Cisco Customer Experience

Protect what matters most with the best in cybersecurity

Advance your security operations capabilities by reducing mean time to detect and contain threats with Cisco Managed Detection and Response.

Every day we connect more desktops, devices, and things, creating new opportunities for service delivery and business growth. To take advantage of these opportunities, businesses must contend with a growing attack surface and an increasing number of cyberthreats, putting their privacy, data, and reputations on the line.

While these risks can be managed and mitigated with the right expertise, there is currently a significant cybersecurity skills shortage globally that adds to the challenge organizations face.

In fact, by 2021, it is projected there will be 3.5 million vacant cybersecurity positions around the world[1].

The key to minimizing the impact of a data breach is reducing time to detection. Without a focused detection capability, breaches can go undetected for months, by which time your organization's critical data is likely compromised.

With Cisco® Managed Detection and Response (MDR), you can reduce breach detection and response times and shield yourself from the high costs of security breaches.

Cybersecurity, managed for you by experts.

Cisco MDR, a managed security service, monitors and detects threats in the network, cloud, and at endpoints with the world's best cybersecurity experts, including:

- **A stronger security posture**, with access to advanced capabilities and experts who understand the expanding attack surface.
- **Greater confidence**, thanks to proven threat intelligence and automation.
- **Faster threat detection** and a more consistent response based on defined investigation and response playbooks supported by Cisco Talos® research.
- **Greater visibility** via integrated security architecture with 24x7x365 threat detection and response, drastically reducing mean time to detect and respond to threats.

Every 14 seconds

a business falls prey to ransomware[2].

While an overwhelming number of alerts come from security monitoring systems, nearly half of the alerts organizations receive go uninvestigated[3].

With more device usage and greater connectivity than ever before, the attack surface expands and evolves rapidly, meaning the frequency of threats will only increase.

Faster detection has results

The faster a data breach can be identified and contained, the lower the costs. Breaches with a lifecycle of less than 200 days are, on average, $1.22 million less costly than breaches with a lifecycle of more than 200 days[3].

0% cybersecurity unemployment rate

The current cybersecurity unemployment rate is zero percent[1].

The demand for cybersecurity professionals is growing at a faster rate than the supply of qualified candidates. In fact, the lack of cybersecurity skills has been identified by IT professionals (53%) as the most problematic skills shortage in organizations today[4]. As such, recruiting, retaining, and affording high-quality security expertise is among the biggest challenges organizations grapple with today.

Advance security operations with leading detection and response capabilities

Cisco MDR is delivered by a team of elite researchers, investigators, and responders, and supported by threat intelligence from Cisco Talos Intelligence Group, the largest non-governmental threat intelligence research team in the world.

The service leverages Cisco's world-class, integrated security architecture to advance your security capabilities, providing greater visibility across the network, cloud, and endpoints.

Organizations increase operational capabilities, advancing the security operations center (SOC) by monitoring multi-cloud, network, and endpoints. The service delivers relevant and prioritized actions with expert guidance and effective automated response to protect your business.

Cisco MDR provides:

- **Detection**, using an integrated cloud security ecosystem that improves mean time to detect and contain security threats. The service delivers relevant, high-confidence and consistent results using proven methodologies, unique intelligence and an experienced team.
- **Analysis** through the enrichment of alerts, including Talos threat intelligence. MDR provides attacker attributes and tactics to analysts with the critical context needed to prioritize the impact and urgency of a threat to a business.
- **Investigation** of identified threats utilizing defined investigation playbooks, which provide added context. When malware, ransomware, bot-net, bad actors and other such bad behavior occurs, we make data-driven decisions that establish relevant, meaningful and prioritized response actions.
- **Response**, which utilizes security orchestration and automated response (SOAR) and case management to execute defined response playbooks and provide detailed threat analysis, including recommended response actions.

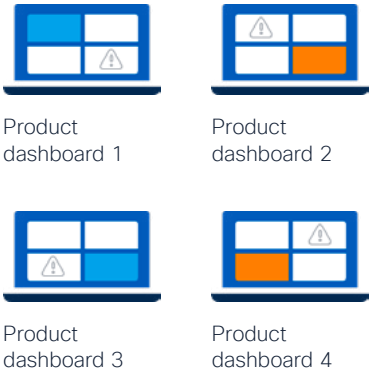
Your security operations with and without Cisco MDR

Before Cisco MDR

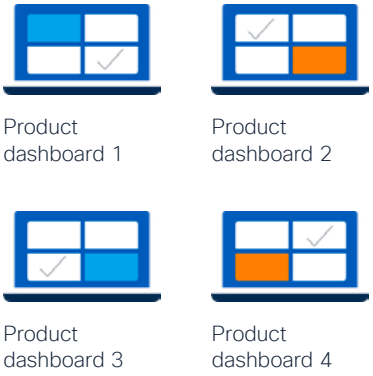
Inefficient, error-prone process required manual threat correlation, and performing complex tasks across multiple systems, which could result in missed threats and delayed responses.

1. Alert triggered

2. Investigation in multiple consoles



3. Response/remediation



Industry average time to detect a threat: 206 days[3]

With Cisco MDR

Accelerate detection and response to security threats provided by an integrated security ecosystem, unique threat intelligence, proven case management, deined playbooks, and response recommendations by an elite team of security experts.

1. Alert Triggered

2. Analysis

3. Investigation

4. Response Actions

MDR can reduce the time to detect and respond from months to hours

MDR leverages Cisco's world-class integrated security architecture

The MDR security architecture consists of Cisco Stealthwatch® Cloud, Advanced Malware Protection (AMP) for Endpoints, Threat Grid, and Umbrella™.

- **Stealthwatch Cloud** applies the latest threat intelligence and analytics capabilities to proactively protect your cloud resources, internal network, and even encrypted traffic against new threats.
- **AMP for Endpoints** correlates Talos threat data against your environment's telemetry data and known behavior, linking your defenses into a single, cohesive shield against emerging malware threats. It continually evolves your endpoint defenses with deep malware analysis, preventing malicious files from spreading.
- **Threat Grid** combines advanced sandboxing with a robust, context-rich malware knowledge base to determine the risk new malware poses to your specific environment and helps prioritize proactive defenses.
- **Cisco Umbrella** enforces security at the DNS and IP layers, blocking threats before they reach the network or endpoints. Under one umbrella, you can extend protection to devices, remote users, and distributed locations anywhere in minutes.

Healthcare industry example use case

Challenge

The increasing transition from paper to digital healthcare record-keeping puts patient information and medical records at risk.

Solution

MDR detects ransomware that can bypass traditional anti-virus defenses, spread laterally, and cripple a hospital's network.

Cisco's expert investigators research the suspicious file access activity and lateral movement attempts throughout the hospital's network.

MDR responds by isolating the host, cleaning the infection, and blocking external command and control servers to prevent any other hosts from being infected.

Outcomes

The threat is identified early in the kill chain, contained and eliminated within the hospital's network to minimize any potential impact and prevent the threat from successfully performing its objectives.

Advanced security analytics and automation are utilized to deliver alerts with correlated insights and actionable next steps tailored to the hospital's security operational policies.

Stay protected with Cisco MDR

To protect and grow your business in an increasingly connected world, it is critical to detect security risks and protect your assets. Cisco MDR puts the best in cybersecurity on guard for you 24 hours a day, providing advanced detection and response capabilities with expert resources that understand the expanding and evolving attack landscape.

MDR helps you improve your organization's security posture and advance security operations efficiency with an expert team and industry-leading threat research.

Protect what matters most. Secure your organization today.

1. The 2019 Official Annual Cybersecurity Jobs Report, Cybersecurity Ventures, 2019
2. Ransomware Report, Cybersecurity Ventures, 2017
3. IBM Security and Ponemon Institute 2019 Cost of a Data Breach Study
4. Enterprise Strategy Group Survey, 2018 - 2019

Learn more

cisco.com/go/mdr

Get in touch.

Contact your Cisco sales representative, partner or visit cisco.com/go/mdr