MANAGED DETECTION & RESPONSE

Solutions Outline

DATASHIELD™
an ADT company

Advanced Threat Detection with DATASHIELD's MDR

Managed Detection and Response (MDR) is the key component of DATASHIELD's Cybersecurity Resilience Platform. MDR, driven by the cutting-edge proprietary SHIELDVision, provides best in class 24 x 7 x 365 comprehensive network visibility in real time, along with the ability to analyze threats potentially missed by other technologies.

Traditional Managed Security Services Providers (MSSP) and simple alerting are just not enough given the current complexity of the cybersecurity landscape. Adequate protection requires a dedicated staff of security experts that can identify real threats and manage false positives. Prevention efforts are important but without proper analysis and remediation, cybersecurity swells to an unmanageable level for most organizations.

> "Real security is about people. On the day you're attacked, it doesn't matter how your network is configured, what kind of boxes you have, or how many security devices you've installed. What matters is who is defending you."
>
> – Bruce Schneier, Managed Security Monitoring: Network Security for the 21st Century

Protect Your Organization

Cybercriminals use a variety of tactics to compromise the security of an organization. No matter the size, organizations at every level are at risk. Whether it be simple phishing or complicated malware attacks, cyber attackers can obtain sensitive information more easily than most suspect. The business and brand consequences both financially and organizationally can cause permanent and irreversible damage.

Why is Cybersecurity so challenging for organizations today? - A variety of factors contribute to this position. As the security landscape evolves, the requirement for specialization is increasing. This coupled with the need for a proper strategy and core competency to implement a cybersecurity platform properly, leaves the average organization at a disadvantage. Put simply a lack of budget, staff and technology make cybersecurity more and more difficult every day.

DATASHIELD's MDR provides the key resources, compliance and vision to execute on the following initiatives.

- Comprehensive 24x7x365 continuous monitoring
- Full network visibility beyond signatures and logs
- Real-time advanced threat detection using cyber threat intelligence
- Active Hunting
- Deep Forensic Analysis

The Next Generation of Cybersecurity

DATASHIELD Managed Detection and Response delivers comprehensive visibility into activity on the network and is a core component of the Cybersecurity Resilience Platform.

Why MDR?

Combating the modern cyber adversary requires 24x7x365 continuous monitoring, active hunting, deep forensic analysis using cyber threat intel, and real-time threat detection.

In today's always online cyber landscape, simple alerting is no longer enough. The traditional MSSP approach including technologies such as firewalls, anti-virus and log management (SIEM) are now only the beginning to a properly secured network. The real difference with MDR is the active trained professionals using the proper strategy with the right tools.

Having the right people, process and technology in place for detection and response is critical to minimizing the risk of a major breach.

Why DATASHIELD?

DATASHIELD is re-defining cybersecurity with an MDR service that acts as an extension of your own internal security team. Utilizing DATASHIELD mean that you only must focus on threats that are valid. DATASHIELD acts as a partner with your company and not only identifies true incidents but puts them into context from a scope and severity standpoint while providing steps for immediate containment and response.

The DATASHIELD Differentiator

What sets DATASHIELD apart? DATASHIELD has delivered MDR before it was an industry standard. Not only does DATASHIELD have more experience in the space than the competition, but it also takes an entirely different approach.

Rather than dictate which products a client must utilize, DATASHIELD is SIEM agnostic and takes a true partnership and consultative approach, outlined by the following process.

- **Understand Your Organization**
  DATASHIELD takes the time to find out why your organization chose the current technology and how that fits in with your business objectives.

- **Keep Risks and Costs Down**
  Rather than remove an existing security infrastructure, the goal is to keep risks negligible and costs low with a best-of-breed SOC as a service solution.

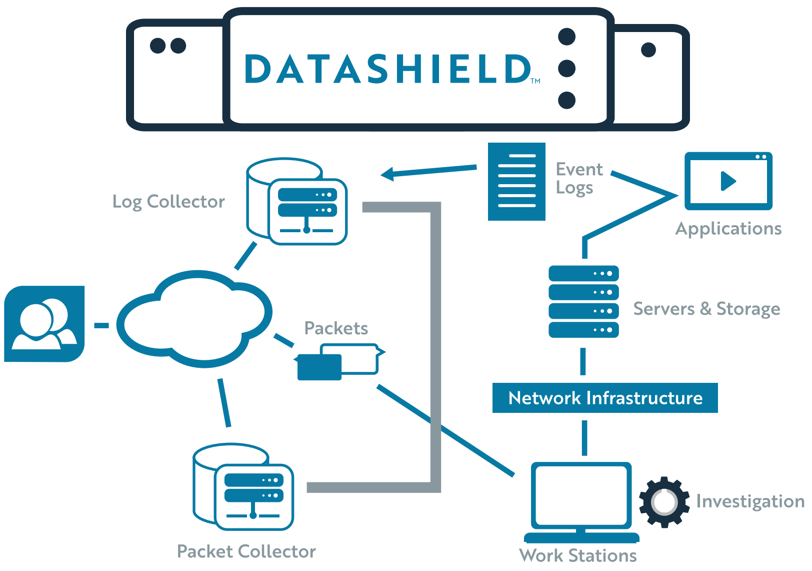
- **Allow for Natural Growth**
  Taking the time for proper solution implementation and utilization allows for scalability as your organization grows.

DATASHIELD Cybersecurity Advanced Monitoring: Architecture

DATASHIELD Improves your Organizations Security Posture through an Advanced Detection, Investigation and Response Architecture.

IMPROVING SECURITY POSTURE THROUGH AN ADVANCED **DETECTION | INVESTIGATION | RESPONSE** ARCHITECTURE

ADVANCED SECURITY OPERATIONS CENTER



1 DETECT ANOMALOUS EVENTS

- Event log collection
- Detection via patterns
- Focus: Indicator/ IoCs

2 DETECT ANOMALOUS BEHAVIOR

- Network Packet Collection
- Detection via pattern as well as Active Hunting
- Focus: Observables/OoCs

3 INVESTIGATE ANOMALIES

- Network session (conversion) analysis
- Host-based memory and disk analysis
- Focus: Indicators/IoCs & Obserables/OoCs

4 RESPOND TO VALID INCIDENTS

- Direct contact with SOC analytics
- Remote support throughout remediation
- Onsite incident response assistance available

5 IMPROVE SECURITY POSTURE

- Add/remove/edit detection patterns (content)
- Refine response procedures
- Advise on preventative additions/changes
- Remediation

DATASHIELD™ MDR

An experienced team of elite cyber security experts working 24x7x365 on your behalf

DATASHIELD employs a World Class, Highly Experienced Team of Security Analysts Who Have Defended Mission Critical Assets in National Security Environments & FORTUNE 500 Organizations.

At the core of our Managed Detection and Response service is our SOC 2 Type II certified US-Based Advanced Security Operations Center (ASOC).

REAL-TIME Threat Detection Leveraging People, Process and Technology

- **Investigation**
  Active Hunting, Alert Management, Report Generation, Customer Environment Monitoring, Technology Management.
- **Validation**
  Cyber Threat Intel (SHIELDVISION), manual intel analysis, automated real-time scanning and querying, past packet data analysis.
- **Notification**
  Customer is notified of verified incidents only – receives scope and severity assessment and recommendations for quick containment and response.

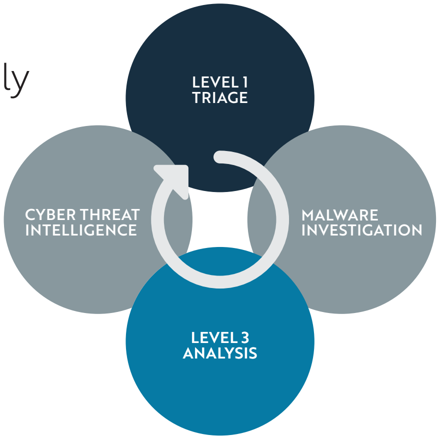
DATASHIELD's industry leading MDR includes the following key components:

- 24 x 7 x 365 monitoring and analytics, providing actionable intelligence and verified incident notifications to quickly mitigate threats and risks
- Advanced Cyber Threat Intel
- Understanding of critical business assets and process
- Experienced security analysts, all U.S. citizens
- U.S. based security operations center, SOC 2 Type II, SSAE 18
- Collaborative participation to support your incident response requirements related to insider threats, zero-day exploits and targeted malware, advanced persistent threats, fraud, espionage and data exfiltration

SOC: Core Capabilites

- Build, Deploy, & Monitor Content
- Perform Investigations & Analysis
- Active Hunting
- IOC Scanning with SHIELDVision
- Reverse Engineer Malware
- Analysis of Customer-Requested Investigations
- Manage Technology
- Real-time System Health/Uptime
- Initial Problem Determination and Remediation

Notify Customer of Verified Incidents only

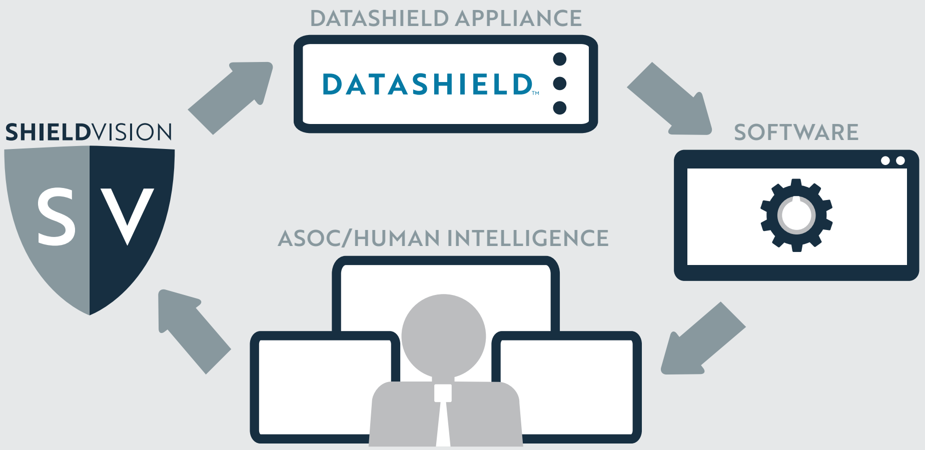


DATASHIELD™ SHIELDVISION

Introducing the most sophisticated threat intelligence platform available today...

By leveraging the most advanced human and technical resources, SHIELDVision provides a centralized platform for organizing, managing and analyzing cyberthreats. Threat intelligence collection, deep forensic analysis by experts and proactive content development help keep your organization safe in real time.

> "With SHIELDVision we can detect threats across our entire customer base simultaneously. Utilizing the latest threat intelligence, we can travel back in time to correlate and identify compromises that may be missed by other technologies."
>
> – Jeff Marshall: DATASHIELD CISO



RISK REDUCTION | AUTOMATION | VISIBILITY

SHIELDVision employs an innovative approach by applying cyber threat intel to packet level data. The Datashield team utilizes the SHIELDVision toolset to "go back in time" to identify compromises that have been missed by other technologies.

Using SHIELDVision the Datashield team applies cyber threat intel not only real-time as data is processed, but against previously captured packet data. With this approach even legacy traffic can be scrubbed against zero day exploit indicators of compromise, anomalies can be detected, and remediation in your environment can be completed.

This process helps close the time gap between detection and remediation greatly reducing the chances of a successful data breach.

DETECTS THREATS IN MINUTES NOT MONTHS

- **Rapid Automated Querying**
  Incident response automation tools that allow DATASHIELD analysts to quickly discover important characteristics of a dataset and find data-driven insights in the corresponding domain.
- **Real Time Alerts**
  Real-time threat analytics and alerting allowing you to defend your organization on the front lines against threats including phishing, malware, ransomware and botnets.
- **Historical Queries**
  Forensic investigation back in time working in concert with new-threat intelligence.
- **Manual and Automated Threat Identification**
  Scanning capabilities via both automated technologies along with manual hunting by cybersecurity experts.
- **Network Monitoring**
  Comprehensive networking monitoring including visibility into routers, firewalls, severs, client systems and software.

DATASHIELD™

Cyber Resilience Platform

Making your organization secure from the inside out...

MDR and DATASHIELD's SOC are at the core of the Cyber Resilience Platform, but that is not all DATASHIELD can do to keep your organization secure, minimize risk and lower total cost of ownership.

The DATASHIELD Cyber Resilience Platform is a hub and spoke cyber strategy that fits within your organization. Ancillary services are available based on your business needs.

Email Security

Email security is data protection 101. DATASHIELD has the technology through its security appliance, MDR and other collective measures to protect your organization at both the account and service level. Securing the content, access control mechanisms and proactive email security measures come standard.

- **Forensic Investigation**
- **Integration with MDR**
- **Malicious Insider Protection**
- **Phishing**
- **Business Continuity**
- **Archiving**

Network and Perimeter Security

DATASHIELD's Network Operations Center (NOC) works in tandem and complements the SOC, allowing for incident and alert handling that minimizes effects on network performance and availability. This ensures your organization can deliver on service level agreements (SLAs) and reduce downtime.

- **Firewall, Router and Switch Management**
- **24x7 Monitoring and Alerting**
- **Firmware Updates / Patching**
- **Troubleshooting**
- **Change Management**
- **Configure Archive / Management**
- **Defined SLA's**

Remediation and Education

Action plans, training and proper strategy are critical for a better overall security posture. DATASHIELD focuses on customer success and retention through a dedicated engagement manager, proper onboarding, asset criticality assessments, status calls, weekly summary reports and monthly executive summaries.

- **Recommended Actions from SOC**
- **Phishing Triage**
- **Incident Response**
- **User Awareness Training**
- **Threat Hunting**
- **Improved Security Posture**

DATASHIELD an ADT Company

Founded in 2009, DATASHIELD, is one of the fastest growing cyber security firms in North America. The company provides cyber security solutions in conjunction with managed detection and response services across all industries. DATASHIELD is a leading provider of managed detection and response services. The company leverages technology coupled with human-based intelligence and internal processes to detect and combat advanced threats in real-time.

Cybersecurity is all we do...

Our mission is to combat the modern cyber adversary and empower organizations with an increased security posture.

> "Cybersecurity risks pervade every organization and aren't always under IT's direct control. Business leaders are forging ahead with their digital business initiatives, and those leaders are making technology-related risk choices every day. Increased cyber risk is real — but so are the data security solutions. [1]"

– Gartner, Information Technology Insights 2019

Real Cyber Security Solutions, Real People.

SCOTTSDALE (Headquarters)
1475 North Scottsdale Rd., Ste #410
Scottsdale, AZ 85257

SALT LAKE CITY
455 E 200 S, Suite 100
Salt Lake City, UT 84111

ONLINE OR BY PHONE
866.428.4567
info@datashieldprotect.com

CONTACT A SECURITY EXPERT TODAY

DATASHIELDProtect.com

DATASHIELD™

datashieldprotect.com

Established over a decade ago from a joint venture with RSA and EMC/Dell, Datashield became ADT's advacned cybersecurity arm in 2017. The company was built by industry leading cybersecurity experts and is recognized as a leader in MDR and integrated platform solutions. The DATASHIELD Resilience Platform is highly scalable, designed to meet the needs of SMBs and global Fortune 500 enterprises alike, providing a holistic and automated approach to achieving cyber resilience goals.