ARMOR INCIDENT RESPONSE AND FORENSICS (IRF)

FOR ON-PREMISE AND MULTI-CLOUD ENVIRONMENTS

As your business grows, your security and compliance protections need to grow with it. But defending on-premise infrastructure isn't enough. Your organization's IT security team needs to be able to see, defend, and respond to threats no matter where its infrastructure resides—and do it at a speed that outpaces not just today's attackers but tomorrow's as well. Digital transformation means embracing the cloud and, once you are there, protecting it with technology and expertise that identifies threats and handles incident response (IR) in public, private, or hybrid clouds—or on-premise IT environments.

ARMOR'S PROACTIVE APPROACH TO INCIDENT RESPONSE

- Hardened CIS server builds
- Aggressive patching program
- On-access scans for antimalware tools
- Edge-based traffic shaping
- Zero-trust model for server positioning
- Integrated threat intelligence
- Advanced analytics and correlations
- Orchestration and automation
- Continuous threat hunting

DETECT, HUNT, AND RESPOND TO CYBERATTACKS

Armor IR services provide a turnkey solution that delivers advanced threat detection, monitoring, security analytics, and continuous response and recovery for threats that have bypassed traditional preventative controls. By rapidly delivering these capabilities, Armor is providing the next generation of IR to your organization—all without breaking the bank.

ARMOR DELIVERS THE INDUSTRY'S LEADING DWELL TIME WITH MANAGED DETECTION AND RESPONSE

RESPONSE THAT ENABLES PROACTIVE INVESTIGATIVE WORKFLOWS

Armor services provide continuous response and remediation to contain affected systems as well as automate and accelerate response to reduce dwell time, disable threat actors, and reduce risk.

AUDIT-READY COMPLIANCE

With security controls mapped to compliance mandates such as PCI DSS, HIPAA/ HITRUST, and GDPR, Armor can provide security and compliance benefits to reduce regulatory scope, simplifying the auditing process and lowering management costs.

RANSOMWARE ADVANCED ANALYSIS AND CORRELATION

Events are analyzed and correlated with event data from your other devices under our threat prevention and response platform's management, delivering enhanced detection of potential threats across your public, private, or hybrid cloud—or on-premise IT environments.

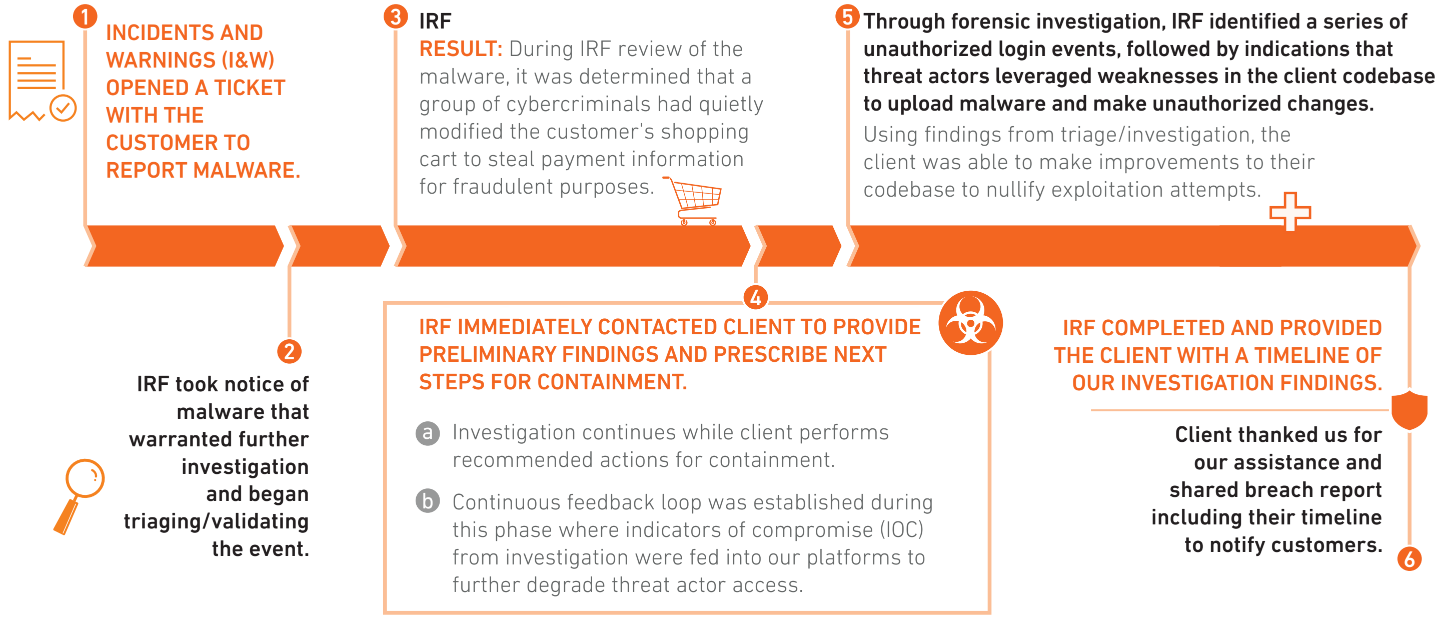
FORENSICS AND INVESTIGATION PROVIDES ANSWERS, NOT ALERTS

Intelligence-driven investigations enable a complete understanding of the scope of the attack, information to help assess risk, and definitive remediation recommendations. This also reduces the dependency on boots-on-the-ground.

To learn more about these recommendations, download the full eBook: **"5 Days to Actions and Objective—Dwell Time as a Critical Security Success Metric."**

ON-DEMAND ACCESS TO CRITICAL EXPERTISE

Bolstering Armor's industry-leading technology is our security operations center (SOC), a force multiplier staffed with experts who tirelessly monitor and protect your critical data workloads and applications across on-premise and cloud infrastructures. Inside the SOC is our acclaimed Threat Resistance Unit (TRU). TRU's mission is to stay one step ahead of threat actors and provide advanced notice and intelligence on emerging threats—all while empowering our SOC with applied intelligence, countermeasure development, forensics, and incident investigation to strengthen its ability to see and respond to even the most sophisticated threats. When you partner with Armor, our security experts extend your security program through 24/7/365 monitoring and protection.



1 INCIDENTS AND WARNINGS (I&W) OPENED A TICKET WITH THE CUSTOMER TO REPORT MALWARE.

2 IRF took notice of malware that warranted further investigation and began triaging/validating the event.

3 IRF
RESULT: During IRF review of the malware, it was determined that a group of cybercriminals had quietly modified the customer's shopping cart to steal payment information for fraudulent purposes.

4 IRF IMMEDIATELY CONTACTED CLIENT TO PROVIDE PRELIMINARY FINDINGS AND PRESCRIBE NEXT STEPS FOR CONTAINMENT.

a Investigation continues while client performs recommended actions for containment.

b Continuous feedback loop was established during this phase where indicators of compromise (IOC) from investigation were fed into our platforms to further degrade threat actor access.

5 **Through forensic investigation, IRF identified a series of unauthorized login events, followed by indications that threat actors leveraged weaknesses in the client codebase to upload malware and make unauthorized changes.**
Using findings from triage/investigation, the client was able to make improvements to their codebase to nullify exploitation attempts.

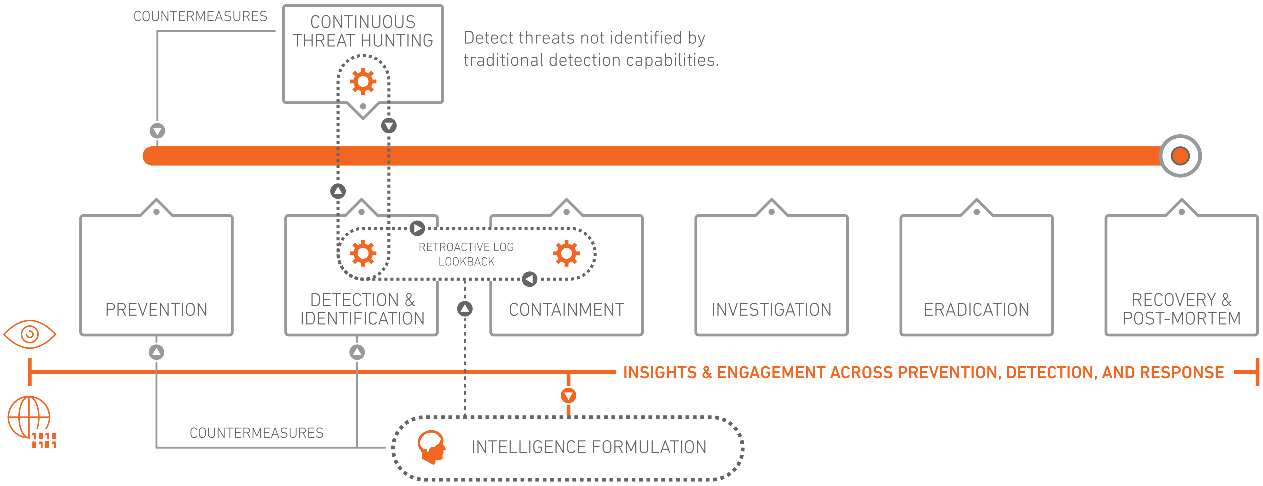
IRF COMPLETED AND PROVIDED THE CLIENT WITH A TIMELINE OF OUR INVESTIGATION FINDINGS.

Client thanked us for our assistance and shared breach report including their timeline to notify customers. 6

SECURITY PROGRAM DESIGNED WITH DWELL TIME AS AN OPERATING PHILOSOPHY

The IRF service provides for investigation with response and remediation options for reported events from the Armor security services. The service consists of four components: event identification; validation and initial triage with client notification; customer consultation; and in-depth forensic investigation, reporting, and supporting remediation efforts. The first three services are included by default, as part of your Armor service, and are limited to a maximum of two hours. Based on the results from the consultation, additional services are available to you and require the purchase of IR time blocks.

HOW DOES IT WORK?


COUNTERMEASURES
CONTINUOUS THREAT HUNTING
Detect threats not identified by traditional detection capabilities.
PREVENTION
DETECTION & IDENTIFICATION
RETROACTIVE LOG LOOKBACK
CONTAINMENT
INVESTIGATION
ERADICATION
RECOVERY & POST-MORTEM
INSIGHTS & ENGAGEMENT ACROSS PREVENTION, DETECTION, AND RESPONSE
COUNTERMEASURES
INTELLIGENCE FORMULATION

EVENT IDENTIFICATION

Armor's platform ingests and correlates data from all Armor-provided security tools, as well as other optional log sources, and generates event notifications for potential indicators of compromise (IOCs). These events are sent to our SOC for validation follow-up. You may also self-report potential security events.

VALIDATION AND INITIAL TRIAGE WITH CLIENT NOTIFICATION

The Armor SOC opens a ticket with your team and investigates each identified event. This may include access to the affected servers to review additional data. Once this has been completed, the SOC provides information on the type, nature, and severity of the event, and it may include recommendations for remediation.

ADVANCED INVESTIGATION, REMEDIATION, AND FORENSICS

Armor security operations engineers will execute the agreed upon actions and record their findings in the ticketing system. Any additional direction, references, or referrals will be made to conclude the process.

ADDITIONAL INCIDENT RESPONSE AND FORENSICS HOURS

You may purchase additional IRF time blocks to address the help you may require from Armor to investigate and provide remediation assistance with security events. These time blocks are purchased in advance and expire 12 months from the date of purchase.

Our IRF service enhances our Armor SECaaS solutions to provide total security protection across your entire IT environment.

Learn more

Armor Anywhere

Armor Complete

CLIENT CONSULTATION

During the consultation, SOC personnel will discuss the event, gather additional information about your environment, and prescribe additional actions. Upon completion, Armor and your team will agree upon any more actions to be taken by the Armor SOC to further investigate, report, and support remediation efforts surrounding the event.

ADDITIONAL INCIDENT RESPONSE & FORENSICS SERVICES

In the event your organization does not use all its purchased IRF time blocks within the 12-month period, you may opt to use the remaining time on any of the following IRF services.

- **Security Awareness Training**
  Armor will remotely deliver a security awareness training session that can be used to fulfill compliance requirements. The standardized training session will last approximately 2 hours.
- **Advanced Security Reporting**
  Reports can be of technical, management, or executive level, and the details will be discussed and agreed upon during a consultation call.
- **Industry Threat Report**
  Reports cover the current state of your industry, existing and expected trends, and any threats.
- **Incident Response & Management Tabletop**
  Armor will conduct an IR tabletop exercise, including tickets and real-time responses, that mimics and tests our IR capabilities and interactions with our IR services. The exercise will begin with an Armor initiated response and include escalation beyond our standard response and company runbooks.

INCIDENT RESPONSE & FORENSICS ACROSS ANY ENVIRONMENT

IRF service is available for all Armor customers. The service runs and is fully supported on AWS, Azure, Google Cloud Platform, and Rackspace for Armor Anywhere customers. IRF is supported on all 5 Armor Complete datacenters (Amsterdam, Dallas, London, Phoenix, and Singapore). It is also available for partners, on-premise environments, and other datacenters if you are running the Armor agent on a supported operating system (OS).

OPTIMIZED FOR

aws

Microsoft Azure

Google Cloud

vmware

PRIVATE CLOUD

HYBRID CLOUD

OTHER CLOUD

ON-PREMISE INFRASTRUCTURE