurance companies to assess their cybersecurity risk profiles and implement a comprehensive plan that recognizes and mitigates that risk.

It's serious business: Fines start at $2,500 per day for a violation but go as high as **$75,000 per day** in the event of a knowing and willful violation.

Traditional security solutions can't solve the problem

Leading security tools utilized for threat hunting and breach prevention – including SIEMs, SOARs, IDS/IPS – are not fully effective in helping organizations achieve compliance. They fall short for a number of reasons:

Too much noise

InfoSec professionals receive over **5,000 intrusion alerts per day** from their installed security tools, making it impossible to investigate all of these incidents.

Netborne-threats are missed

Firewalls, SIEMs, EDR solutions, and other security tools **mainly focus on north-south traffic monitoring and perimeter protection**. Yet this can only provide threat detection for what these tools can see and only on devices on which they can be deployed.

Large attack surface

Today's organizations have IT infrastructures that are highly complex, dynamic, and scalable. They're composed of networks, assets, data, and IoT devices, **spanning and residing in a mix of on-premise servers, remote data centers, public clouds, and hybrid environments.**

Two complex challenges to meeting compliance:

1 Security tool ineffectiveness

2 IoT vulnerabilities

Let's take a closer look at these two issues...

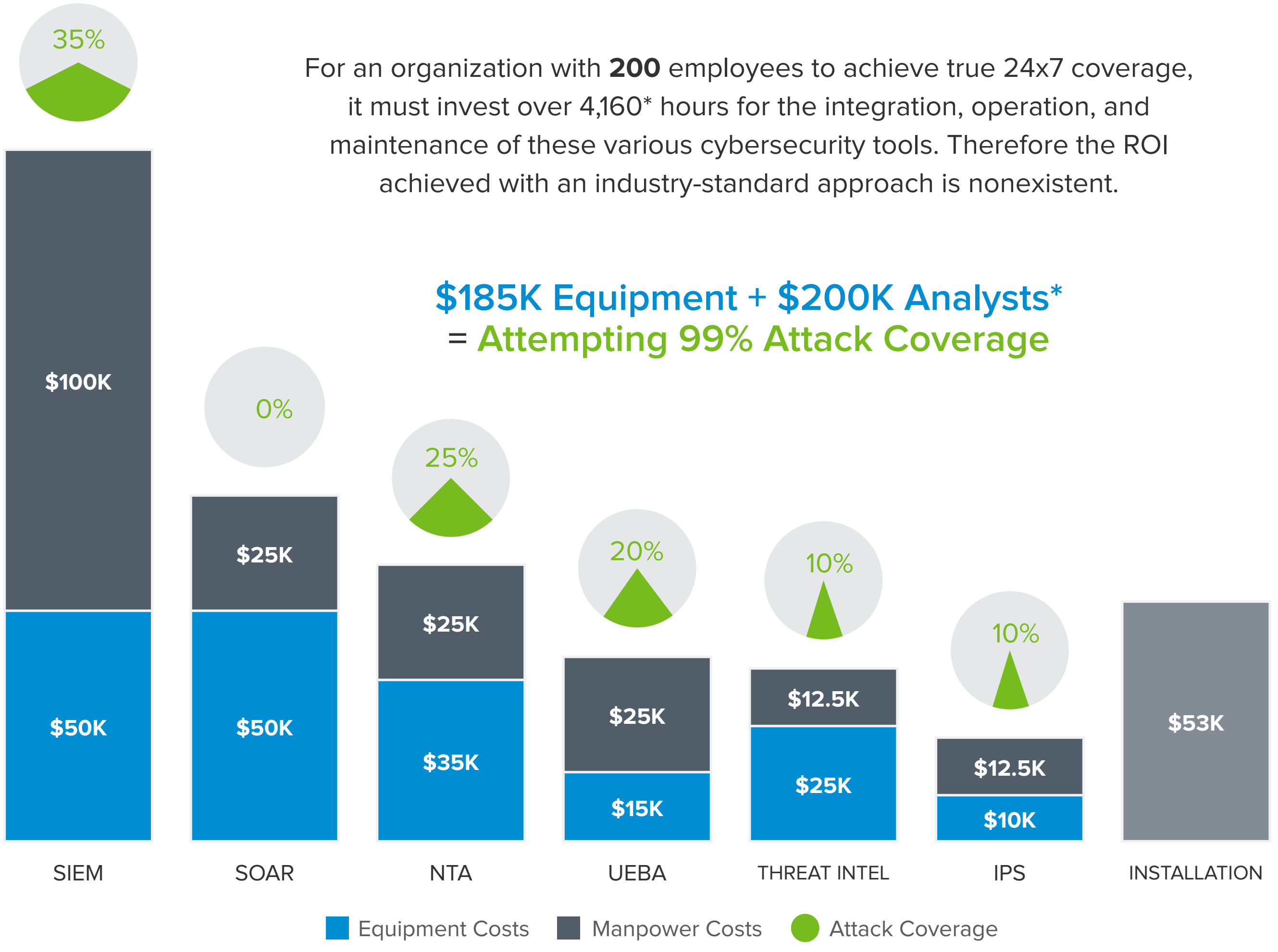
The Security tool ineffectiveness dilemma

A typical organization has deployed many different security tools in their efforts to protect vital data.

Yet, these tools present real challenges ranging from unactionable information, reliance on highly-trained analysts, high costs, and limited threat surface coverage.

For an organization with **200** employees to achieve true 24x7 coverage, it must invest over 4,160* hours for the integration, operation, and maintenance of these various cybersecurity tools. Therefore the ROI achieved with an industry-standard approach is nonexistent.

$185K Equipment + $200K Analysts*
= Attempting 99% Attack Coverage



aria

Companies need a security solution that can complement and enhance existing security tools such as firewalls, SIEMs, IDS/IPS tools, SOARs, and more — all to reduce costs and make them even more effective.

* Manhour calculations based upon a 2080 work week and an average hourly costs of a cybersecurity professional is $48.

IoT devices are vulnerable to attacks, resulting in an expanded threat surface

Today, the Internet of Things (IoT) trend is exploding and continuing to deliver many important benefits related to operation efficiencies and end-user conveniences.

Yet IoT devices also present a very real security risk, a challenge that doesn't have an easy answer. Traditional security tools, such as endpoint detection and response (EDR) applications, generally can't be deployed on IoT devices since they lack processing power or are completely closed by the vendor.

Additionally, legacy applications simply can't accept EDR solutions, for the same reasons described earlier. Without a way to secure these devices, many companies are exposed to a larger threat attack surface – and more risk than they even know.

To combat this vulnerability, modern security tools should be able to monitor all IoT devices on a network and surgically stop threat conversations – while still keeping unaffected production applications and IoT devices up and running.

INDUSTRY SNAPSHOT: INTERNET OF MEDICAL THINGS (IoMT) DEVICES

CONSUMER PRODUCTS FOR HEALTH MONITORING

These devices – such as FitBit, Nike Fuelband, or Withings – generally communicate using Bluetooth to nearby personal mobile devices.

WEARABLE, EXTERNAL MEDICAL DEVICES

This category includes portable insulin pumps, which often use propriety wireless protocols to communicate.

INTERNALLY EMBEDDED MEDICAL DEVICES

Pacemakers and other medical devices are implanted in the patient but communicate wirelessly, either with propriety wireless protocols or Bluetooth.

STATIONARY MEDICAL DEVICES

Devices such as hospital-based chemotherapy dispensers or home-care cardio-monitoring for bedridden patients, often use basic wireless networks, such as WiFi in hospitals or patients' homes.

ARIA Cybersecurity solutions help meet compliance regulations

Many breaches start as missed threats residing inside a corporate network. This means effective security – and data privacy compliance – requires full visibility into your network traffic. Yet adding another specialized security solution to existing infrastructure is not the answer.

It is critical that any potential threats are detected and verified as quickly as possible. Yet this is hard to achieve, especially with the east-west communication paths used by public cloud, data center, and on-premise data and application stores.

Instead, the ARIA Cybersecurity suite of solutions has been designed to work seamlessly with SIEMs, SOARs, IDS/IPS tools, firewalls, and other security systems to orchestrate the security and protection of high-value assets across the entire enterprise.

By accelerating incident response and threat containment efforts, our solutions give you a critical edge in complying with even the most stringent industry regulations.

Four Significant Benefits of ARIA ADR

1 - Enables clientless threat detection

This includes for IoT devices as well as legacy systems transparently from within the network.

2 - Stops threats

ARIA ADR with ARIA PI can stop the attacks once detected automatically – by stopping the threat conversation without impacting normal device operation.

3 - Improves performance of existing tools

Boosts modern SIEMs, SOARs and other tools by enhancing such processing with new rules and playbooks designed to protect IoT.

4 - Applies and enforces microsegmentation

ARIA PI with ARIA ADR prevents rogue IoT devices from attempting to communicate with any devices or applications that they should not.

ARIA solutions: automated breach detection, response, containment and remediation

ARIA ADR is a cybersecurity platform of an orchestrator and security applications that are designed to properly secure your network and compute environment, enterprise-wide. It is easily deployed in east-west traffic paths to inspect, record, and segment all network communications.

It speeds-up detection, response, and containment, and provides new compliance capabilities, including:

- **Know if any PII/ePHi records were accessed, and if so, which specific records were impacted.**
- **Encrypt all PII/ePHI data, no matter where it is stored, used, or accessed.**
- **Provide auditable reporting on any breach – what happened, when did it start, what files were accessed, and who was involved.**

aria ADR

Six security tools in one for total coverage at a fraction of the cost

ARIA Advanced Detection and Response (ADR) is an AI-driven SOC in a box that provides the capabilities of six cybersecurity tools into one. With ARIA ADR, you will automate the detection, verification, and remediation of cyber-attacks, while eliminating the labor-intensive intervention required by expensive security experts and SOAR tools. This unique approach makes the ARIA ADR solution extremely cost-effective to purchase and operate and the best way to quickly find and stop all major attack types.

aria PACKET INTELLIGENCE

Complete network visibility, accelerated incident response, and better threat containment

The ARIA SDS Packet Intelligence (PI) application provides complete visibility into internal network traffic, including east-west network data flows. The application creates analytics for every packet that are ingested by packet delivery accounting tools, quality of service SLA monitoring applications, or as security analytics by SIEMs. This enables better, more comprehensive threat detection, faster investigative responses, and immediate threat containment.

Better cybersecurity – and regulatory compliance – starts now

- **Provide** complete visibility into the internal network, including east-west traffic.
- **Improve** detection and accelerate the investigation of network-borne threats.
- **Gain** security and reporting tools to maintain compliance with even the most challenging state, federal, and international regulations.
- **Contain** threats surgically without taking important devices offline.

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

aria CYBERSECURITY SOLUTIONS   ariaSDS   nVoy SECURITY APPLIANCES   Myricom NETWORK ADAPTERS