

# Netsurion and MITRE ATT&CK Framework

## Use real-world adversary techniques to better detect cybersecurity threats

### Overview

With cyber criminals spending an average of 127 days in an organization's environment, cyber threats require rapid detection and elimination to reduce costly damage. Threat groups and nation-state attackers often use distinct tactics and techniques that signify attempted compromise. These unique adversary tactics and techniques are compiled in a repository called the MITRE ATT&CK® knowledge base, but implementing it on your own can be complex and time consuming.

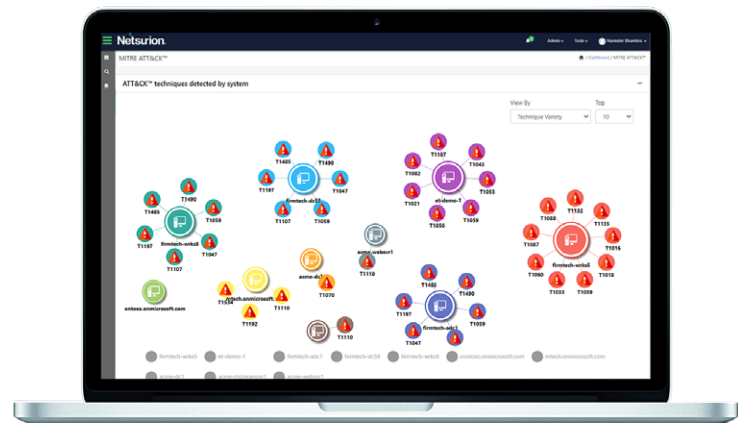
Netsurion integrates this database of known adversary techniques into our platform to accelerate threat detection and incident response. ATT&CK enables organizations of all sizes to fortify their defenses and stop similar attack techniques in the future.

### What is ATT&CK and How it Helps

Developed by MITRE, the ATT&CK framework is based on real-world observations. The framework's descriptions of tactics, techniques, and procedures (TTPs) enable security defenders to identify relationships between individual observations and known threat actors.

Mapping the MITRE ATT&CK knowledge base with the Netsurion solution improves threat hunting and comprehensive discovery of ongoing attacks. This threat intelligence is available in the Netsurion console for better visibility and threat enrichment.

Our managed solution with its 24/7/365 security operations center (SOC) monitoring enables you to prioritize your most concerning alarms, detect hidden threats, and identify advanced risks that could lead to a data breach.



### Benefits

- Creates a common language for describing attack patterns which simplifies information sharing
- Provides better detection and investigation advantages in the first critical moments of an incident
- Integrates with Netsurion to block adversary actions
- Updates adversary knowledge over time as the threat landscape evolves
- Improves rapid cybersecurity decision making

### How it Works

**Step 1:** Correlates your Netsurion log data with the MITRE ATT&CK knowledge base.

**Step 2:** Provides the ATT&CK dashboard within the Netsurion console with detected adversary techniques.

**Step 3:** Continues to monitor for ATT&CK techniques within your organization for further investigation and threat hunting.

**Step 4:** Enables defenders to prioritize investigations and respond to threats more quickly and with better accuracy.

## Features

### Risk Management

- Prioritize threats earlier in the cybersecurity lifecycle
- Tailor threat response to industry threats and actual security gaps
- Protect your organization from future threats that use known exploits

### Detection and Dashboards

- Identify patterns and TTPs quickly to pinpoint suspicious behavior
- Provide drill down capabilities such as the Netsurion ATT&CK Techniques Detected by System; Netsurion ATT&CK Timeline; and ATT&CK Navigator™
- Offer multi-tenant capabilities for MSPs and very large enterprises

### Real-Time Alerting

- Enrich threat intelligence context with actual techniques used by hackers
- Detect anomalous behavior with machine learning, threat intelligence, the ATT&CK knowledge base, and Netsurion's 24/7 SOC analysts

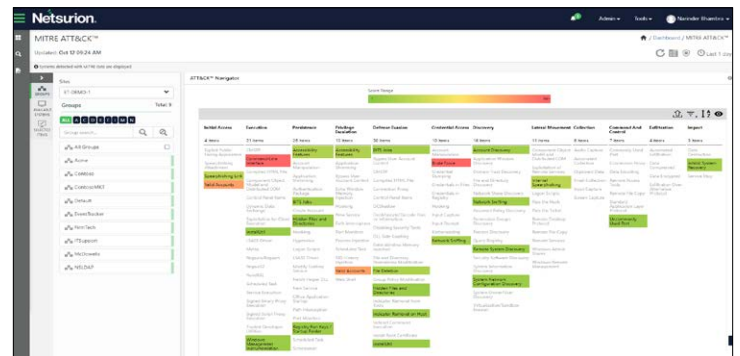
### Simplicity and Ease of Use

- Incorporated into the Netsurion one-stop-shop console
- Pivot to MITRE's ATT&CK website for more in-depth insights on adversaries, techniques, and remediation steps
- Provide techniques and adversary behavior against popular platforms such as Microsoft 365, Microsoft Defender for Identity (formerly Azure ATP), and Amazon Web Services (AWS)

### Technical Specifications

- Netsurion 9.3 or higher

The integration of the MITRE ATT&CK framework into Netsurion provides insights for a range of users in your organization. IT and security analysts with practitioner responsibilities benefit from the hands-on visibility in the Netsurion console. The threat intelligence enrichment based on actual adversary techniques helps further detection and prioritize which exploits to investigate.



Organizational executives can utilize ATT&CK to understand adversaries in your industry better and to identify gaps in protection and security maturity. Your entire company benefits from the intuitive dashboard and single-pane-of-glass visibility that save time in operational security and increases effectiveness in early threat detection.

### MITRE ATT&CK Overview

The MITRE Company is a not-for-profit organization that provides practical solutions to make the world a safer place. It operates federally-funded research and development centers across the United States.

The MITRE ATT&CK framework covers over 133 threat actors and hundreds of their distinctive threat techniques. ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) is continuously updated, providing you with more effective defense, detection, and remediation.

Businesses, government agencies, global partners, and vendors widely adopt ATT&CK as a methodology to inform defenses and share threat intelligence.

Learn more here: [www.attack.mitre.org](http://www.attack.mitre.org).