WatchGuard MDR

Program Guide

About This Document

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Copyright, Trademark, and Patent Information

About WatchGuard

For 25 years, WatchGuard has pioneered cutting-edge cybersecurity technology and delivered it as easy-to-deploy and easy-to-manage solutions. With industry-leading network and endpoint security, secure Wi-Fi, multi-factor authentication, and network intelligence products and services, WatchGuard enables more than 250,000 small and midsize enterprises from around the globe to protect their most important assets including over 10 million endpoints. In a world where the cybersecurity landscape is constantly evolving, and new threats emerge each day, WatchGuard makes enterprise-grade cybersecurity technology accessible for every company. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America.

For additional information, follow WatchGuard on social media. Also, visit our InfoSec blog, Secplicity, for real-time information about the latest threats and how to cope with them at www.secplicity.org.

Address

255 S. King St.
Suite 1100
Seattle, WA 98104

Support

www.watchguard.com/support
U.S. and Canada +877.232.3531
All Other Countries +1.206.521.3575

Sales

U.S. and Canada +1.800.734.9905
All Other Countries +1.206.613.0895

Contents

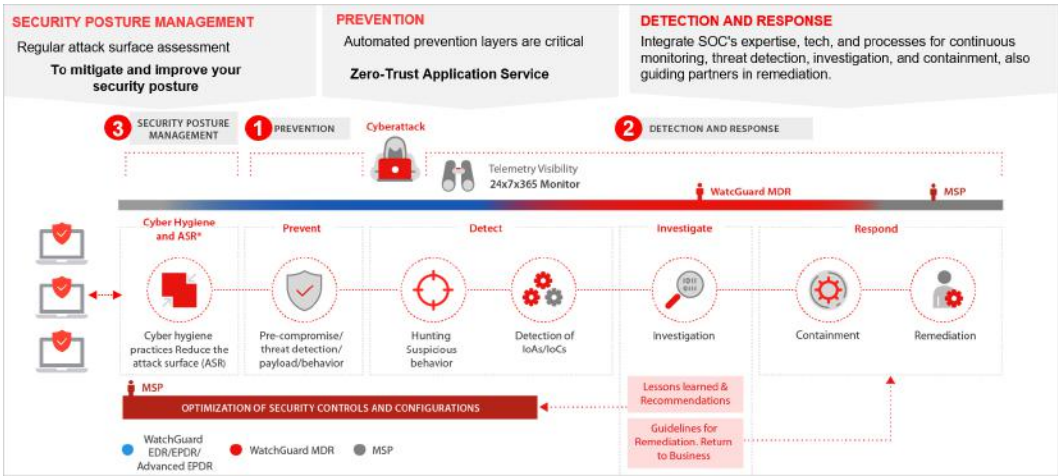
About WatchGuard MDR

WatchGuard Managed Detection and Response (MDR) keeps your customers' endpoints safe with security monitoring, threat hunting, attack detection, investigation, and containment. It provides guided recommendations to remediate affected assets and to improve customer security posture. WatchGuard MDR enables you to provide MDR services to your customers with minimal investment in a modern SOC (security operations center), expensive technology, or cybersecurity experts.

Powered by innovative AI technologies, the MDR service is fully managed by WatchGuard's SOC. Our cybersecurity experts provide 24/7 support to you and your customers to elevate their overall cyber resiliency and minimize the time to detect and respond to threats. In the event of a potential cyberattack, the WatchGuard Global Cybersecurity team guides you through the containment and remediation process. To minimize the time to respond in case of an attack, you can delegate the containment to WatchGuard.

Additionally, when you enroll a customer in the MDR service, the WatchGuard team helps you strengthen the security posture of your customer to immediately improve their overall resiliency to cyber threats.

WatchGuard MDR supports you with regular, automatically delivered health status reports. The reports include protection and risk status for the managed endpoints, monthly service activity, and recommendations to mitigate and remediate identified threats.



Roles and Responsibilities

Partners and the WatchGuard Global Cybersecurity team work together to provide MDR services to customers. Before you get started with WatchGuard MDR, it is helpful to understand the roles and responsibilities for both partners and the WatchGuard team.

Partner Role

Partner responsibilities include:

Determine Eligibility and Initiate Partner Onboarding

You must meet with your WatchGuard account manager to confirm eligibility requirements and to initiate the partner onboarding process. For more information, go to *Partner Eligibility and Onboarding*.

Purchase and Allocate Licenses

Each time you purchase a new MDR service license for one of your customers, you activate the license then allocate the MDR service to the customer endpoints in WatchGuard Cloud. For more information, go to *Purchase and Allocate Licenses*.

Enroll Your Customer

For each new customer, complete the MDR enrollment form in WatchGuard Cloud. For more information, go to *Customer Onboarding*.

Follow Remediation Guidelines

If an incident occurs, follow recommendations from the WatchGuard Global Cybersecurity team to remediate the incident so the customer can return to business-as-usual as soon as possible. For more information, go to *Incidents*

WatchGuard Global Cybersecurity Team Role

The WatchGuard Global Cybersecurity Team responsibilities include:

Monitor, Analyze, and Triage

WatchGuard MDR proactively monitors and analyzes telemetry data from your customer endpoints to identify, aggregate, and prioritize indicators and alerts.

Investigate

WatchGuard MDR determines whether an abnormal activity is malicious and requires a response.

Provide Threat Response

A threat response includes alerts that include details of the investigation, the list of affected endpoints, and guidelines to remediate the threat. When you onboard each customer, you specify whether you want to allow WatchGuard to isolate affected endpoints in response to a threat.

Search for Threats

WatchGuard threat hunters search for threats that might have evaded existing detection controls, based on threat intelligence and relevant indicators of compromise (IOCs) observed over time. If the threat hunting activity reveals indicators of malicious activity, the threat hunters perform an investigation. Additionally, WatchGuard creates new indicators of attack (IoAs) and indicators of compromise (IoCs) to improve the efficacy and efficiency of the service.

Deliver Reports

WatchGuard MDR automatically delivers weekly health status and monthly service activity reports. For more information, go to *Reports*.

Provide Remediation Guidance

The WatchGuard team provides remediation guidance for the detected threats. For more information, go to *Incident Remediation*.

Partner Eligibility and Onboarding

To be eligible to offer the WatchGuard MDR service, you must provide managed services and have experience with the installation, support, and troubleshooting of WatchGuard EDR, EPDR, Advanced EPDR, or Panda AD360. Your staff must also have access to your customers' environments, so that they can respond quickly when the MDR service detects a compromise attempt.

In addition, you must attend an initial partner onboarding session.

Eligibility

To offer MDR services, you must:

- Have a team with operational management capabilities within your customer environments.
- Have at least one person available 24 hours a day, 7 days a week, in case the WatchGuard Global Cybersecurity team needs to contact you. For example, we might need your help to determine if activity we detect on your customer's network is approved by you or your customer or indicates a potential security threat.

We also recommend:

- You have at least one staff member with a current WatchGuard Endpoint Security technical certification.
- You have a scalable business plan in place to support the growth of the MDR service.

Onboarding Process

When you meet the eligibility requirements, you work with WatchGuard to move through the onboarding process:

1. Contact your account manager to express interest in WatchGuard MDR.
2. After your account manager qualifies your organization as eligible, they forward the request to the onboarding team.
3. The onboarding team interviews you or your team to collect essential data and to review your responsibilities.
4. Sign the Terms of Service agreement.
5. Schedule a call with the onboarding team to complete the Partner Onboarding form.

Confirm Endpoint Security Installation and Configuration

For a successful implementation of the MDR service, it is important that WatchGuard Endpoint Security software is correctly deployed and configured on your customer's endpoints.

To help you verify your customer's WatchGuard Endpoint Security products are configured correctly and securely, the onboarding team provides a checklist of important configuration settings. Make sure that:

- The WatchGuard Endpoint Agent is installed on all endpoints.
- The management UI is protected by multi-factor authentication.
- Anti-tamper protection is enabled.
- Protection cannot be uninstalled without a password.
- All endpoints are configured to use Hardening or Block mode.
- Anti-exploit protection is enabled for all endpoints.

WatchGuard also recommends that you allocate the WatchGuard Full Encryption and Patch Management modules to the customer account.

For more information about how to install and configure WatchGuard Endpoint Security products, review these Help topics and KB articles:

- Get Started with WatchGuard Endpoint Security
- Endpoint Security Installation Requirements
- Endpoint Security Installation Plan
- Best Practices – Installation Tips for Groups and Settings
- Best Practices – Post-Deployment Tips for Endpoint Security
- WatchGuard Endpoint Security Modules
- URLs used by Panda and WatchGuard Endpoint Security products

Purchase and Allocate Licenses

You purchase WatchGuard MDR as an add-on SKU to an existing WatchGuard Endpoint Security product license.

- The license must include the same number of endpoints for WatchGuard MDR as the customer has for WatchGuard EDR, WatchGuard EPDR, Advanced EPDR, or Panda AD360.
- The customer must have at least 15 endpoints.
- WatchGuard MDR is not available as an NFR (Not for Resale) license.
- To experience the WatchGuard MDR service in your own environment, newly onboarded partners can obtain a 60-day trial. Trial licenses are not available for customer environments.

After you purchase the license, you must activate the license and allocate the endpoints in WatchGuard Cloud. For more information, go to Activate an Endpoint Security License and Allocate Endpoints in *Help Center*.

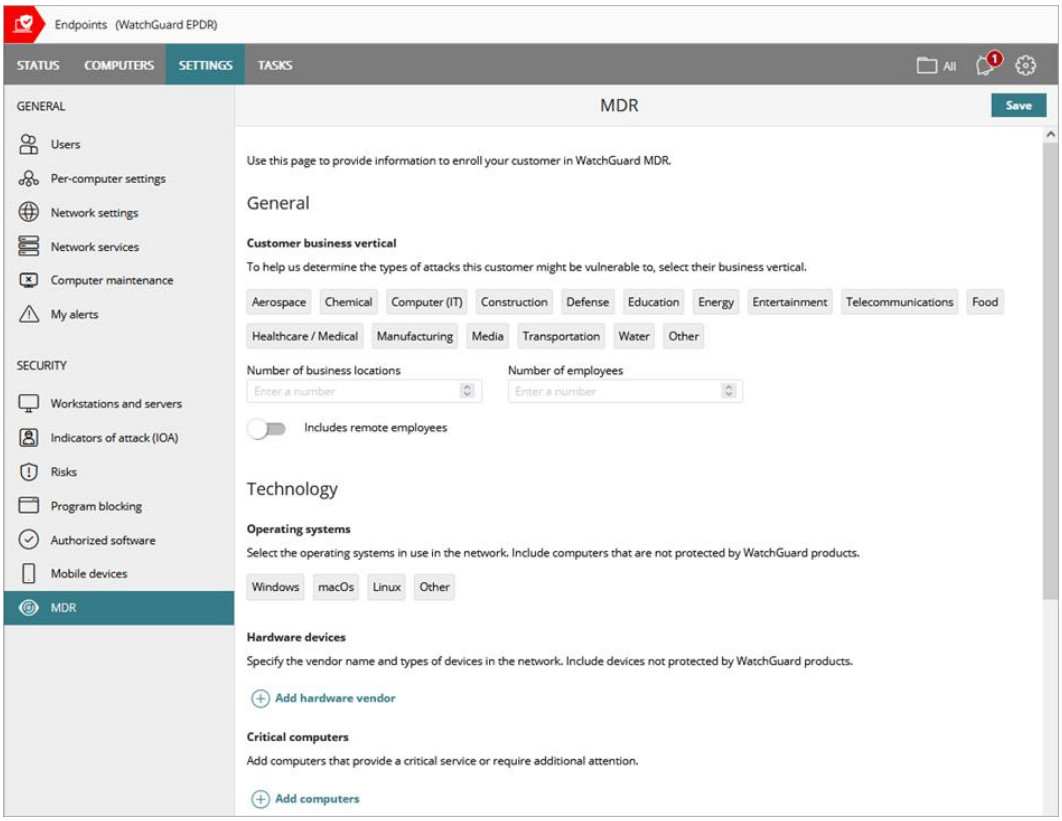
You cannot allocate an MDR license to a delegated account. For more information, contact your account manager.

Customer Onboarding

After you purchase, activate, and allocate the MDR license for a new customer in WatchGuard Cloud, complete the MDR enrollment form. The information you provide in the form helps the WatchGuard Global Cybersecurity team understand the customer environment, which devices provide critical services, and whether WatchGuard can automatically isolate infected computers.

To enroll a customer in WatchGuard MDR:

1. In WatchGuard Cloud, select the Subscriber account you want to enroll in WatchGuard MDR.
2. Select **Configure > Endpoints**.
3. Select **Settings**.
4. From the left pane, select **MDR**.
   The MDR enrollment settings page opens.



For more information about the enrollment form, go to Configure WatchGuard MDR in *Help Center*.

After you complete the MDR enrollment form for a customer, the WatchGuard team assesses the attack surface at the endpoints and makes recommendations to help you to strengthen the customer's security posture and improve their overall resiliency to cyber threats.

Incidents

Incident remediation and optimization are not actively part of the WatchGuard MDR service. When the WatchGuard Global Cybersecurity team contacts you or your security team about an incident, you must follow the guidelines provided by the team.

Incident Notification

If a WatchGuard MDR customer experiences a security incident, depending on the severity and escalation path you choose during partner onboarding, a member of the WatchGuard team contacts you by email or phone.

Possible incident severity levels are:

Security Level	Description	Notification
High	Indicators of targeted attacks with the potential to lead to a confirmed breach or unauthorized system access, which poses an imminent threat to customer assets.	The WatchGuard team first sends an incident report to the email address you designate during partner onboarding. Depending on the defined escalation path, the email might be followed by a phone call.
Critical	A validated breach or unauthorized system entry that presents an imminent danger to customer assets, encompassing active attackers, data encryption or destruction, and data exfiltration.	A member of the WatchGuard team calls the phone number you specify during partner onboarding.
Medium, Low, and Informational	Incidents that do not pose an imminent security threat.	The WatchGuard team includes this information in the Monthly Summary report.

For more information about the information provided in the Incident, Weekly Summary, and Monthly Summary reports, go to *Reports*.

Incident Report Email

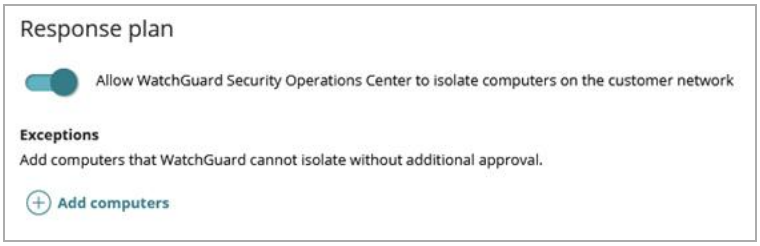
For lower severity concerns, the WatchGuard team sends an incident report by email. An incident report contains the incident data and recommendations for remediation. Specifically, the report includes this information:

- **Executive Summary** – Shows a summary of the incident. For example, this might include the malicious file type found, the vulnerability that allowed the attack, and the endpoint configuration that protected the network.

- **Analysis** – Provides a more detailed explanation of the attack attempt, including file names and locations, impacted users, and times.
- **Case Details** – Shows a table of customer, host, and file details.
- **Recommendations** – Provides a list of recommended actions to remediate the threat. For example, the team might recommend that you run an on-demand scan on the infected device to remove any traces of malware, change the user account credentials, or make sure that directories created by the malware are deleted from devices.

Incident Mitigation

When you enroll a customer in WatchGuard MDR, you can choose to allow the WatchGuard team to automatically isolate computers on the customer network when an incident occurs.



Incident Remediation

When an incident occurs, you are responsible for the remediation or post-incident activities. The WatchGuard team provides guidelines on how to execute the remediation for the customer. They might also make recommendations on how to improve the customer's security posture to avoid being compromised by threat actors using the same techniques in the future.

Reports

WatchGuard MDR automatically delivers weekly health status and monthly service activity reports to help you mitigate and remediate identified threats.

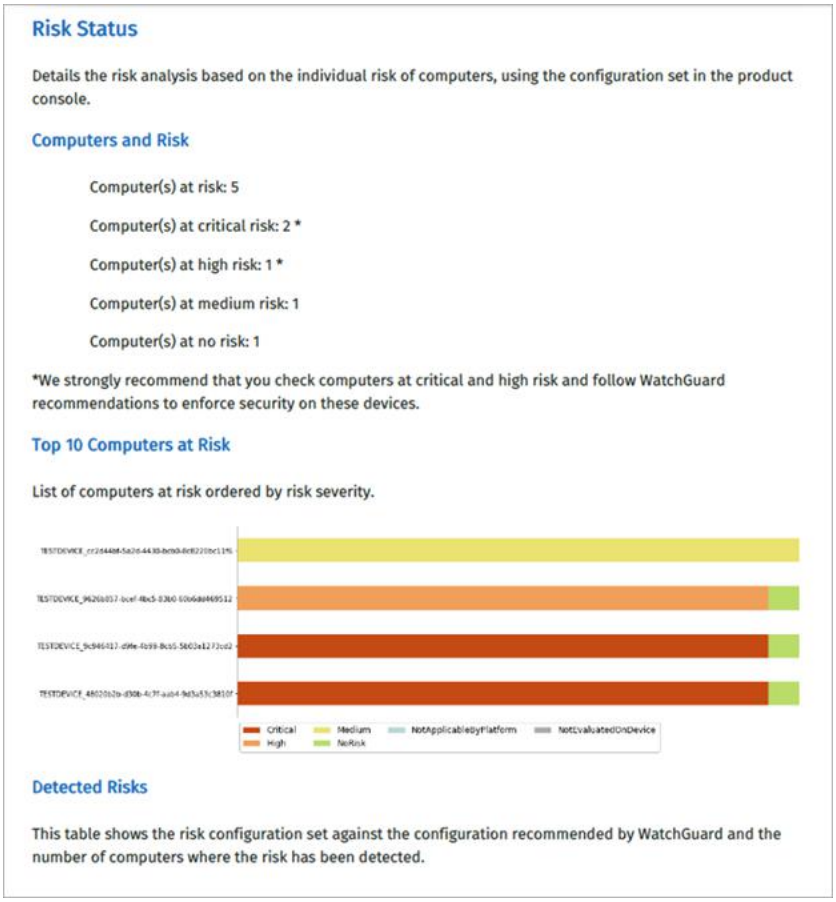
Weekly Summary Report

Weekly reports provide details about the health status of the managed endpoints. WatchGuard sends weekly reports to the email addresses you specify in the **Reports** section of the MDR enrollment form in WatchGuard Cloud.

The report includes updates on health issues or significant misconfigurations that could degrade the overall security posture of the environment or negatively impact the protection, monitoring, investigation, or the ability to take response actions. The report also includes recommended actions to mitigate and remediate identified threats. This weekly report includes:

- **Protection Status** – Shows the number of computers found on the customer network and their protection status. It also includes the number of computers found that are not managed by WatchGuard Endpoint Security.

- **Risk Status** – Provides a risk analysis based on the individual risk of computers, using the Risk settings in the WatchGuard Endpoint Security management UI. For more information, go to Configure Risk Settings in *Help Center*.



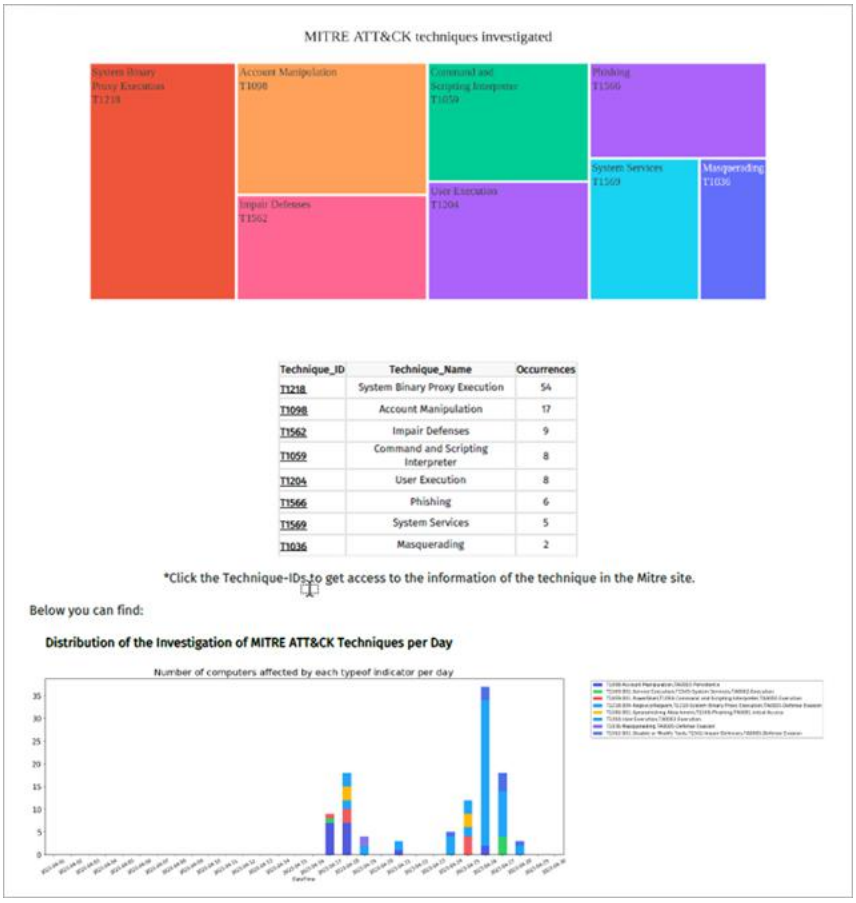
Monthly Summary Report

Monthly reports provide information for the previous month's service activity, including the status of the service, the notifications or communications provided, and the status of open incidents. WatchGuard sends monthly reports to the email addresses you specify in the **Reports** section of the MDR enrollment form in WatchGuard Cloud.

The monthly report includes:

- **Executive Summary** – Shows a summary of the protection status and risk level for computers found on the customer network.
- **Protection Level** – Shows the number of protected and unprotected computers found on the customer network. It also indicates if the risk monitoring settings for the customer match those recommended by the WatchGuard Global Cybersecurity team, the current risk level, the risks trend for the previous three months, and information about critical and high severity vulnerabilities detected.

- **Risk Level** – Provides an overall risk level, as well as a risk level for:
  - Malicious applications
  - Exploits
  - IOAs
  - Malwareless attack attempts
- **Activity** – Provides a summary of the protection activity performed in the month, including:
  - Number of programs scanned by Endpoint Security
  - Number of exploits detected
  - Number of potentially unwanted programs detected
  - Number of events sent to, processed by, and analyzed by the WatchGuard team to identify potential threats
  - Information about the threats detected
- **Advanced Threat Detection** – Shows the anomalous activity identified and investigated by the WatchGuard team and shows association with MITRE ATT&CK framework attack techniques.
- **Attack Attempts Identified and Reported** – Indicates if any attacks were identified that require the customer or Service Provider to take action.



Technique_ID	Technique_Name	Occurrences
T1218	System Binary Proxy Execution	54
T1098	Account Manipulation	17
T1562	Impair Defenses	9
T1059	Command and Scripting Interpreter	8
T1204	User Execution	8
T1566	Phishing	6
T1569	System Services	5
T1036	Masquerading	2

*Click the Technique-IDs to get access to the information of the technique in the Mitre site.

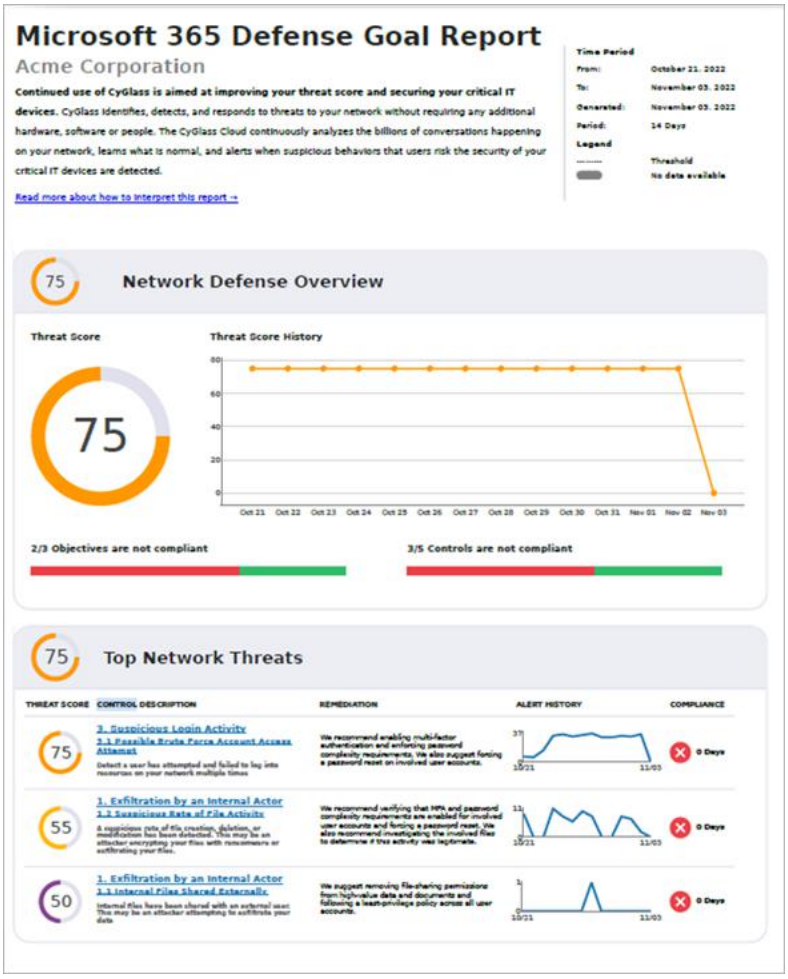
Below you can find:

Distribution of the Investigation of MITRE ATT&CK Techniques per Day

Bi-weekly Microsoft 365 Defense Goal Report

If the customer uses Microsoft 365, and you provide WatchGuard a read-only account for the customer tenant, you can receive a Microsoft 365 Defense Goal report. The report provides data collection analysis of alerts for incidents that occur within a customer Microsoft 365 environment. The report includes:

- **Threat Score History** – The Microsoft 365 Threat Score represents your exposure to cyberattack through the Microsoft 365 product suite. It is an aggregation of the threat scores for each of the controls presented in the report.
- **Top Network Threats** – Shows a list of the three highest-risk controls covered in the report.
- **Objective and Control Detail** – Provides details for each of the defense objectives included in the Defense Goal. For each objective, the details include the compliance status, alert history, and suggestions for remediation.
- **Control Violation Detail and Remediation** – Provides a detailed description of the controls that were violated for the report period and remediation suggestions.



To enroll in WatchGuard MDR, make sure you meet the partner eligibility requirements documented in the *Partner Eligibility and Onboarding* section, and then contact your WatchGuard account manager.