+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 06/12/2026

Sign up

WatchGuard Endpoint Security Essential Training

2 days (14 hours)

Overview

WatchGuard Endpoint Security is a solution for protecting endpoints and servers that helps prevent, detect, investigate, and remediate threats targeting endpoints. It combines antivirus protection, behavioral detection, EDR, application control, monitoring, and incident response.

Our WatchGuard Endpoint Security Essentials training will help you master the fundamentals of deploying, configuring, and operating a WatchGuard endpoint security solution.

You will learn how to administer the cloud console, organize devices, deploy agents, configure security policies, and tailor protections to user endpoints, servers, and sensitive profiles.

Upon completion of this training, you will be able to analyze alerts, investigate an endpoint incident, isolate a compromised machine, implement remediation actions, and utilize monitoring dashboards.

This training also covers best practices for endpoint hardening, application control, exception management, reporting, day-to-day operations, and collaboration with SOC or cybersecurity teams.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Understand the architecture and use cases of WatchGuard Endpoint Security

- Deploy agents and organize machines, groups, and policies
- Configure antivirus, EDR, application control, and web security protections
- Analyze alerts, events, suspicious behavior, and endpoint incidents
- Implement response actions: quarantine, blocking, isolation, and remediation
- Utilize dashboards, reports, and best practices for administration

Target Audience

- System administrators
- Security administrators
- Cybersecurity analysts
- SOC analysts
- Security managers
- IT teams responsible for protecting workstations and servers

Prerequisites

- General knowledge of system administration
- Basic understanding of cybersecurity and endpoint protection
- General understanding of malware, security alerts, and IT incidents

Technical prerequisites

- A computer with a modern web browser
- A stable internet connection

WatchGuard Endpoint Security Essentials Training Agenda

[Day 1 - Morning]

Introduction to WatchGuard Endpoint Security

- Understand the role of WatchGuard Endpoint Security in a strategy for protecting endpoints and servers
- Distinguish between EPP, EDR, EPDR, and Advanced EPDR approaches
- Identify threats targeting endpoints: malware, ransomware, scripts, phishing, and suspicious behavior
- Explore the cloud management console, dashboards, and key security modules security
- Understand the protection cycle: prevention, detection, investigation, containment, and remediation
- Hands-on workshop: explore the WatchGuard Endpoint Security console, identify active protections
  and analyze the status of the endpoint fleet

[Day 1 - Afternoon]

Deploying agents and security policies

- Preparing to deploy agents on user workstations and servers
- Organize groups, profiles, machines, users, and security policies
- Configure antivirus, antimalware, anti-exploit, and behavioral protection
- Implementing controls for applications, devices, scripts, and web access
- Tailor policies to specific profiles: office workstations, servers, sensitive users, and remote workers
- Hands-on workshop: create an endpoint security policy, apply it to a group of machines, and verify its deployment

Threat prevention and endpoint hardening

- Understand prevention mechanisms against ransomware, unknown malware, and fileless attacks
- Configure exclusions, allowlists, blocks, and application control rules
- Reducing the attack surface on workstations and servers
- Manage updates, signatures, detection engines, and protection settings
- Avoiding common mistakes: overly permissive policies, excessive exclusions, and lack of profile segmentation
- Apply a hardening checklist for critical endpoints

[Day 2 - Morning]

EDR Detection, Alerts, and Investigation

- Understand how EDR detection and behavioral analysis work
- Analyze alerts, events, processes, files, network connections, and suspicious actions
- Prioritize incidents based on their severity, context, and affected assets
- Investigating an endpoint alert: timeline, indicators, affected machine, and user actions
- Identifying attack indicators: unusual execution, persistence, privilege escalation, and lateral movement
- Hands-on workshop: analyze a security alert, reconstruct the timeline of an incident, and assess its risk level

[Day 2 - Afternoon]

Incident response and remediation

- Implement response actions: quarantine, deletion, blocking, isolation, and restoration
- Isolate a compromised device to limit the spread of a threat

- Manage false positives, exceptions, restored items, and remediation decisions
- Document an endpoint incident and prepare relevant information for security teams
- Define a response process tailored to desktop, server, and remote work environments
- Hands-on workshop: Handling an endpoint incident from start to finish, from alert to remediation

Monitoring, reporting, and best practices for operations

- Use dashboards to monitor the security status of the endpoint fleet
- Create reports on threats, incidents, vulnerable machines, and remediation actions
- Establish an operational routine: review alerts, exceptions, policies, and non-compliant endpoints
- Align WatchGuard Endpoint Security with SOC, ITSM, and incident response practices
- Define best practices for administration: roles, access, logging, updates, and governance
- Hands-on workshop: Build an endpoint monitoring dashboard and define a daily operations checklist
  Daily

Target Audience

This training is intended for both individuals and companies, large or small, seeking to train their teams on new advanced IT technology or to acquire specific business knowledge or modern methods.

Assessment upon enrollment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency in various types of technologies, as well as their expectations and personal goals regarding the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

Teaching Methods

Practical Course: 60% Practical, 40% Theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the trainer, supported by examples and reflection sessions, and group work.

Assessment

At the end of the session, a multiple-choice questionnaire is used to verify that the skills have been properly acquired.

Certification

A certificate will be issued to each trainee who has completed the entire training program.