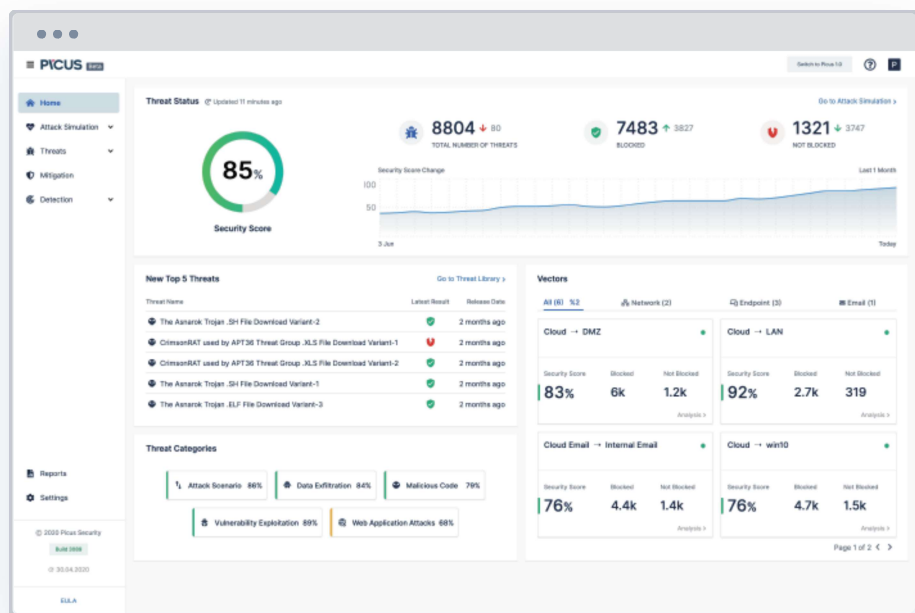


## SECURITY CONTROL VALIDATION & MITIGATION

Threat-centric, pervasive, flexible end-to-end security validation

Today's security leaders face a herculean task: maintaining a hard baseline against ever evolving cyber threats, while balancing requirements and investment. Modern cyber security stacks are often complex, but hardly gap-free. While security analysts try to weather a storm of threat intelligence coming from multiple sources, skills and resources are required to turn huge amounts of data into concrete tactics to validate security effectiveness. The foundation of readiness is frequent testing and validation. With all these tools and responsibilities, how often do you ask yourself "am I secure?"

Picus Security Control Validation and Mitigation is a threat centric, flexible platform that allows to measure security effectiveness and quickly assess controls, automatically and consistently identify gaps, and instantly apply selected mitigation advice for the purpose of security validation, hardening and mitigation. The platform is powered by an extensive Threat Library curated by Picus Labs, and a broad set of mitigation advice coming from the Picus Technology Alliance Network.



### HIGHLIGHTS

- **Maximise ROI**  
Utilise your security investments at their maximum. Manage your security estate effectively.
- **Automated and consistent validation**  
Streamline the validation process through automatic, continuous and pervasive security testing.
- **Elevate the quality of the visibility insight**  
Monitor your security posture through consistent and continuous validation.
- **Speed up mitigation and change management**  
Automate and speed up security policy and signature management.
- **Empower your teams with threat-centric validation**  
Leverage on the Picus Threat Library and benefit from constant vigilance and awareness of the global threat landscape for timely and precise operations.



### THREAT EMULATION BASED ON THE MOST EXTENSIVE THREAT LIBRARY

By undertaking global threat watch, imminent threat analysis and commonality evaluation processes, Picus Labs maintains a proprietary Threat Library around the clock and provides thousands of curated, indicative real-world threat samples and scenarios. All content is tied to MITRE ATT&CK with over 90% coverage.



### FAST DEPLOYMENT, EASY MANAGEMENT

The Picus Platform engine assesses the readiness level of network, web application, endpoint and email security controls in production networks, either while operating 24x7 or on-demand when required. Picus is categorically safe, technology agnostic, requires limited deployment effort and fully automated.



### VENDOR-SPECIFIC MITIGATION FOR PRECISION AND SPEED

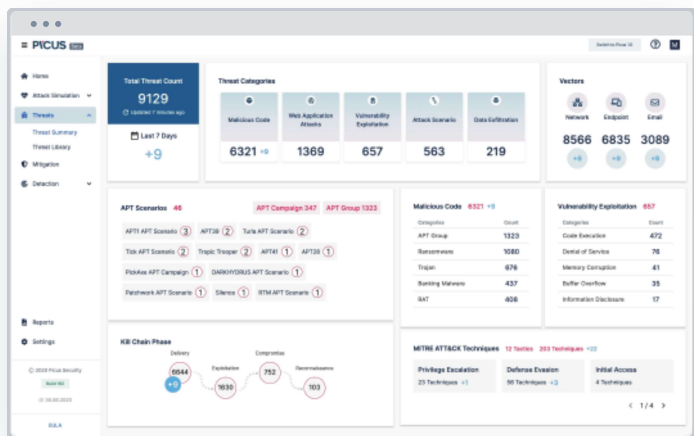
Picus Mitigation Library carries technology-specific security policy insights. Laser-focused mitigation advice from our Technology Alliance Ecosystem can be applied to alliance vendors for rapid remediation. Solutions include next-generation firewall, network intrusion prevention systems, and web application firewalls.

## HOW IT WORKS

The Picus Security Control Validation and Mitigation solution consists of Picus Threat Library, Threat Emulation Module, and Mitigation Library. While the Threat Emulation Module continually collects adversarial content from the Threat Library and runs assessments, the Mitigation Library reveals available signatures and policies developed by the vendors to address the identified security control gaps.

### PICUS THREAT LIBRARY

Picus Threat Library contains thousands of daily-updated malware, vulnerability exploits, web application attack samples, and atomic adversarial techniques selected via commonality evaluation of global threat watch data. Hundreds of nation-state and vertical driven attack scenarios are included. Content is mapped to the frameworks of MITRE ATT&CK, Cyber Kill Chain, and OWASP and presented in relation to targeted applications, targeted operating systems, severity level as well as Common Vulnerabilities and Exposures/Common Weakness Enumeration (CVE/CWE) references. Through the Threat Library, users find samples of the most recent adversarial techniques at their fingertips, allowing them to stay ahead of newest threats, saving the hassle of setting up and maintaining an in-house repository. SOC analysts, threat hunters and incident responders, security operations teams, red team and pen-testers can utilize this granular content for various testing scenarios.



### PICUS MITIGATION LIBRARY

While Picus Labs' Red Team adds new adversarial content to the Threat Library, the Blue Team examines the solution inventory of Picus' technology partners to enrich each threat and technique sample with mitigation alternatives. New threats and associated mitigation alternatives are added daily.

Picus Mitigation Library provides vendor-specific policy insights for the following categories: network security controls, next-generation firewall, network intrusion prevention systems, web application firewalls, Endpoint Detection & Response (EDR) solutions, SIEM platforms.

## TECHNOLOGY ALLIANCES

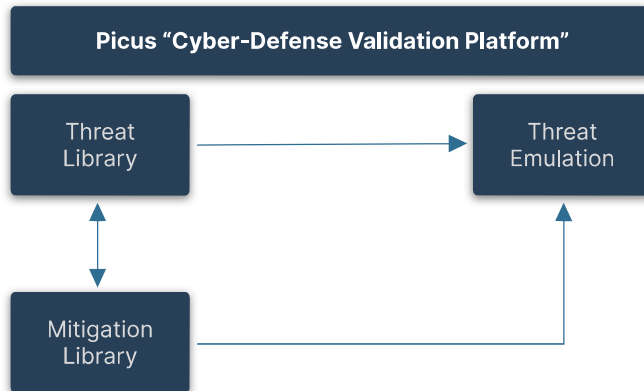
### NETWORK SECURITY



### SIEM



### EDR



### PICUS THREAT EMULATION MODULE

Picus Threat Emulation Module is the pivotal piece of the Picus Platform, bridging your defensive capabilities with the largest adversarial library available and with the Mitigation Library for eliminating risks quickly.

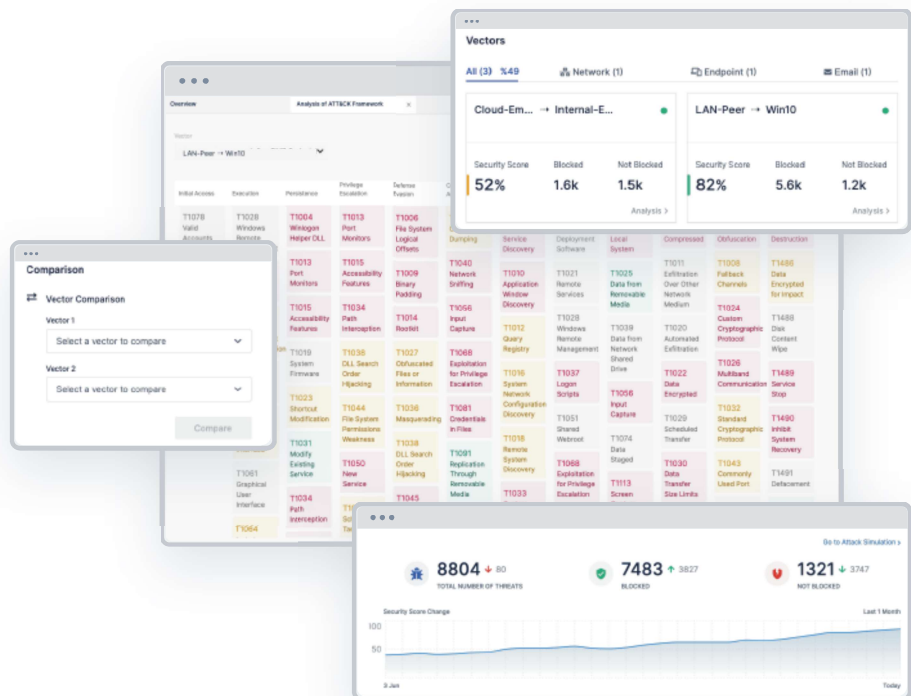
The Threat Emulation Module assesses the "readiness level" of network, web application, endpoint, and email security controls in production networks, either while operating 24x7 or on-demand for red team practices. The emulation module can be configured over multiple attack vectors simultaneously and can process thousands of adversarial scenarios from the Picus Threat Library across your whole defensive estate, cloud based or on-premise, in a matter of hours.

Picus assessments are categorically safe, technology agnostic, and require limited deployment effort. Emulated attacks are run between agent peers. Each Picus peer has the capability of taking the attacker or victim side of the emulation based on the scenario, significantly simplifying the deployment requirements. The validation output collected by Picus is presented in real time and in retrospect, distilled as security scoring and threat-based checks (blocked vs unblocked threats) and drives prevention advice and mitigation actions.

Picus Threat Emulation Module has an easy to use and functional user interface.

## KEY USABILITY FEATURES

- Executive level reporting.
- Advanced notification features on sudden success rate drop situations.
- Easy navigation among different attacks vectors.
- Advanced historical and vector-based comparisons.
- Enriched threat or technique information visibility containing CVE, CWE, OWASP, cyber-kill chain, MITRE ATT&CK references, hash information, targeted operating systems, targeted applications and others.



## USE CASES



### FOR SECURITY LEADERS

- Build cross-departmental defense capabilities through clear-cut cyber-attack readiness visibility.
- Manage cyber-security function based on attack readiness based metrics and KPIs.
- Help answer questions on the readiness status about the threats covered publicly.

- Support budget discussion with evidence on limitations and explain cybersecurity risk in the business context.
- Demonstrate the value delivered by cybersecurity operations against a stream of adversarial activities.

- Empower cyber-security teams by giving them the toolset for uncovering new configuration requirements against the changing adversarial landscape instantly.
- Reveal systemic shortcomings such as poor service quality, network flaws, new employee onboarding shortcomings, aged technologies, and others.



### FOR SOC MANAGERS

- Gain granular and technology-related visibility on security control gaps.
- Empower threat hunters and incident responders by providing real threat samples and specific validation capacity.



### FOR SecOps MANAGERS

- Build, sustain, and harden the security baseline across the security controls such as next-generation firewall, intrusion prevention systems, web application firewalls, email gateways, and endpoint controls.
- Respond to emerging threats quicker and speed up change management during mitigation operations.



### FOR RED TEAMERS

- Automate the test process using the readily available threat samples and attacker and victim attributes.
- Apply larger number of test scenarios in a given time frame.
- Gain flexibility in delivering continuous and on-demand assessments.

## REQUIREMENTS

### Picus Manager

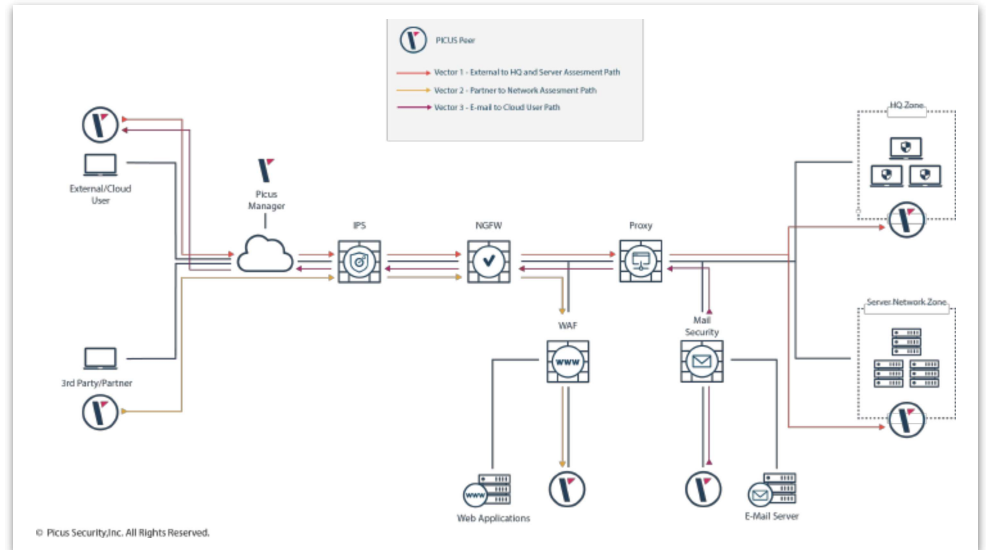
VMware ESX/i 5.1 or later. Hyper-V Server 2008 and later. Physical Servers: Any hardware supporting CentOS 7 x64 (minimal installation).

### Picus Network and Email Peer

VMware ESX/i 5.1 or later. Hyper-V Server 2008 and later. Physical Servers: Any hardware supporting CentOS 7 x64 (minimal installation).

### Picus Endpoint Peer

Supports Windows 7 SP1, Windows 8.1, Windows 10, Windows Server 2012 R2 and Windows Server 2016 with .NET Framework 4.5.2 or above.



## DEPLOYMENT COMPONENTS

**Picus Manager** – provides an easy-to-use web user interface from which Picus assessments and reports are managed.

**Picus Network and Email Peer** – A vector defines the network path followed by an attack. Any vector terminates in two peers (an attacker and a victim). A network peer can be selected either as a victim or attacker peer.

**Picus Endpoint Peer** – Simulation peer to test endpoint security. It can only be configured as a victim peer.

**Picus Integration Peer** – provides integration with security solutions/systems in the customer environment for Picus Security modules.

## DEPLOYMENT OPTIONS

**Picus Manager** – Available as HyperV and VMware virtual images or also available on physical/virtual servers which support CentOS 7 x64.

**Picus Network and Email Peer** – Available as HyperV and VMware virtual images. It is also possible to install Picus Peers on physical servers and PCs which support CentOS 7 x64.

**Picus Endpoint Peer** – Runs on Microsoft Windows. Picus does not distribute any Endpoint Peer image. It is expected that Endpoint Peer is to be installed on an instance of the organization's Windows golden image.

**Picus Integration Peer** – Available as HyperV and VMware virtual images. It is also possible to install Picus Peers to physical servers and PCs which support CentOS 7 x64.