PRESIDIO®

SOLUTIONS BRIEF

Cybersecurity

Presidio MDR

Managed Detection & Response

KEY CHALLENGES IN CYBERSECURITY

Ransomware and breaches are top of mind for organizations globally. The proliferation of security applications, alarms, and alerts can overwhelm a security team, delaying an effective response and putting their business at risk. The challenge of protecting the business 24x7x365 can overwhelm many organizations.

- **Alert Prioritization** – the volume of alerts is growing exponentially with each system, and the constant expansion of the threat landscape makes it very difficult for analysts to find, prioritize, and remediate threats
- **Threat Intelligence** – keeping current with threats is a significant challenge, while recognizing that speed in response is paramount to protecting critical infrastructure and data
- **Coverage** – managing services, monitored and operated every minute of every day to support the highest levels of security, and effectively responding to incidents can be daunting
- **Lack of Skilled Personnel** – retaining skilled cyber resources is further exacerbated with staying on top of the exponential threat landscape across dozens of technology innovations

A NOTE ON CYBER INSURANCE

Business continuity and cybersecurity insurance costs are major concerns, with cybersecurity being the top insurance claim category in 2020. Implementing protections is paramount and often, cyber insurance carriers are establishing Managed Detection and Response (MDR) as a minimum requirement. Without it, clients are finding themselves uninsurable after their first ransomware claim.

THE SOLUTION

Presidio MDR defends against credential thefts, malware outbreaks, security breaches, data exfiltration, and other potential security incidents such as ransomware. Presidio MDR integrates with traditional enterprise and cloud platforms to consolidate security event data and decisions through an intuitive platform.

Presidio MDR helps clients move from a reactive position to a proactively defensive security posture and includes the following core platform and key expert resources:

- SIEM and/or EDR Technology
- SecOps Portal
- Threat Engine
- Premium Threat Intelligence Feeds
- Tactical Security Reviews
- Threat Strike Team

Full-Service Protection

Presidio MDR is a fully managed service providing the technology, strategy, and processes to improve a client's security posture.

Security Expertise

Presidio Security Expertise constantly evolves for today's threat landscape leveraging Presidio cybersecurity governance & offensive security expertise

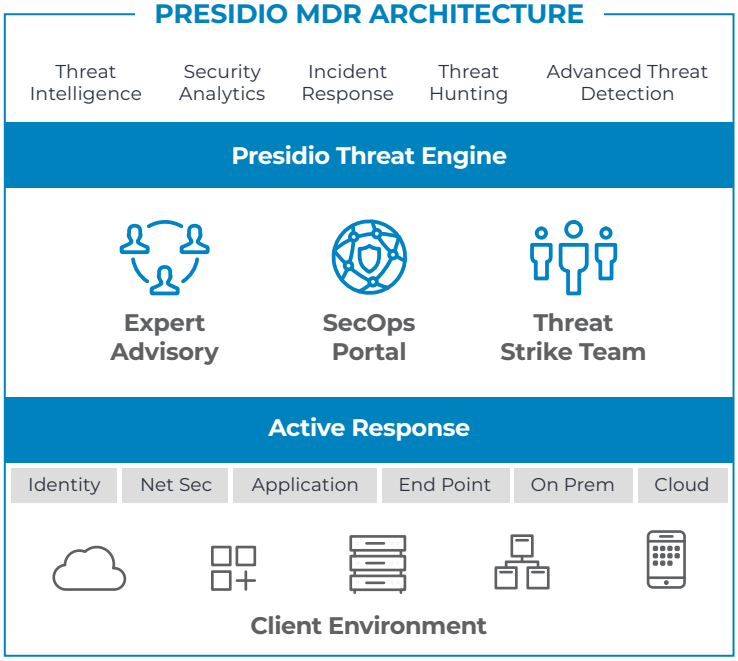
Effective & Efficient

Decrease Mean Time to Detect and Respond to potential security incidents to reduce risk and business impact

Visibility & Insight

Clients benefit from security insights, crowdsourced threat data, and experience across the entire Presidio security portfolio 24x7x365 with actionable alerts and real-time dashboards

Presidio MDR



Presidio MDR delivers a new standard of effective threat detection and response, leveraging security event data from traditional enterprise as well as cloud platforms. Presidio MDR efficiently renders meaningful and accurate verdicts in the face of today's threat landscape, providing data enriched alerts through an intuitive dashboard and offering an optional Active Response capability to automatically take protective action in minutes, rather than hours or days.

Presidio MDR is centered on four core features:

Research and Threat Intelligence
The Presidio MDR Threat Framework aligns with multiple security industry frameworks to ensure the right coverage for end-to-end threat mitigation across the entire infrastructure. A team of experienced security analysts leverages information from a host of resources, including premium threat intelligence feeds and crowdsourced intel from across the global Presidio portfolio.

Threat Detection
Presidio MDR Threat Detection combines threat hunting with high-fidelity use cases known as the Presidio Threat Framework. The proprietary Threat Framework use cases are developed around the MITRE ATT&CK and Lockheed Martin Kill Chain frameworks and are designed to identify specific real-world attacks in client environments.

Visibility and Control
Presidio MDR goes beyond simply opening tickets for a client's cyber team to investigate and resolve. Presidio MDR offers actionable security insights and context-rich notifications through a real-time dashboard that enables clients to confidently take appropriate remediation actions.

The Presidio Threat Engine passes only high-fidelity alerts that, when integrated with Active Response, reduce a client's response time from hours to minutes.
The intuitive dashboard supports the ability to:

- Disable accounts
- Add/remove indicators from exclusion lists
- Quarantine endpoints
- Isolate workloads

One Team
The Presidio Threat Strike Team provides 24x7x365 coverage, tailored alerting, and customized strategic guidance. Each client receives a named Client Success Manager (CSM) and named Primary and Secondary Analysts who provide primary points of contact and become intimately familiar with each client's environment, priorities, and security posture.

The named CSM and analysts are backed by a team of experienced security professionals working closely together 24x7x365 to identify and manage threats.

Presidio MDR

PRESIDIO CYBERSECURITY FLEX SERVICES

Presidio recognizes that simply implementing a technology solution may leave operational or compliance gaps. With the goal of protecting the business, Presidio MDR offers powerful cybersecurity services to fit each client's current threat or compliance concerns. Some services may be used annually, while many clients in high profile industries will repeat strategic services on a quarterly or bi-annual basis. Presidio works with clients to map out individualized service plans to achieve business, risk, and compliance outcomes.

Presidio offers a suite of professional cybersecurity services with Presidio MDR.

- Assessment Services define critical gaps and remediation
- Policy and Compliance Services support a strong, well-documented cybersecurity posture
- Testing Services provide data-driven results
- Incident Response Services support preparedness goals

Assessment Services

- External Vulnerability
- Internal Vulnerability
- Infrastructure Hardening
- Operating System Hardening

Policy & Compliance

- Security Policy Development

Testing Services

- External Penetration Test
- Internal Penetration Test
- Web Application Penetration Test
- Remote Wireless Penetration Test

Incident Response

- Incident Response Tabletop Exercise
- Incident Response Retainer

External Vulnerability Assessment: Scan Internet-facing information assets and services to uncover vulnerabilities and their associated risk levels

Internal Vulnerability Assessment: Scan internal networks to uncover vulnerabilities that present risk to the security of information assets and services

Infrastructure Hardening Assessment: Evaluate infrastructure devices for secure configuration practices and provide prioritized guidance for remediation

Operating System Hardening Assessment: Evaluate workstation and server devices for secure configuration practices and provide prioritized guidance for remediation

Security Policy Development: Collaborate with key stakeholders to understand the organization's culture, business needs, and security requirements to ensure information security policies and standards are enforceable and address the entire landscape

External Penetration Test: Test the external implementation of security controls to exploit vulnerabilities and demonstrate what a malicious actor could gain unauthorized access to

Internal Penetration Test: Test the internal implementation of security controls to demonstrate how an internal threat could gain unauthorized access to critical assets, sensitive data, and establish a foothold

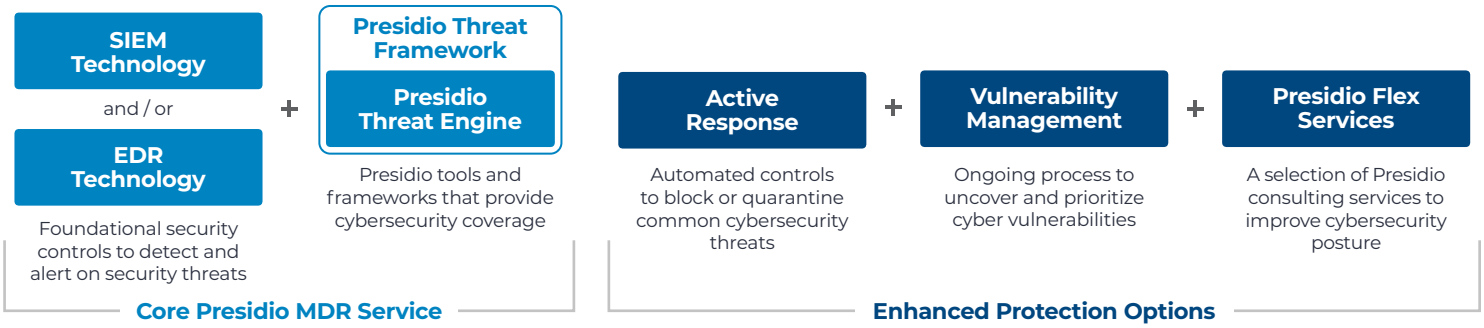
Web Application Penetration Test: Test externally available web applications to evaluate security controls and identify vulnerabilities an attacker could exploit to obtain access to sensitive data and organizational compromise

Remote Wireless Penetration Test: Test an organization's wireless technology and security controls to identify vulnerabilities within the wireless infrastructure

Incident Response Tabletop Exercise: Perform a controlled, simulated exercise to evaluate Incident Response/Incident Handling plans, team/departmental coordination, escalation workflows, and leadership decision-making

Incident Response Retainer: Retain Incident Response services from teams experienced in the triage, identification, containment, and eradication of security threats when a breach occurs

Presidio MDR



BENEFITS OF PRESIDIO MDR

Implementing the right tools and best practices with Presidio MDR and specialized cybersecurity services will provide a positive impact on business operations.

Rapid Integration
Presidio MDR seamlessly integrates with SIEM and EDR systems, protecting against a growing threat landscape, and future-proofs operations with continuous support for more technology integrations.

Enhanced Visibility
As a provider of protection services for a community of clients, Presidio MDR consolidates threat intelligence across multiple systems for the latest protections. As soon as a threat appears in one client, remediation is proactively implemented across all clients.

Reduced Mean Time to Detect / Mean Time to Respond
Time to remediate is critical to business continuity. Presidio MDR reduces initial responses from hours to minutes, not just with notifications, but also with active responses to immediate cyber threats.

Security Framework Alignment
Presidio MDR is designed as a professional managed service that aligns with multiple security frameworks to ensure the right coverage and constantly evolving for today's threat landscape – operating non-stop 24x7x365.

Operational Excellence
With Cybersecurity Flex Services, each client can easily adjust to immediate changes in their operational status or can continue to validate the integrity of their environment with regularly scheduled cybersecurity analysis.

Enhanced Security Posture
Presidio MDR is a critical component of a strong cybersecurity posture. Presidio cybersecurity services can help to support audits, while providing confidence that the quality of work is meeting industry standards.

Improved IT Operations
Presidio MDR provides crucial threat detection 24x7x365 with powerful detection and remediation. Presidio Cybersecurity Flex Services enable rapid support for enhanced cybersecurity consulting expertise. With the current market of cyber risks, finding and retaining skilled personnel can be an unsurmountable challenge.

Return on Investment (ROI) / Risk Avoidance
The Presidio MDR solution enhances an organization's ability to protect their business. The ROI crosses from the traditional reduction in total cost of operations to also deliver a dramatic reduction of risk of brand, liability and other impacts of ransomware and cybersecurity threats.

Financial Optimization
A predictable OPEX model that reduces cost and risk and support for cyber insurance and regulatory requirements provides bottom line benefits.

Corporate Brand Protection
Presidio MDR reduces the risk of a major data breach. Investments in cyber protects the corporate brand.

Presidio MDR

WHAT MAKES US DIFFERENT

Presidio is a trusted partner to our clients, securing their infrastructure, employees, customers and assets from ever-growing cyber threats. Our clients trust Presidio:

- **End-to-End Protection** – Presidio MDR is a powerful platform, integrating with the broad spectrum of cyber products to support the entirety of the cyber infrastructure, from the border, through the network, down to every endpoint.
- **Cyber Intelligence** – The Presidio cyber intelligence data is comprised of knowledge from thousands of data sources, dozens of cyber products, transactions, and events supporting rapid detection and response in a managed services deployment. In addition to our own accumulated intelligence, we have intelligence sources familiar with Classified (government) and Dark Web threats.
- **Speed and Accuracy** – Deep knowledge of every layer of the IT and cyber architecture, combined with proven methodologies supports responding in record time to potential threats. The response can be deployed in minutes instead of hours or days.

WHY PRESIDIO

Presidio is a leading digital systems integrator, with deep experience in 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. Our clients benefit from:

- 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
- Multi-discipline experts provide for a broad view of client's potential vulnerabilities
- Deep security services bench and broad security services solutions provide domain expertise and consistent deliverables

INFORMATION SECURITY

CISA Certified Information Systems Auditor – An ISACA® Certification

CISM Certified Information Security Manager – An ISACA® Certification

PCI Security Standards Council – Qualified Security Assessor

ISO 27001 Certified

G2700

CISSP ISSAP

CISSP ISSMP

CISSP Certified Information Systems Security Professional

TECHNICAL ASSESSMENT

Cisco Certified CCIE Security

Cisco Certified CCNP Enterprise

Cisco Certified CCDP Design

Cisco Certified CCNA Security

Cisco Certified Specialist

Cisco Certified CCDA

INFRASTRUCTURE SECURITY

Offensive Security Certified OSCP

GCIA

GCIH

GCDA

GCFE

GPEN

GCFA

GSEC

GCWN

GCTI

GMON

GREM

CISA Cyber+Infrastructure

VENDORS AND STANDARDS

MCSE Microsoft Certified

VMware Certified Professional

Citrix Certified Professional

Citrix Certified Expert

HCISPP

netskope

paloalto PCNSE7

CMMC-AB Registered

LogRhythm Certified Platform Administrator

LogRhythm Certified Security Analyst

aws certified Cloud Practitioner

PMI PMP®

ICS-CERT

paloalto Networks

citrix

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.

Contact Presidio today: www.presidio.com