PICUS

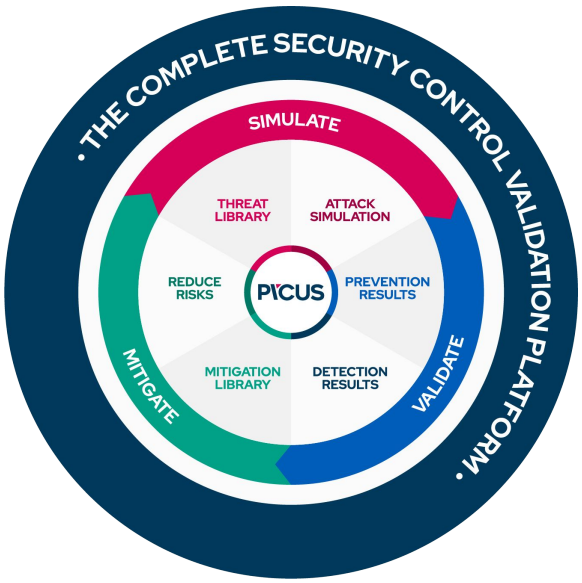
# TECHNOLOGY SOLUTION BRIEF

April 2022

## Overview

**The Picus Complete Security Control Validation Platform** leverages Breach and Attack Simulation (BAS) technology to validate security controls in a continuous and risk-free way. It also provides actionable mitigation recommendations, which enable organizations to quickly and effectively address threat prevent and detection gaps.

- **Simulate:** Simulate real-world threats against your networks, endpoints, and cloud-based security controls.
- **Validate:** Validate the effectiveness of your prevention and detection security controls in order to identify and prioritize security gaps.
- **Mitigate:** Leveraging vendor-specific mitigations and best practices to harden security controls.



# Table of Contents

# Platform Benefits

- ✔ Validates preparedness against the latest threats
- ✔ Tests controls continuously, 24/7
- ✔ Optimizes prevention and detection capabilities
- ✔ Evidences security effectiveness and value of investments
- ✔ Enhances SOC efficiency and effectiveness
- ✔ Aids security decision making and prioritization
- ✔ Operationalizes MITRE ATT&CK

## Primary Use Cases

### Security Control Validation

Validate that your security controls provide the protection you need to defend against the latest cyber threats.

### Security Posture Management

Determine your level of security risk at any moment and avoid assumptions.

### Security Control Rationalization

Maximize the value of existing investments and ensure that new ones deliver the value you expect.

### Enhancing SOC Effectiveness

Increase the effectiveness and efficiency of SOC controls and processes to reduce the time it takes to detect and respond to threats.

### Compliance Enablement

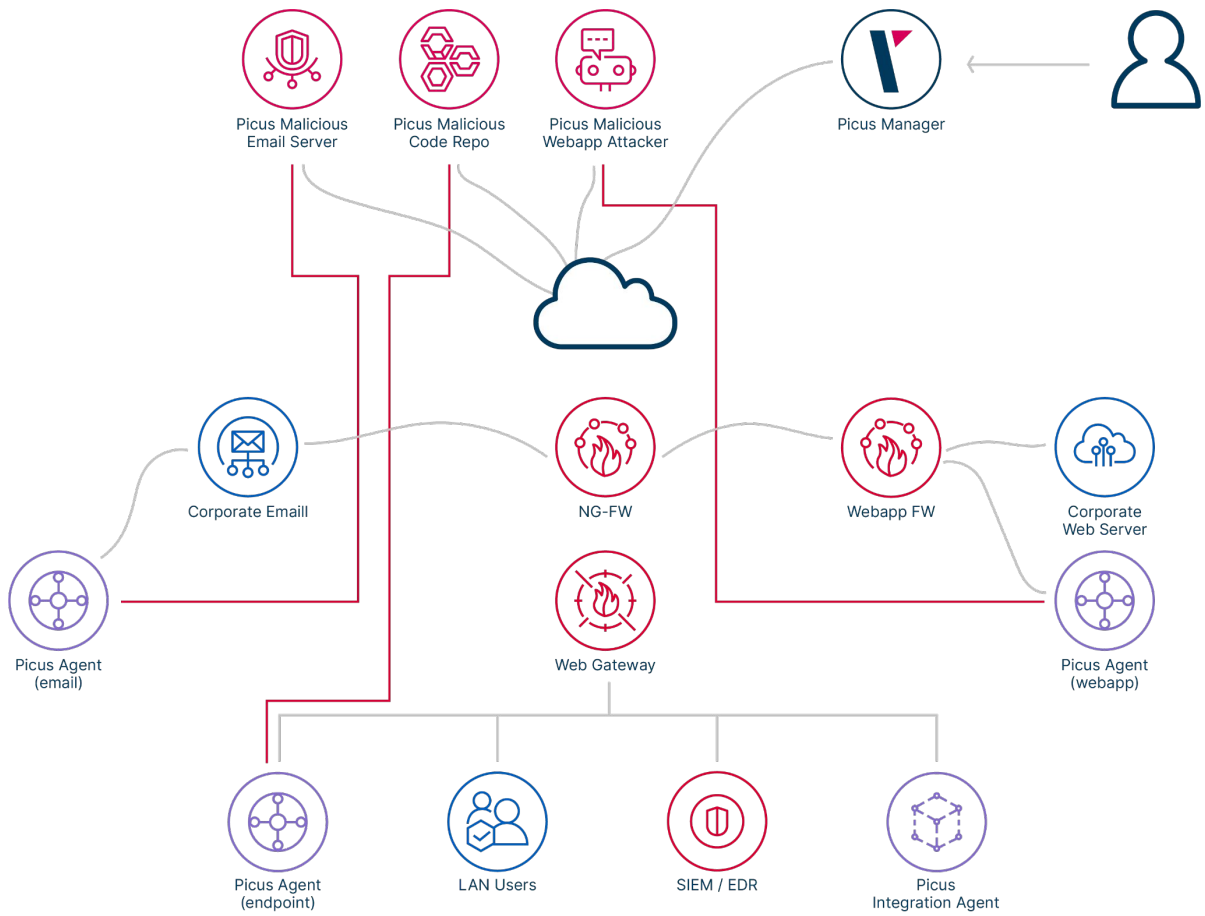
Achieve a proactive approach and demonstrate that you comply with the latest regulations and standards.

# How It Works

## 1. Our Approach to Attack Simulation

To validate security controls, The Picus Platform does not require agents to be installed on each and every endpoint/server/device in your network. Validating security controls actually means validating the security policies of the security controls. Therefore, Picus needs only one endpoint system with a policy assigned to it to validate the same security policy used across thousands of endpoints. In the example of a 1,000 endpoint and server infrastructure, if there are only three endpoint policies - for standard-users, privileged-users and servers - then Picus needs only three agents (deployed on endpoints with respective policies) to validate the effectiveness of endpoint security controls. Deploying three agents is recommended for validating the controls in a continuous manner. However, for what-if-based assessments where one-time visibility is sufficient , a single agent can be moved within a network to assess different scenarios.

The diagram below is a sample topology which shows how Picus Agents can be deployed in production environments to validate network, email, and endpoint controls.



# How It Works

## 2. How Picus Attack Simulation Modules Work

### 2.1. Network Infiltration

**Definition:** This module is designed to infiltrate malicious payloads through HTTP/S from The Picus Manager to the Picus Agent.

**Aim:** To validate that malicious codes infiltrated are prevented/detected by network and/or endpoint security controls.

**Form-factor:** This module needs a Picus agent to initiate malicious files downloads from The Picus Manager. Users can leverage Browser and Endpoint simulation agents to run infiltration attack simulations.

Browser-run simulations can be performed on-demand by logging into The Picus Platform. Users can leverage endpoint simulation agents to schedule simulations and execute them on-demand.

**Security:** Malicious code samples do not harm the system as Picus Agents do not execute these malicious codes but immediately destroy them once they are delivered to the agent.

### 2.2. Email

**Definition:** This module is designed to deliver malicious payloads by email from the The Picus Manager to the Picus Agent.

**Aim:** To validate that malicious email attachments and links are prevented/detected by email security controls.

**Form-factor:** The module requires malicious emails to be sent to a dedicated inbox (such as picus@company.org). Users can leverage two methods to monitor the inbox against malicious email delivery; by configuring an Endpoint simulation agent to check the inbox or by creating an email forwarding rule to direct incoming emails to a Picus provided inbox.

**Security:** Malicious code samples do not harm the system as Picus agents do not execute these malicious codes and they are immediately removed once delivered to the inbox.

## 2. How Do Picus Attack Simulation Modules Work?

### 2.3. Web Application

**Definition:** This module is designed to deliver web application attack techniques through HTTP/S from The Picus Manager to The Picus Agent.

**Aim:** To validate that malicious webapp requests are prevented/detected by Web Application Firewalls and detection controls.

**Form-factor:** This module requires an agent to mimic a webserver by listening port TCP80/443 and respond to requests sent by The Picus Manager. For The Picus Manager to establish connection with the agent, the agent requires a public IP address. This requires a NAT rule to be defined on the infrastructure and that real IP to be defined on The Picus Platfom. In case endpoint firewall enabled on the agent OS, Picus Agent has a helper script to create an exception on Windows Firewall. Please check Picus' Support Portal for more information.

**Security:** Picus Agents do not host any web pages or accept connections from non-Picus assets. To further decrease the attack surface, it is possible to only publish Picus Agents to IP addresses of The Picus Manager.

### 2.4. Endpoint

**Definition:** This module is designed to simulate scenario attacks in order to assess whether endpoints are effective at preventing and detecting the most commonly used MITRE ATT&CK techniques

**Aim:** To validate that scenario attacks are prevented and/or detected by endpoint security controls.

**Form-factor:** Scenario attacks are simulated by Windows-based attack agents. Users can optionally provide credentials on agents in case they need privilege-requiring attacks to be simulated.

**Security:** Each scenario attack is made up of atomic adversary techniques (mapped to MITRE ATT&CK. Scenarios do not run any malicious code but notepad-like "safe" apps to prove code execution. A Picus agent runs each scenario followed by clean-up functions to restore the endpoint's operating system to the last known state.

## 2. How Picus Attack Simulation Modules Work

### 2.5 Data Exfiltration

**Definition:** This module is designed to exfiltrate sensitive data in different formats through HTTP/S.

**Aim:** To validate that exfiltration of personal and financial data is prevented/detected by network and detection security controls.

**Form-factor:** Data Exfiltration attacks are simulated by Windows-based attack agents. Support for Linux and MacOS agents is coming soon.

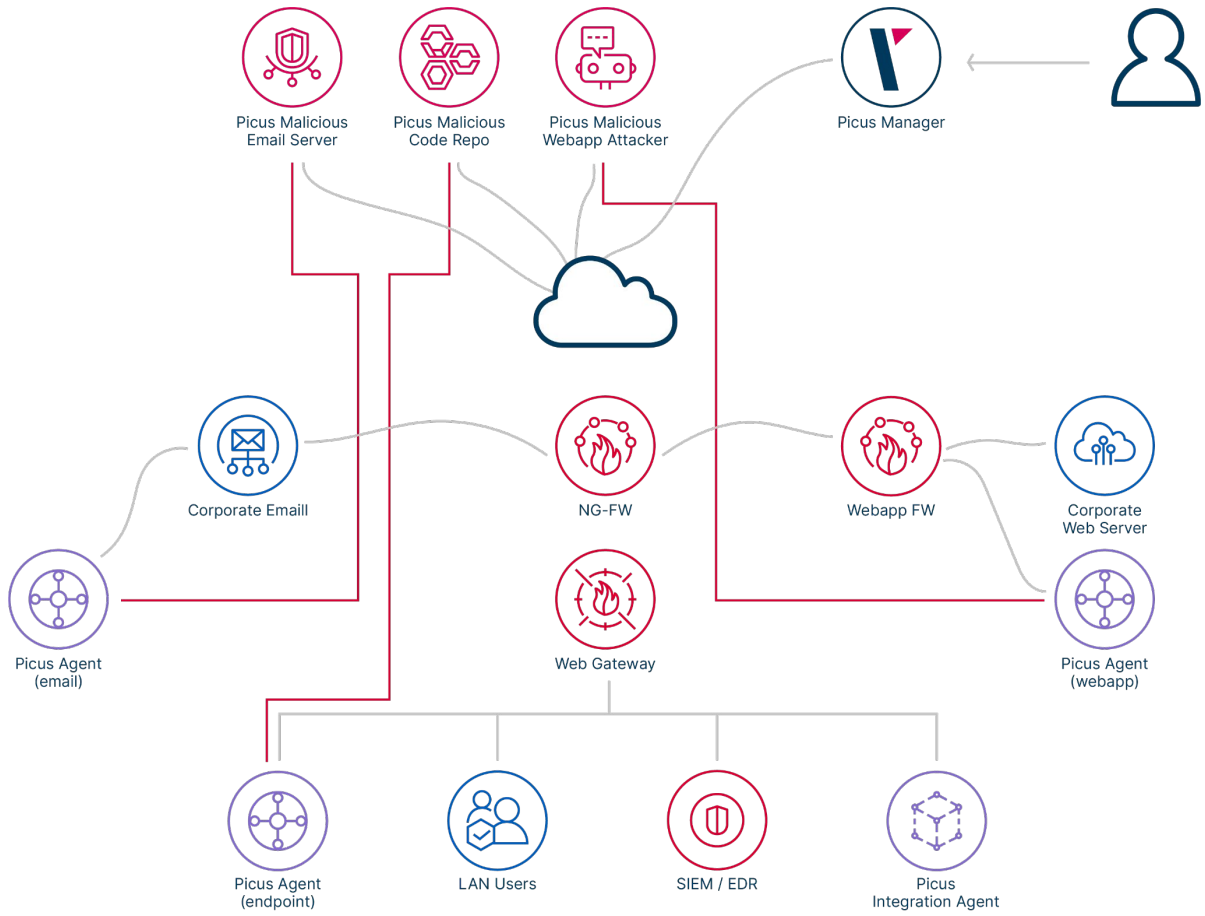
**Security:** The Picus Data Exfiltration module evaluates the effectiveness of Data Loss Prevention Solution to prevent the exfiltration of critical information. It does this by employing multiple methods of extraction used by internal and external threat actors.

# How It Works

## 3. Detection Analytics

To validate the effectiveness of Security incident and Event Management (SIEM) and Endpoint Detection and Response (EDR) tools, The Picus Platform also offers optional Detection Analytics. To active Detection Analytics on each attack simulation module listed in section 2, an additional license must be obtained.

To deploy Detection Analytics, an integration agent must be deployed to enable The Picus Platform to query and analyse SIEM and/or EDR logs/telemetry and alerts generated as a direct result of attack simulations.



# FAQ

## 1. What is the user data processing policy of Picus?

Picus Security prioritizes information security extremely highly and holds ISO 27001 and SOC 2 certifications. Our security program is designed to address privacy risks related to personal information. All user-related data collection processes have privacy at the center by design and by default. Picus does not share with any third parties any user-related data.

Customer-specific data can only be accessed at the request and consent of customer for troubleshooting purposes and such requests are restricted to authorized support-operations personnel only. Picus is using state-of-art technologies to provide reliability and security. Below are the processes that leverage anonymous user-related data:

- Picus anonymously collects software usage data from which statistics are created to analyze and improve user experience. It's not possible to identify users or customer accounts from anonymized data points. This process is designed to comply with GDPR requirements.
- Picus anonymously collects assessment results to improve Attack Research and Mitigation Recommendation processes. Aggregated results may also be used for marketing purposes. It's not possible to identify users or customer accounts from anonymized data points. This process is designed to comply with GDPR requirements.

## 2. What security measures does Picus have in place to protect data?

Picus Security gives top priority to protecting data and holds ISO 27001 and SOC 2 certifications as evidence of an active and continuously improving security program. Below are some highlighted measures that are in place to protect user data. For more information please write to security@picussecurity.com.

**Protection of data at rest**

The Picus Platform stores and processes customer data in isolation via AWS provided system boundaries. The data hosted on The Picus Platform is encrypted using the industry-standard AES-256 algorithm.

The Picus Platform stores the following data: login credentials, settings and assessment results. The data is backed up using the same encryption algorithm used for operational storage.

# FAQ

## 2. What security measures does Picus have in place to protect data?

Agents are stateless processes; no customer-related data is stored within them. Agents are also subject to the aforementioned encryption scheme to protect any sensitive data that may possibly reside in system logs.

All data is retained indefinitely as long as the customer has a valid and active Picus License in place. In certain situations like degradation of performance, Picus may archive a portion of the least recently used/generated data but only with the approval of customers.

**Protection of data in motion**

Picus uses Communication Channel and Attack Channel terms to define the communication patterns among Picus components. Communication Channel covers all communications among Picus Platform and Agents. It is used for attack scheduling, collecting attack results, and identifying the status of the Agents within the system. Attack Channel is where scheduled attacks and heartbeats are delivered among Agents.

Within the Communication Channels, all communications are initiated from Agent to the Platform. Picus Platform does not initiate connections to the Agents. All Communication Channel traffic is encrypted by HTTPS where 2048 bit RSA and TLS v1.2 are used by default.

As Attack Channel is only used for delivering malicious payloads, there is no user information that needs to be protected here. Therefore Attack Channel utilizes several protocols via both encrypted and clear-text methods.

## 3. How can I access knowledge base articles and open support tickets?

To access support materials and contact Picus Security's Customer Support Team, please visit our dedicated support portal at https://support.picussecurity.com

# FAQ

## 4. Are Picus simulations safe?

Yes, totally. The Picus Platform simulates real-world threats but by conducting attacks via dedicated( close-loop) connections there is no risk of damage and disruption to production environments. Picus agents have static IP addresses. Attacks from addresses assigned to Picus can therefore be treated as simulations.

## 5. Does Picus collect any confidential or proprietary information from customer environments?

No. The Picus Platform does not communicate with company assets and therefore does not collect or store any customer information. Picus agents communicate only with each other.

## 6. How is the Picus Threat Library created and maintained?

The Picus Labs team closely monitors the threat landscape, leveraging a wide range of threat intelligence sources and conducting digital forensics to identify and analyze new tactics, techniques and procedures (TTPs). Whenever a significant new threat, vulnerability or adversarial technique is identified, Picus' SLA is to ensure a simulation is added to the platform's threat library within 24 hours.

The Picus Threat Library includes:

-Malware attacks
-Email attacks
-Vulnerability exploitation attacks
-Web application attacks
-Endpoint attacks
-Data exfiltration attacks

# 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