Cybersecurity

Ransomware Mitigation Kit
Reduce Your Risks from Ransomware

THE CHALLENGE

Organizations are challenged with increased regulatory compliance, cybersecurity best practice compliance, along with cyber insurance demands and rising costs. In Q4 of 2021 the average downtime associated with a ransomware attack was 22 days, while ransom costs continue to grow. Whether the enterprise infrastructure is on-premise, in the cloud, or in a hybrid environment, the ramifications of a ransomware attack can be enormous, from data loss to financial loss and worse, reputation and trust.

THE SOLUTION

This multi-faceted approach orchestrates powerful protections to help rapidly secure the environment. The Ransomware Mitigation Kit synchronizes industry leading products and services to detect, prevent, isolate, and recover the IT environment, saving both time and additional cost.
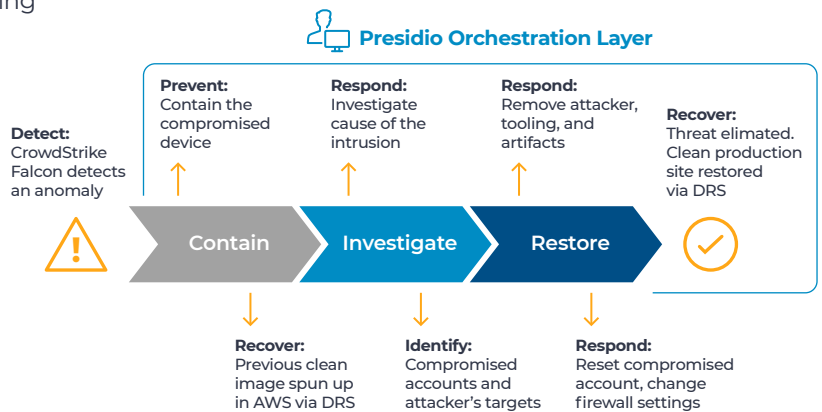
OFFERINGS OVERVIEW

An industry first, the collaboration of these vendors offers organizations a quick-start to implementing a powerful set of ransomware protection technologies. By implementing the Ransomware Mitigation Kit customers can gain comprehensive visibility, breach protection, and recovery across all their digital assets to:

- ◆ Quickly detect and prevent attacks
- ◆ Swiftly respond and mitigate attacks
- ◆ Be positioned to recover to a clean version of your infrastructure in minutes, increasing business resiliency and operational efficiencies

STRUCTURED IMPLEMENTATION

- ◆ **The Presidio Ransomware Workshop:** The Workshop provides actionable insights into security misconfigurations and deviations from NIST-CSF recommended cloud, hybrid and on-prem security architectures to help clients prevent, detect, and recover from breaches.

- ◆ **CrowdStrike:** A powerful endpoint protection platform powered by a cloud-scale AI, with unified next-generation antivirus, endpoint detection and response (EDR), IT hygiene, and a 24/7 managed hunting service – all delivered via a single lightweight agent with minimal performance impact.

- ◆ **The AWS Elastic Disaster Recovery Services (AWS DRS):** AWS' Disaster Recovery Services continuously replicate machines into a low-cost staging area in the target AWS account and preferred region.

- ◆ **Presidio Layered Orchestration:** Orchestration takes data from CrowdStrike in the event of a breach, automatically identifies clean AWS DRS checkpoints, and allows the administrator to use "one-click" to continue operations, while remediation is taking place on the infected machines. This multi-faceted approach orchestrates powerful protections to help rapidly secure the environment. The Ransomware Mitigation Kit synchronizes industry leading products and services to detect, prevent, isolate, and recover the IT environment, saving both time and additional cost.

Presidio Orchestration Layer

Detect: CrowdStrike Falcon detects an anomaly

Prevent: Contain the compromised device

Respond: Investigate cause of the intrusion

Respond: Remove attacker, tooling, and artifacts

Recover: Threat elimated. Clean production site restored via DRS

Contain → Investigate → Restore → ✓

Recover: Previous clean image spun up in AWS via DRS

Identify: Compromised accounts and attacker's targets

Respond: Reset compromised account, change firewall settings

Ransomware Mitigation Kit: Reduce Your Risks from Ransomware

KEY BENEFITS

Ransomware Mitigation Kit quick-start engagements deliver the necessary training, tools, and assistance to help accelerate protections. The solution supports prediction and prevention of modern threats through the industry's most comprehensive set of endpoint and cloud workload telemetry, threat intelligence, and AI-powered analytics. With this offering, a strong security posture is established, business continuity is enabled, and cyber-resilience is solidified.

- Prevent ransomware
- Provide a rapid recovery should a ransomware incident occur
- Reduce recovery time objectives (RTO)
- Support recovery point objectives (RPO)
- Gain comprehensive visibility, discovery, mitigation, and recovery for on-prem, hybrid or cloud deployments
- Isolate compromised systems and recovery of operations to a cost-effective instance in the cloud with minimal impact
- Simplify implementation
- Gain operational efficiency improvements
- Close the skills gap for hard-to-find cloud security resources

WHAT MAKES US DIFFERENT

The Ransomware Mitigation Kit is the first structured multi-vendor industry solution with proven top tier providers. The solution offers powerful orchestration between the Endpoint Protection & Response (EDR) and the backup solutions to drive rapid response with automated playbooks. Clients can be confident that their solutions will work together with a single touchpoint for support. Regardless of where the concern lies, our support team will coordinate with all parties for a seamless deployment.

WHY PRESIDIO

Presidio is a global digital services and solutions provider accelerating business transformation through secured technology modernization. The Presidio team provides deep experience in secure networking, cloud computing and broad hybrid infrastructures. Presidio recognizes that cybersecurity is foundational to the success of any business and has a highly specialized expert team at the ready.

- Services methodology built on recognized industry standards including NIST, CIS, and ISO
- Compliance depth & breadth including PCI, HIPAA, NERC CIP, GDPR, CCPA, SOC 2, ISO 27001, DFARS 800-171, CMMC
- Deep security services bench and broad security services solutions provide domain expertise and consistent deliverables
- Thought leadership across technologies
- Experience in architecting, implementing, securing, and managing any digital transformation needs
- Multi-discipline experts provide for a broad view of client's potential vulnerabilities
- Close integration between design, delivery, and customer experience teams results in professionally implemented solutions for your unique needs

Presidio Cybersecurity Practice covers a broad security services portfolio. Our highly skilled and tenured cybersecurity practitioners maintain leading industry certifications, provide thought leadership and practical industry experience. We have conducted thousands of engagements across all major industry segments. Getting started with Presidio is easy. Let's explore how we can secure your business.

INFORMATION SECURITY

TECHNICAL ASSESSMENT

INFRASTRUCTURE SECURITY

VENDORS AND STANDARDS

For further information, contact:
ransomwaremitigationkit@presidio.com