PICUS | THE COMPLETE SECURITY CONTROL VALIDATION PLATFORM

# PACKAGING GUIDE

## BUNDLE #1

### Ransomware Readiness

**Attack Modules included:**

Network Infiltration

Endpoint

- **Ransomware-only Threat Library Content**
- **Two simulation agents**
- **Vendor-specific mitigation recommendations for one vendor technology**

**Detection Analytics**

- EDR Integration ADD-ON

## BUNDLE #2

### End User Security Readiness

**Attack Modules included:**

Network Infiltration

Email Infiltration

Endpoint

- **Full Threat Library Content**
- **Threat Builder**
- **Four Simulation Agents**
- **Vendor-specific mitigation recommendations for one vendor technology**

**Detection Analytics**

- EDR Integration ADD-ON
- SIEM Integration ADD-ON

## BUNDLE #3

### Complete Security Posture

**Attack Modules included:**

Network Infiltration

Email Infiltration

Web Application

Endpoint

Data Exfiltration

- **Full Threat Library Content**
- **Threat Builder**
- **Seven Simulation Agents**
- **Vendor-specific mitigation recommendations for two vendor technologies**

**Detection Analytics**

- EDR Integration ADD-ON
- SIEM Integration ADD-ON

PICUS | THE COMPLETE SECURITY CONTROL VALIDATION PLATFORM

# Feature Comparison Chart

| Feature | Ransomware Readiness | End User Security Readiness | Complete Security Posture |
|---|---|---|---|
| Threat Library | Ransomware Only | Full | Full |
| Number of Simulation Agents | 2 | 4 | 7 |
| Threat Builder | ✘ | ✔ | ✔ |
| **Attack Modules** | | | |
| Endpoint Module | ✔ | ✔ | ✔ |
| Network Infiltration Module | ✔ | ✔ | ✔ |
| Email Infiltration Module | ✘ | ✔ | ✔ |
| Data Exfiltration Module | ✘ | ✘ | ✔ |
| Web Application Module | ✘ | ✘ | ✔ |
| **Prevention Mitigation** | | | |
| Generic Mitigation | ✔ | ✔ | ✔ |
| Vendor-Specific Mitigation | 1 | 1 | 2 |
| **Detection Analytics** | | | |
| SIEM Integration | ✘ | Add-on | Add-on |
| EDR Integration | Add-on | Add-on | Add-on |

| | Add-Ons for Bundles |
|---|---|
| | **Ransomware Readiness Add-ons** |
| 1 | Additional Single Simulation Agent |
| 2 | Detection Analytics for EDR (per vendor) |
| 3 | Additional Vendor-specific Mitigation Recommendations (per vendor) |
| 4 | Web Application Attack Module |
| | **End User Security Readiness Add-ons** |
| 1 | Additional Single Simulation Agent |
| 2 | Detection Analytics for EDR (per vendor) |
| 3 | Detection Analytics for SIEM (for all simulations, per vendor) |
| 4 | Additional Vendor-specific Mitigation Recommendations (per vendor) |
| 5 | Web Application Attack Module |
| | **Complete Security Posture Add-ons** |
| 1 | Additional Single Simulation Agent |
| 2 | Detection Analytics for EDR (per vendor) |
| 3 | Detection Analytics for SIEM (for all simulations, per vendor) |
| 4 | Additional Vendor-specific Mitigation Recommendations (per vendor) |

**Note:**
Aforementioned bundles and add-ons are offered as an annual subscription. Discounted multi-year subscriptions are available.

## DISCLAIMER

*Product packaging offered in this document is valid and effective only within the United States.*

*All descriptions, images, references, features, content, specifications, products, and prices of products described or depicted in this document are subject to change at any time without notice. We will correct errors that we discover, and we reserve the right to revoke any stated offer and to correct any error, inaccuracy, or omission.*

# The Picus Platform Attack Modules

## Attack Modules

The output of each of the below simulations will provide a clear overview of how successful the simulated attacks were in your environment, enabling you to measure your security posture and prioritize the mitigation of prevention and detection gaps.

- **Network Infiltration:** Identify the exposure of your web browsing security to malicious code and exploit infiltration attacks. These simulations can be simulated by Browser and Endpoint simulation agents.
- **Email:** Test the effectiveness of your Email Security solutions against both malicious attachments and malicious URLs. Email attacks can be simulated quickly and can validate all kinds of Email solutions, including M365 and Google.
- **Web Application:** Assess the effectiveness of your network security controls such as NGFWS, IPSs an WAFs against web application attacks.
- **Endpoint:** Validate if Endpoint Security solutions are tuned properly and are providing protection against the latest attack vectors. This attack module is focused on assessing AV and EDR tools.
- **Data Exfiltration:** Simulate Data Exfiltration of sensitive data over typical covert channels, leveraging various protocols, ports, and file formats. The platform supports many critical data types such as Personal Identifiable Information (PII), and payment card data.

# Picus Platform Agents

## Simulation Agents

Each bundle includes a maximum permitted number of active simulation agents. The type of agents available will depend upon the bundle selected.

- **Browser Agents** (*an unlimited number of browser agents are included free as part of every bundle package and do not count towards an agent limit*). Browser agents enable users to simulate network infiltration attacks without the need to install software and therefore require minimal configuration.

- **Email Agents** (*available as part of the End User Readiness and Complete Security Posture Bundles*). Email Agents must be deployed to support The Picus Platform's Email Assessment Attack Module.

- **Endpoint Agents** (*available as part of the Ransomware Readiness, End User Readiness and Complete Security Posture Bundles*). Endpoint Agents must be deployed to support The Picus Platform's Endpoint Assessment and Network Infiltration Modules. Endpoint agents are available for Windows, Linux*, and macOS*.

Email and Endpoint Simulation Agents can be deployed across an environment but only the maximum number of agents can be active any any one time. Validating security controls actually means validating the security policies of the security controls. This means, for example, that Picus requires only one endpoint agent to validate the same security policy used across thousands of endpoints.

## Integration Agents

Integration agents enables The Picus Platform to integrate with SIEM and/or EDR controls to validate log and telemetry ingestion and alert generation. Integration agents are not included as part of the specified bundles and are separately licensable per technology. See the Detection Analytics section for more information.

*some attack simulation functionality is restricted on Linux and macOS.

# Picus Platform Mitigations

## Mitigation Recommendations for Prevention Controls

It is critical to respond fast to the identified security control gaps discovered with attack simulations. Mitigation recommendations provide insight on how security control gaps can be hardened to improve organizations' response to threats.

Picus provides two mitigation approaches in its product:

- **Generic Mitigation:** Provides best practices for hardening security controls or mitigating the impact of threats by hardening underlying infrastructure. Examples include MITRE ATT&CK best practices, network and email security hardening best practices.

- **Vendor-Based Mitigation:** These mitigations focus on providing actionable mitigations specific to a security vendor, answering the question: "How can my network security stack can prevent this threat?" in seconds. For each threat in Network Infiltration Assessment module, Picus highlights vendor signature-id so that security teams can quickly respond to that threat. Picus not only provide this mapping for new threats but also keep this mapping up-to-date for all relevant threats in Threat Library. This module is licensed per vendor and below vendors are supported for vendor-based mitigations.

# Picus Platform Detection Analytics Modules

## Detection Analytics Modules

The Detection Analytics Modules assess your capability of detecting adversarial tactics in your environment. Attack modules provide insights about the threats that are prevented during simulations, yet questions like “Can those threats be detected?” and “Did we get notified about those malicious activities?” cannot be answered without a SIEM/EDR integration.

The Picus Platform’s Detection Analytics Module functionality answers these questions by integrating SIEM/EDR solutions and enriching simulation results. With this module (available for each attack module) users will be able to identify the logs/alerts generated in an automated way. All the communications to SIEM/EDR systems area from the Picus Integration agent, which can be installed in a customer’s environment.

- **SIEM Integration:** The Picus Platform integrates with SIEM tools through their APIs to validate that that log sources are being ingested and that correlation rules are in place to trigger alerts when security events are identified.
- **EDR Integration:** The Picus Platform integrates with EDR tools through their APIs to validate that the most relevant endpoint data is being captured and analyzed and that detection rules and watchlists are in place to detect attacks (and that they also trigger reliably).

## Supported Integrations

### SIEM

splunk>

IBM Security QRadar

Microsoft Azure Sentinel

CyberRes ArcSight

securonix

elasticsearch

### EDR

Microsoft Defender for Endpoint

vmware Carbon Black

CROWDSTRIKE

SentinelOne

**Note:**
More integrations are added regularly. Please contact us if you wish to see other vendors in this list.

# About PICUS

At Picus Security, we help organizations to continuously validate, measure and enhance the effectiveness of their security controls so that they can more accurately assess risks and strengthen cyber resilience.

As **the pioneer of Breach and Attack Simulation (BAS),** our Complete Security Control Validation Platform is used by security teams worldwide to proactively identify security gaps and obtain actionable insights to address them.

picussecurity