Executive Summary

Imagine this: You understand all the ways cyber attackers can threaten your organization. You know what to do about them, and you’re ready.

It’s not a dream. Companies of all sizes use MITRE ATT&CK to understand precisely how threat actors operate. And they rely on Cisco Security to take action and be prepared.

Cisco Security defends your organization from threats documented in ATT&CK. In this paper, we mapped our solutions to ATT&CK with relevant, supporting detail so you can make informed decisions about cybersecurity investments. Discover for yourself the breadth and depth of our coverage and capability in the context of ATT&CK.

With unrivaled threat intelligence and an industry-leading zero trust approach, Cisco helps you attain effective security to face known threats that MITRE discovered -- and tomorrow’s evolving threats.
ATT&CK Background:

Already know a thing or two about ATT&CK? Then feel free to skip this section. Otherwise, here’s what you need to know. MITRE Corporation says that ATT&CK is “a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.” They trademarked ATT&CK™ to abbreviate Adversarial Tactics, Techniques, and Common Knowledge. It’s available for free to everyone.

Here’s how they did it. Since 2013, MITRE researchers investigated numerous methods (tactics, techniques, procedures) that cyber attackers use to compromise and breach critical systems. Then they organized and cataloged them in ATT&CK Matrices, ranging from attackers’ first steps to their ultimate goal: impact on mission critical systems or mobile devices. ATT&CK Matrices provide clear, structured ways to understand how attackers work. And MITRE continues to update ATT&CK on a regular basis.

MITRE published four ATT&CK matrices so far.

- **ATT&CK Enterprise**, covering threats against Cloud, Windows, Linux, and macOS systems
- **ATT&CK Mobile**, covering threats against Apple iOS and Android devices
- **ATT&CK ICS**, describing how attackers operate on Industrial Control System networks
- **Pre-ATT&CK**, covering the ways attackers prepare before they launch attacks

Att&CK takes the reverse approach: Instead of highlighting proven security controls, ATT&CK focuses on attackers’ behaviors. For example, the CIS Controls is a cyber best practice that recommends **controlled use of administrative privileges** as a protection against cyberattacks. Conversely, ATT&CK describes **account manipulation** behavior that attackers use to maintain unauthorized access and remain undetected.

ATT&CK doesn’t stop there. It also provides **mitigation** approaches for each method of attack so that you can prepare for them. However, ATT&CK mitigations do not prescribe any specific products or services that can help -- it’s up to you to figure out what you’ll need. And it doesn’t prioritize anything, so deciding where you start is your responsibility too.

**Don’t worry. This paper makes it easier to understand and act on ATT&CK.**

Read on. You’ll see how Cisco Security products and services align with the MITRE ATT&CK Enterprise Matrix. And skip around: this is more like a reference document than a traditional whitepaper. Read only the sections you need.
What you will learn

This paper aligns Cisco Security products and services with the MITRE ATT&CK Enterprise Matrix so that you can make informed decisions on cybersecurity investments. MITRE published this article for questions you should ask anyone who says they're using ATT&CK, so we structured this paper according to their advice.

Therefore, you'll learn:

- Why we’re using MITRE ATT&CK
- How we’re mapping our capabilities to ATT&CK
- The strengths and weaknesses of our approach
- How we plan to update our ATT&CK mappings
- The level of detail to which we map to ATT&CK
- Our solutions’ specific capabilities mapped to ATT&CK with supporting statements

Remember that we intentionally limited the scope of this paper to ATT&CK Enterprise, but our extensive portfolio addresses other ATT&CK matrices as well. If you’re interested in ATT&CK Mobile, ATT&CK ICS, or Pre-ATT&CK, please talk with us. We can do much more than what’s discussed in this paper.

Why are we using ATT&CK?

Many organizations ask us about our capabilities in the context of ATT&CK. And if you’re using it too, then you’re probably familiar with the four common use cases that MITRE identified:

- Detection & Analysis
- Threat Intelligence
- Assessment & Engineering
- Adversary Emulation

No matter what your specific reason or use case, chances are you’ll need security technologies and/or services to accomplish your goals. That’s why we’re using ATT&CK: to educate you about our vast portfolio in its context. We’re also building ATT&CK knowledge directly into our products. For example, our new threat hunting capability in Cisco AMP for Endpoints helps uncover hidden threats faster with built-in queries that are cataloged and mapped directly MITRE ATT&CK. It combines our new Orbital Advanced Search technology with expertise from Cisco Talos to proactively find sophisticated threats.

How are we mapping to ATT&CK?

In this article, MITRE reminds us that ATT&CK can help you improve your defenses. They also say, “if someone says they’re using ATT&CK, what does that mean?” Though MITRE describes mapping as the alignment of security capabilities to applicable Techniques, we take a different tack here:

This paper maps our solutions to Mitigations because they’re the specific advice from MITRE on how to act on threats. It focuses primarily on our Cisco Security solutions, but we aligned some capabilities from other areas of our portfolio as well. Please don’t view this paper as the final word on everything we do, though. It isn’t. Its scope is limited to the Enterprise Matrix.
What are the strengths and weakness of our approach?

Our approach is designed to help you act quickly on MITRE’s advice. ATT&CK helps you understand attackers’ behavior from high-level Tactics to specific Techniques (and Sub-Techniques) all the way down to highly detailed Procedures. Ultimately, though, Mitigations are the key. They are the action you need to take to improve your cyber defenses.

<table>
<thead>
<tr>
<th>The Advantages of Our Approach Are</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Faster Action.</strong> For each Mitigation, you’ll know exactly how we help. We make it easy to understand which Cisco solution to use and why. Sure, it’s important to understand how attackers behave, but it’s equally important (perhaps more so) to know how to defend against their methods.</td>
<td></td>
</tr>
<tr>
<td><strong>Simplicity.</strong> A single Mitigation can defend against several discrete Tactics, Techniques, and Procedures (TTPs), so mapping to Mitigations is much simpler. For example, the Multi-factor Authentication (M1032) Mitigation addresses 17 different Techniques like Account Manipulation (T1098), Brute Force (T1110), and Network Sniffing (T1040).</td>
<td></td>
</tr>
<tr>
<td><strong>Stability.</strong> The list of TTPs is very long and changes constantly, and the new Sub-Techniques bring even more changes. The Mitigations list is much shorter and changes less often. And remember, MITRE’s site maps Mitigations back to Techniques, so that work is already done.</td>
<td></td>
</tr>
<tr>
<td><strong>Supporting Detail.</strong> We didn’t just use checkboxes. We took the time to explain how and why our individual solutions support and align with each Mitigation.</td>
<td></td>
</tr>
</tbody>
</table>

MITRE’s Savvy ATT&CK Consumer article says: “Since ATT&CK has limitations, that means any method of using ATT&CK also has limitations. Since all approaches to using ATT&CK have pros and cons, we recommend asking what the limitations are to the selected approach. Some may feel that a disadvantage of this paper is that it doesn’t map to TTPs. If you’re one of them, then please talk to us. Our cyber experts will help with that level of detail.

How are we updating ATT&CK mappings?

ATT&CK is a living model that MITRE regularly updates, so we expect frequent changes too. We have also reviewed the new Sub-Techniques (currently in beta), and fortunately they don’t change our mapping approach based on Mitigations. We’ll continue to monitor MITRE’s progress over time, and we’ll learn from you about what’s important. Our portfolio doesn’t stand still either: We continue to add new capabilities to each and every one of our products. Therefore, we’ll view our document as a living model too, and we’ll revisit it periodically -- and we’ll summarize our own updates so they’re easy to spot.

What level of detail are we mapping to ATT&CK?

The MITRE blog suggests that mapping detail is based on the four levels of TTPs: Tactics, Techniques, Sub-Techniques, and Procedures. “You should ask what level of detail someone is using when they map to ATT&CK and why they chose that level,” they suggest. Recall that we discussed our mapping approach above, so we won’t revisit that rationale here.
As for the level of detail: the Mitigation Map section below explains how and why our solutions support ATT&CK. It’s not just a checkbox and or product name. We don’t want you to have to guess.

How do we offer more context about ATT&CK mappings?

Glad you asked! That’s the whole purpose of the Mitigation Map section below. It’s our detailed mappings between Cisco solutions and ATT&CK Enterprise mitigations with the context detail you’ll need for both the what and the how.

How much of ATT&CK do we cover?

“It is unrealistic for any single defensive product or service to cover all of ATT&CK,” MITRE writes, and we agree. We don’t cover 100% and we’d be suspicious too if anyone claimed complete coverage. But as you read through our Mitigation Map, you’ll see for yourself the breadth and depth of our portfolio -- and we’ll help you make focused cybersecurity investments that really matter.

So how much of ATT&CK do we cover? A lot. It’s probably not worth being more precise than that. Chances are you’re not buying new solutions to cover everything anyway. You probably have specific questions, and we have specific answers.

SecureX: Our Integrated Security Platform

Hopefully you’ve heard about SecureX. It connects the breadth of Cisco’s integrated security portfolio (reflected in this paper) and your entire security infrastructure for a consistent experience that unifies visibility, enables automation, and strengthens your security across network, endpoint, cloud, and applications. The result is simplified security, built into the solutions you already have.

MITRE ATT&CK, on the other hand, guides you down to highly specific, discrete adversary behavior. In other words, ATT&CK essentially “disintegrates” security by decomposing attackers’ behavior into very specific things. For example, from Privilege Escalation (Tactic) you learn how attackers use Process Injection (Technique) to access a legitimate process’s memory and gain elevated privileges. And APT37 (Procedure) explains how APT37 (a suspected North Korean cyber espionage group) -- injects its ROKRAT malware into the cmd.exe process on Windows.

To defend against Process Injection, MITRE offers two Mitigations:

• Behavior Prevention on Endpoint that recommends using endpoint security solutions to help block process injection from occurring, and
• Privileged Account Management that recommends using tools like Yama to restrict the use of ptrace to authorized users only

There’s no question that ATT&CK’s detail is incredibly useful to understand how attackers work. “Disintegrating” security in this way is a very good thing for cyber defenders. However, let’s not lose sight of how important an “integrated” security approach is to defend against the entire range of Enterprise ATT&CK: from Initial Access to Impact and everything in between. That's Cisco SecureX.
# Mitigation Map

## Mitigation Map Overview

- We listed ATT&CK Mitigations in alphabetical order.
- We placed MITRE’s Mitigation code number in parenthesis for each, and we link directly from the code number to the relevant section on MITRE’s site as well.
- Next we copied over MITRE’s mitigation description for handy reference.
- Then we explain how specific products and services in our portfolio support that Mitigation.
- We don’t expect you to read this section from beginning to end. If you’re interested in just a few Mitigations, then skip directly to those sections.

A short disclaimer: Just because we’ve listed a specific product or service under a Mitigation, we are not saying that it covers the Mitigation completely. We’re saying the solution helps accomplish the Mitigation, and how it helps. And there’s always so much more to say than a short paragraph, so please talk with us about any questions or clarifications you need.
Summary
The following table summarizes our mappings. The vertical axis shows each MITRE ATT&CK Mitigation and its identifier, and the horizontal axis shows Cisco capabilities. Green cells indicate where our capabilities align, and the remainder of this section explains why and how.

<table>
<thead>
<tr>
<th>ATT&amp;CK Enterprise Mitigations</th>
<th>Network</th>
<th>Cloud</th>
<th>Endpoint</th>
<th>App</th>
<th>SOC</th>
<th>CX</th>
</tr>
</thead>
<tbody>
<tr>
<td>M1036 Account Use Policies</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>M1015 Active Directory Configuration</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>M1049 Antivirus/Antimalware</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M1013 Application Developer Guidance</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M1048 Application Isolation and Sandboxing</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>M1047 Audit</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>M1040 Behavior Prevention on Endpoint</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>M1046 Boot Integrity</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>M1045 Code Signing</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M1043 Credential Access Protection</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>M1053 Data Backup</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M1042 Disable or Remove Feature or Program</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>M1055 Do Not Mitigate</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M1041 Encrypt Sensitive Information</td>
<td>✔ ✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>M1039 Environment Variable Permissions</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M1038 Execution Prevention</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M1050 Exploit Protection</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M1037 Filter Network Traffic</td>
<td>✔ ✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>M1035 Limit Access to Resource Over Network</td>
<td>✔ ✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>M1034 Limit Hardware Installation</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M1033 Limit Software Installation</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATT&amp;CK Enterprise Mitigations</td>
<td>Network</td>
<td>Cloud</td>
<td>Endpoint</td>
<td>App</td>
<td>SOC</td>
<td>CX</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------</td>
<td>-------</td>
<td>----------</td>
<td>-----</td>
<td>-----</td>
<td>----</td>
</tr>
<tr>
<td>M1032 Multi-factor Authentication</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
</tr>
<tr>
<td>M1031 Network Intrusion Prevention</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
</tr>
<tr>
<td>M1030 Network Segmentation</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
</tr>
<tr>
<td>M1028 Operating System Configuration</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
</tr>
<tr>
<td>M1027 Password Policies</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
</tr>
<tr>
<td>M1026 Privileged Account Management</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
</tr>
<tr>
<td>M1025 Privileged Process Integrity</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
</tr>
<tr>
<td>M1029 Remote Data Storage</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
</tr>
<tr>
<td>M1022 Restrict File and Directory Permissions</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
</tr>
<tr>
<td>M1044 Restrict Library Loading</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
</tr>
<tr>
<td>M1024 Restrict Registry Permissions</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
</tr>
<tr>
<td>M1021 Restrict Web-Based Content</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
</tr>
<tr>
<td>M1054 Software Configuration</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
</tr>
<tr>
<td>M1020 SSL/TLS Inspection</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
</tr>
<tr>
<td>M1019 Threat Intelligence Program</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
</tr>
<tr>
<td>M1051 Update Software</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
</tr>
<tr>
<td>M1052 User Account Control</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
</tr>
<tr>
<td>M1018 User Account Management</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
</tr>
<tr>
<td>M1017 User Training</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
</tr>
<tr>
<td>M1016 Vulnerability Scanning</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
</tr>
</tbody>
</table>
Account Use Policies (M1036)
Mitigation Description: Configure features related to account use like login attempt lockouts, specific login times, etc.

- **Duo** provides modern, effective multifactor authentication that helps eliminate the problem of brute force attacks on passwords. Duo controls application usage based on the trust established in user identities and the trustworthiness of their devices. It enables you to create adaptive access policies based on role, device, location, and many other contextual factors that help prevent accounts from being exploited.

- **ISE** secures network access through authentication and role-based authorization, and it integrates with multi-factor authentication solutions like Duo and RADIUS RFC-2865 compliant token servers to mitigate the risk of password-based attacks.

- **Cloudlock** is a cloud-native cloud access security broker (CASB) that protects user accounts from attackers. It uses advanced machine learning algorithms to detect anomalies based on multiple factors, and it identifies activities outside approved countries and spots actions that seem to take place at impossible speeds across distances.

Active Directory Configuration (M1015)
Mitigation Description: Configure Active Directory to prevent use of certain techniques; use SID Filtering, etc.

- **Security Strategy, Risk, and Compliance Services** can help you document your processes and identify any program and technology gaps. And we’ll recommend steps you can take to improve your cybersecurity profile.

Antivirus/Antimalware (M1049)
Mitigation Description: Use signatures or heuristics to detect malicious software.

- **AMP/Threat Grid** employs global threat intelligence, advanced sandboxing, real-time malware blocking, and advanced malware analysis capabilities to detect, contain, and remove malicious software.

- **Endpoint Security Analytics** delivers AnyConnect endpoint data to prebuilt Splunk analytics and dashboards that discovers threats such as zero-day malware, dangerous user behavior, and data exfiltration.

- **Encrypted Traffic Analytics** is a Cisco solution based on Stealthwatch and certain Cisco router, switch, and wireless LAN controllers that employs advanced network analytics and machine learning to discover malware threats encrypted traffic -- without the need for decryption.

- **Web Security** uses AMP technology to detect and block malware that originates from web browsing.

- **Email Security** uses AMP technology to detect and block stealthy malware in email attachments, or from emails that contain hyperlinks to malicious websites.

- **Duo** uses AMP technology to prevent infected devices from logging into your applications safeguarding against the spread of malware.

Application Developer Guidance (M1013)
Mitigation Description: This mitigation describes any guidance or training given to developers of applications to avoid introducing security weaknesses that an adversary may be able to take advantage of.

- **Security Strategy, Risk, and Compliance Services** help you document your processes and identify any program and technology gaps. And we’ll recommend steps you can take to improve your cybersecurity profile.

Application Isolation and Sandboxing (M1048)
Mitigation Description: Restrict execution of code to a virtual environment on or in transit to an endpoint system.

- **Threat Grid** combines advanced sandboxing with threat intelligence into one unified solution to protect organizations from malware. With a robust, context-rich malware knowledge base, you will understand
what malware is doing, or attempting to do, how large a threat it poses, and how to defend against it.

- **Tetration** uses approved-list application segmentation, behavior baselining, and detection of common vulnerabilities to quarantine affected servers before an incident causes damage. It secures workloads consistently across bare metal, virtual, and containerized workloads both on-premises and in the cloud.

**Audit (M1047)**

**Mitigation Description:** Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses.

- **Duo** checks devices for outdated, vulnerable operating systems or insecure configurations to prevent risky or potentially compromised devices from accessing critical applications and data. It enables adaptive access policies based on role, device, location, and other factors to respond to changing user context. Duo also lets you manually prevent logins: If a user loses their authentication device or reports it stolen, Duo lets you disable and disassociate the device from the user.

- **AnyConnect** checks devices for compliance with your security policy, working with ISE to prevent risky or potentially compromised or devices from accessing your network.

- **AMP** determines which endpoints have software with a specific Common Vulnerabilities and Exposures (CVE) entries, regardless of when the application last ran. You can then isolate endpoints that have critical vulnerabilities from the network before attackers can exploit them.

- **Tetration** detects common vulnerabilities and identifies application anomalies through process behavior deviations, allowing you to proactively quarantine affected servers before damage occurs. Its open policy model works across bare metal, virtual, and containerized workloads both on-premises and in the cloud.

**Behavior Prevention on Endpoint (M1040)**

**Mitigation Description:** Use capabilities to prevent suspicious behavior patterns from occurring on endpoint systems. This could include suspicious process, file, API call, etc. behavior.

- **AMP** blocks malware at the point of entry, provides visibility into file and executable-level activity, and removes malware from PCs, Macs, Linux, and mobile devices.

- **Tetration** identifies application anomalies through process behavior deviations, allowing you to proactively quarantine affected servers before damage occurs.

- **Security Connector** is an app for Apple iOS devices that offers visibility into network traffic and blocks connections to malicious sites -- wherever users go. It's the result of a close partnership between Cisco and Apple to strengthen security for mobile workers. People can easily mistype URLs or click on a phishing link within a message, leading them to malicious sites that compromise their devices. Security Connector prevents connections on both a DNS and IP address level, even over cellular networks and public Wi-Fi.

- **Duo** verifies the trust of any device. It identifies risky devices; enforces contextual access policies; and assesses, monitors, and reports on device health. Healthy devices reduce security risk, and Duo helps prevent devices from exhibiting suspicious behavior patterns on endpoints.

- **Cloudlock** uses APIs to manage the risks in your cloud app ecosystem, using advanced machine learning algorithms to detect anomalies. It also identifies activities outside approved countries and spots actions that seem to take place at impossible speeds across distances.

**Boot Integrity (M1046)**

**Mitigation Description:** Use secure methods to boot a system and verify the integrity of the operating system and loading mechanisms.
• **Security Strategy, Risk, and Compliance Services** can help you document your processes and identify any program and technology gaps. And we'll recommend steps you can take to improve your cybersecurity profile.

**Here are a few things we do to help ensure the integrity of our own products:**

• **Cisco IOS Software** is designed to prevent adversaries from compromising Cisco devices like routers. Learn more about [Cisco IOS Software Integrity Assurance](https://www.cisco.com/c/en/us/products/static-security/ios-security-integrity-assurance/index.html).

• **Cisco Trust Anchor Technologies** provide a highly secure foundation for certain appliance-based Cisco products. Capabilities include image signing, secure boot, and the Trust Anchor module -- a tamper-resistant, strong-cryptographic, single-chip solution that provides hardware authenticity assurance to uniquely identify the product. That way its origin can be confirmed to Cisco, providing assurance that the product is genuine.

**Code Signing** *(M1045)*

**Mitigation Description:** Enforce binary and application integrity with digital signature verification to prevent untrusted code from executing.

• **Tetration** calculates and tracks SHA-256 hashes for each running process. It cross-checks these hashes with knowledgebases like VirusTotal to discover potentially untrusted code in your critical workloads. Tetration significantly reduces the attack surface, minimizes lateral movement in case of security incidents, and more quickly identifies Indicators of Compromise (IOCs). Tetration collects rich telemetry from servers, applying machine learning, capturing processes executed on the server, including information about process parameters, start and stop time, process binary hash, and more.

**Credential Access Protection** *(M1043)*

**Mitigation Description:** Use capabilities to prevent successful credential access by adversaries; including blocking forms of credential dumping.

• **AMP** uses command line capture and its Exploit Prevention feature to block credential dumping on endpoints. And together with its Device Trajectory and File Trajectory capabilities, you gain visibility into events that precede and follow a compromise including parent processes, connections to remote hosts, and unknown files that may have been downloaded by malware.

• **IPS** has Snort signatures to identify and stop credential dumping tools like Mimikatz from entering your network.

• **ISE** manages passwords through its built-in RADIUS and TACACS+ authentication servers, enabling you to enforce strong passwords that hackers cannot readily crack. It also integrates with multifactor authentication solutions like Duo, RADIUS RFC-2865 compliant token servers, and others to mitigate the risk of successful credential dumping attacks. ISE also enforces network segmentation through Group Based Policy (formerly known as TrustSec) that limits the scope of credential dumping attacks, or block them entirely, as adversaries attempt to move laterally with stolen credentials.

• **Duo** multi-factor authentication can limit the damage caused by dumped credentials. Though an attacker may gain one authentication factor, the username and password, they won’t have the second factor and will be unable to exploit dumped credentials.

• **Stealthwatch** monitors network traffic for suspicious activity, like lateral movement that usually occurs after credential dumping attacks. It significantly reduces the time-to-detection for these types of attacks.

**Data Backup** *(M1053)*

**Mitigation Description:** Take and store data backups from end user systems and critical servers. Ensure backup and storage systems are hardened and kept separate from the corporate network to prevent compromise.
• **Cisco Data Protection Solutions** can help maintain the integrity of your data, giving you architectural simplicity, rapid scaling, operational efficiency, and our broad ecosystem of software partners offer proven data protection solutions for any size and type of environment.

**Disable or Remove Feature or Program (M1042)**

Mitigation Description: Remove or deny access to unnecessary and potentially vulnerable software to prevent abuse by adversaries.

- **AMP for Endpoints** blocked application feature prevents unauthorized applications from executing, disables vulnerable applications until patches have been applied, and limits use of specific files that you suspect but haven’t confirmed as malware.

- **Tetration** provides visibility into the installed software packages and their versions, patch level, and other data in its specialized dashboard. It checks this information against information-security vulnerabilities listed in the Common Vulnerabilities and Exposures (CVE) database and receives constant updates as new ones are found. When Tetration detects a vulnerability, it provides complete details including the severity and impact score. Security operations can quickly locate all instances of that vulnerable software and predefined policies can take specific actions, such as quarantining a host when servers have packages containing vulnerabilities.

**Do Not Mitigate (M1055)**

Mitigation Description: This category is to associate techniques that mitigation might increase risk of compromise and therefore mitigation is not recommended.

Even though MITRE suggests that it’s better not to mitigate some attack techniques and procedures, please share your concerns with our Security Strategy, Risk, and Compliance Services team. Leverage their experience and expertise at finding innovative solutions or compensating controls that can address the risks you face.

**Encrypt Sensitive Information (M1041)**

Mitigation Description: Protect sensitive information with strong encryption

- **AnyConnect Secure Mobility Client** provides highly secure remote access to the enterprise network, from any device, at any time, from any location. It supports strong encryption for data in transit, including AES-256 and 3DES-168, and next-generation encryption, including NSA Suite B algorithms and more.

- **NGFW and ASA** offer site-to-site VPN capabilities to secure data in transit.

- **Email Encryption** keeps your email secure and confidential. The Cisco Registered Envelope Service provides email encryption from the cloud, seamlessly securing your outbound messages with the most reliable email encryption algorithms available.

**Environment Variable Permissions (M1039)**

Mitigation Description: Prevent modification of environment variables by unauthorized users and groups.

Though Cisco Security solutions don’t prevent modification of Windows environment variables, please share your concerns with us. Our Security Strategy, Risk, and Compliance Services can help you document your processes and identify any program and technology gaps. And we’ll recommend steps you can take to improve your cybersecurity profile.

**Execution Prevention (M1038)**

Mitigation Description: Block execution of code on a system through approved/denied application lists and/or script blocking.
• **AMP for Endpoints Exploit Prevention** provides an integral preventative security layer for protecting endpoints, servers, and virtual environments from file-less and memory injection attacks, as well as obfuscated malware. It changes the static nature of the defense landscape to a dynamic one, making it more difficult for attackers to plan and execute successful attacks.

It also controls applications running on endpoints. Through its blocked applications feature, you can stop users from executing certain files without fully quarantining them. It prevents unauthorized applications from executing, disables vulnerable applications until patches have been applied, and limits specific files that you suspect but haven’t confirmed as malware. You can add any file hash (SHA-256 value) to a blocked applications list, but only executable files types will be prevented from opening.

• **Tetration** protects multi-cloud and on-premises workloads including virtual machines, bare-metal servers, and containers. Tetration uses machine learning, behavior analysis, and algorithmic approaches to offer this holistic workload-protection strategy, allowing you to contain lateral movement by implementing micro-segmentation, proactive identification of security incidents using behavior analysis, and reduction of the attack surface by identifying software-related vulnerabilities.

**Exploit Protection (M1050)**

**Mitigation Description:** Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring.

• **AMP for Endpoints Exploit Prevention** provides an integral preventative security layer for protecting endpoints, servers, and virtual environments from file-less and memory injection attacks, as well as obfuscated malware. It does so by changing the static nature of the defense landscape to a dynamic one, making it more difficult for attackers to plan and execute successful attacks. Exploit Prevention uses several technologies that work together to prevent, detect, and remediate malicious code at the endpoint.

The core in-memory prevention technologies include:
- Exploit Prevention which defends endpoints from memory attacks commonly used by obfuscated malware and exploits targeting software vulnerabilities of protected processes.
- System Process Protection, which defends critical Windows system processes from being tampered with or compromised through memory injection attacks by other offending processes.

The core on-disk detection technologies include:
- AMP Cloud which blocks malware using the global threat intelligence that is constantly augmented with new threat knowledge from Cisco Talos™, Cisco Threat Grid, and Cognitive Intelligence research.
- TETRA, a traditional signature-based antivirus engine, resides on the endpoint, and provides on-disk malware detection capabilities; TETRA is a part of the AMP Connector for Windows.
- Malicious Activity Protection (MAP), which performs runtime detection and blocking of abnormal behavior associated with a running file or process (for example, ransomware-related behaviors).
- Custom Detections, which deliver robust control capabilities to the security analyst by providing the ability to define custom signatures and enforce blocked application lists using industry-standard formats.

The core post-infection detection technologies include:
- Device Flow Correlation, which inspects incoming and outgoing network communications of a process/file on the endpoint and allows the enforcement of a restrictive action according to the policy.
- Cloud Indicators of Compromise (IOC’s), which help surface suspicious activity observed on the endpoints through pattern recognition; related alerts serve as the trigger for more in-depth investigations and response.
- Endpoint IOCs, which are a powerful threat-hunting capability for scanning post-compromise indicators across multiple endpoints and can be imported from custom open IOC-based files.

- **Tetration** secures hybrid multi-cloud workloads and contains lateral movement of attacks using micro-segmentation. It allows only permitted traffic to flow between application components and users, blocking everything else by default. This approach prevents a persistent threat from entering or searching for additional vulnerabilities by moving from one infected workload to another.

**Filter Network Traffic** *(M1037)*

**Mitigation Description:** Use network appliances to filter ingress or egress traffic and perform protocol-based filtering. Configure software on endpoints to filter network traffic.

- **NGFW** is our threat-focused, next-generation firewall that filters network traffic through protocol-based filtering, URL filtering, application visibility and control. Its complete line of physical and virtual appliances is designed for your ingress and egress network bandwidth requirements.

- **NGIPS** works with NGFW to detect and filter threats from network traffic. It receives new policy rules and signatures every two hours, ensuring that you always have the very latest threat intelligence. For vulnerability prevention, NGIPS flags suspicious files and analyze identified threats that haven't been identified yet. And its high-performance appliances and flexible deployment options are designed to meet your throughput and scalability requirements.

- **AMP for Endpoints** uses endpoint isolation to filter traffic and stop threats from spreading with one-click isolation of an infected endpoint—all without losing control of the device. It reduces the footprint of attacks and fast-tracks remediation.

- **ISE** uses Group Based Policy (formerly TrustSec) and other technologies to filter and segment network traffic through authorization policies. Authorization profiles act as containers, where a number of specific permissions allow or block access to a set of network services.

**Limit Access to Resource Over Network** *(M1035)*

**Mitigation Description:** Prevent access to file shares, remote access to systems, unnecessary services. Mechanisms to limit access may include use of network concentrators, RDP gateways, etc.

- **ISE and NGFW** work with AnyConnect to authenticate and authorize access to resources over a network. They prevent access to unauthorized systems like sensitive file shares and critical systems, and control how an authorized user can access them. For instance, you can define granular authorization policies that permit database administrators to access certain databases with their corporate-issued laptops and from your corporate network, but not from BYOD devices or from remote locations.

- **ISE and NGFW** function as centrally managed VPN concentrators for remote AnyConnect clients for consistent control of remote users. And ISE enforces network access control policies, supporting device certificates and the IEEE 802.1x standard. ISE also restricts use of DHCP to registered devices to prevent unregistered devices from communicating with trusted systems.

- **Tetration** allows you to secure hybrid multicloud workloads and contain lateral movement using micro-segmentation. Tetration allows only the required traffic between application components and users, blocking everything else. This approach prevents a persistent threat from entering or searching for additional vulnerabilities.

**Limit Hardware Installation** *(M1034)*

**Mitigation Description:** Block users or groups from installing or using unapproved hardware on systems, including USB devices.

Though Cisco Security solutions don’t block users or groups from installing unapproved hardware, please share your concerns with us. Our Security Strategy, Risk, and Compliance Services help you document your processes.
and identify any program and technology gaps. And we’ll recommend steps you can take to improve your cybersecurity profile.

**Limit Software Installation (M1033)**

**Mitigation Description:** Block users or groups from installing unapproved software.

Though Cisco Security solutions don’t block users or groups from installing unapproved software, please share your concerns with us. Our Security Strategy, Risk, and Compliance Services help you document your processes and identify any program and technology gaps. And we’ll recommend steps you can take to improve your cybersecurity profile.

**Multi-factor Authentication (M1032)**

**Mitigation Description:** Use two or more pieces of evidence to authenticate to a system; such as username and password in addition to a token from a physical smart card or token generator.

- **Duo** provides modern, effective multi-factor authentication to verify user identity before granting access. Duo is engineered to provide a simple, streamlined login experience for every user and any application, and as a cloud-based solution, it integrates easily with your existing technology.
  - Duo Push is the most commonly used second-factor authentication method, where users simply download the Duo Mobile app and are automatically prompted to confirm each login attempt with a single tap. Duo also allows users to physically authenticate by tapping a U2F USB device or using a built-in biometric authenticator, such as TouchID, via WebAuthn. It also accommodates more traditional second-factor authentication using a secure passcode generated by a physical token, a mobile device, or a network administrator.

  In addition, Duo has two FIPS-compliant Federal Editions that deliver strong cloud-based authentication and device visibility tailored to the demands of public sector organizations:
  - Duo Federal MFA, which offers agencies federal-grade authentication; and
  - Duo Federal Access, which adds stronger role-based and location-based access policies, biometric authentication enforcement, access based on device hygiene, and user notification to self-remediate out-of-date devices. Duo Federal Access is FedRAMP Authorized at the FedRAMP Moderate Impact Level.

- **ISE** secures network access through authentication and role-based authorization, and it integrates with multifactor authentication solutions like Duo, RADIUS RFC-2865 compliant token servers to mitigate the risk of password-based attacks.

**Network Intrusion Prevention (M1031)**

**Mitigation Description:** Use intrusion detection signatures to block traffic at network boundaries.

- **NGIPS** uses intrusion detection signatures and policy rules to block traffic at network boundaries. It provides network visibility, security intelligence, automation and advanced threat protection. NGIPS uses industry-leading intrusion prevention capabilities and multiple techniques to detect even the most sophisticated network attacks and protect you against them. Its high-performance appliances operate in-line with Fail-To-Wire/Bypass technology to ensure continuous network availability.

**Network Segmentation (M1030)**

**Mitigation Description:** Architect sections of the network to isolate critical systems, functions, or resources. Use physical and logical segmentation to prevent access to potentially sensitive systems and information. Use a DMZ to contain any internet-facing services that should not be exposed from the internal network.
• **ISE** builds scalable, manageable network segmentation directly into the network without the typical configuration complexity. It enables your network to enforce role-based, least privilege access throughout your organization. Group Based Policy, formerly known as TrustSec, is the software-defined segmentation technology ISE uses to enforce segmentation through security groups. Group Based Policy is open through IETF, available within OpenDaylight, and supported on third-party and Cisco platforms like NGFW.

• **NGFW** sets the foundation for integrating powerful threat prevention capabilities into your existing network infrastructure, making the network a logical extension of your firewall solution. It enables your DMZ to contain internet-facing services that should not be exposed from the internal network, and it allows only authorized internal devices to reach the internet. NGFW supports Group Based Policy for consistent segmentation policy enforcement with ISE.

• **Tetration** Clusters and Policies discovers relationships and groups systems, important prerequisites for network segmentation policy. ACI policy contracts, firewall configurations, and network access control lists can then leverage these discoveries to improve the accuracy and scalability of segmentation policies.

**Operating System Configuration (M1028)**

**Mitigation Description:** Make configuration changes related to the operating system or a common feature of the operating system that result in system hardening against techniques.

Though Cisco Security solutions do not control operating system configurations, please share your concerns with us. Our Security Strategy, Risk, and Compliance Services can help you document your processes and identify any program and technology gaps. And we’ll recommend steps you can take to improve your cybersecurity profile.

**Password Policies (M1027)**

**Mitigation Description:** Set and enforce secure password policies for accounts.

• **ISE** secures network access, enabling you to define password policies for user accounts so that passwords meet your organization’s specified criteria. Authentication policies can be role-based, using both predefined and custom user attributes.

**Privileged Account Management (M1026)**

**Mitigation Description:** Manage the creation, modification, use, and permissions associated to privileged accounts, including SYSTEM and root.

• **ISE** controls network administrators’ privileged access to networking equipment through its built-in Terminal Access Controller Access-Control System (TACACS+) server. It works with Active Directory groups for granular, role-based access control. For example, your Infrastructure Team might require full access to networking equipment, while your Operations Team might only need access to “show” commands.

• **AMP** uncovers hard-to-detect system behavior, such as PowerShell-based exploits; privilege escalation; modifications of access control lists; attempts to enumerate systems; and the use of vssadmin to delete shadow copies or disable safe boots.

**Privileged Process Integrity (M1025)**

**Mitigation Description:** Protect processes with high privileges that can be used to interact with critical system components through use of protected process light, anti-process injection defenses, or other process integrity enforcement measures.

• **AMP for Endpoints Exploit Prevention** protects against malware and other exploits that target unpatched or zero-day vulnerabilities to gain privileges and system control. It understands how processes operate on Windows systems to protect critical system components and applications.
Remote Data Storage (M1029)

Mitigation Description: Use remote security log and sensitive file storage where access can be controlled better to prevent exposure of intrusion detection log data or sensitive information.

- Cisco Security Analytics and Logging stores NGFW logs securely in the cloud, making them accessible and searchable from Cisco Defense Orchestrator. It identifies and enriches high-fidelity alerts so you can prioritize threat alerts and focus on what matters most. It improves network visibility so you can quickly detect threats in real time and remediate incidents with confidence and at scale. You’ll gain insights from behavioral analytics and get actionable security intelligence to help make your security team more efficient and effective.

Restrict File and Directory Permissions (M1022)

Mitigation Description: Restrict access by setting directory and file permissions that are not specific to users or privileged accounts.

Though Cisco Security solutions do not control file and directory permissions, please share your concerns with us. Our Security Strategy, Risk, and Compliance Services help you document your processes and identify any program and technology gaps. And we’ll recommend steps you can take to improve your cybersecurity profile.

Restrict Library Loading (M1044)

Mitigation Description: Prevent abuse of library loading mechanisms in the operating system and software to load untrusted code by configuring appropriate library loading mechanisms and investigating potential vulnerable software.

- AMP for Endpoints Exploit Prevention restricts library loading and makes system memory unpredictable to attackers. It appends a small Dynamic-Link Library (DLL) to the Windows loader, proactively changing the process structure and protecting it from abusive library loading.

  For example, attackers often use Reflective DLL injection to load a DLL into a host process from memory rather than from disk, bypassing the Windows loader. AMP Exploit Prevention protects against reflective loading by randomizing the API of the host process, causing malicious code to execute deceptive stubs instead of the attackers’ mapping functions. This stops abusive library loading and keeps applications running normally.

Restrict Registry Permissions (M1024)

Mitigation Description: Restrict the ability to modify certain hives or keys in the Windows Registry.

Though Cisco Security solutions don’t control access within the Windows Registry, please share your concerns with us. Our Security Strategy, Risk, and Compliance Services help you document your processes and identify any program and technology gaps. And we’ll recommend steps you can take to improve your cybersecurity profile.

Restrict Web-Based Content (M1021)

Mitigation Description: Restrict use of certain websites, block downloads/attachments, block Javascript, restrict browser extensions, etc.

- NGFW provides URL filtering and application visibility and control to restrict the use of websites and applications.

- Web Security restricts web-based content by automatically blocking risky sites and testing unknown sites before allowing users to click on them. Powered by our Talos threat research organization, Web Security provides in-depth URL filtering and reputation analysis, multiple antivirus engines, Layer 4 traffic monitoring, Advanced Malware Protection (AMP), and Cognitive Threat Analytics (CTA). And it goes deeper than blocking or allowing certain websites, permitting or denying specific functionality within the sites.
• **Umbrella** is a cloud-delivered security service that brings together essential functions that you can adopt incrementally, at your pace. Umbrella unifies secure web gateway, DNS-layer security, cloud-delivered firewall, cloud access security broker functionality, and threat intelligence. Deep inspection and control ensure compliance with acceptable-use web policies and protects against internet threats. Accelerated threat detection/response and centralized management makes it ideal for decentralized networks.

• **Email Security** defends against a wide variety of email-based attacks, including but not limited to phishing, malicious attachments, business email compromise, and ransomware. It works with Web Security to ensure links in content or attachment do not hit malicious or unauthorized URLs. It also works with Cisco Advanced Malware Protection to identify and block stealthy malware in attachments, while industry-leading URL intelligence combats malicious links. And it enhances the security of email in Microsoft Office 365.

• **Security Connector** is an app for Apple iOS devices that offers visibility into network traffic and blocks connections to malicious sites -- wherever users go. It’s the result of a close partnership between Cisco and Apple to strengthen security for mobile workers. People can easily mistype URLs or click on a phishing link within a message, leading them to malicious sites that compromise their devices. Security Connector prevents risky connections on both a DNS and IP address level, even over cellular networks and public Wi-Fi.

• **AnyConnect Secure Mobility Client** uses optional Umbrella technology to protect roaming users from web-based threats whether or not they’re on your corporate network.

**Software Configuration (M1054)**

*Mitigation Description:* Implement configuration changes to software (other than the operating system) to mitigate security risks associated to how the software operates.

Cisco Security solutions don’t manage software configurations for technologies like Microsoft Office, PowerShell, or browsers specifically mentioned in MITRE’s Techniques Addressed by Mitigation.

Of course, we manage software configurations for our own security products. For example, we have several options for managing network security, including cloud-based, centralized, or on-box management systems to streamline security policy and device management.

Please share your change and configuration management concerns with us. Our Security Strategy, Risk, and Compliance Services can help you document your processes and identify any program and technology gaps. And we’ll recommend steps you can take to improve your cybersecurity profile.

**SSL/TLS Inspection (M1020)**

*Mitigation Description:* Break and inspect SSL/TLS sessions to look at encrypted web traffic for adversary activity.

• **Firepower Threat Defense** supports SSL/TLS decryption for deep inspection of encrypted web traffic. And since many organizations have security policies against older versions of SSL/TLS, you can use the SSL Decryption policy to block traffic that uses an SSL/TLS version that you prohibit.

• **Umbrella** proxies and inspects web traffic sent over HTTPS, going beyond simply inspecting normal URLs to identify and stop encrypted adversary activity.

• **Web Security** decrypts SSL-encrypted web traffic and applications, scanning for threats and stopping encrypted adversary activity.

**Threat Intelligence Program (M1019)**

*Mitigation Description:* A threat intelligence program helps an organization generate their own threat intelligence information and track trends to inform defensive priorities to mitigate risk.
• **Talos** is our industry-leading threat intelligence organization, a team of cybersecurity experts who analyze threats, track trends, and generate intelligence information that informs all of our security solutions. Many organizations don’t have the resources to run their own threat intelligence programs, and most others want their programs backed by the best. No matter what Cisco Security solution you have, you can rest assured that it’s back by our premier threat intelligence team.

• **SecureX** is our integrated security platform designed for your threat intelligence program and SOC enabling them to see and understand their security posture, track trends, detect threats, investigate incidents, and quickly take action to mitigate risks.

• **Threat Response**, part of our SecureX platform, uses Talos threat intelligence and your product telemetry to detect, investigate, and remediate threats. It integrates with other Cisco Security solutions to take immediate action.

• **Threat Grid** is an essential solution for your threat intelligence team. It combines advanced sandboxing with threat intelligence into one unified solution to protect organizations from malware. With a robust, context-rich malware knowledge base, you will understand what malware is doing, or attempting to do, how large a threat it poses, and how to defend against it.

• **Managed Security Services** are backed by state-of-the-art global Security Operations Centers (SOCs) that provide 24-hour managed security services. Whether you want to outsource your threat intelligence program or want to bolster your existing capabilities, we’ll help you identify and mitigate threats before they affect your business.

  You can advance your security operations capabilities while reducing mean time to detect and containing threats faster with Managed Detection and Response. Let us respond to alerts, provide insights on attacks, and provide expert guidance to stop threats and prevent breaches.

  You can also simplify and automate Cisco and third-party device monitoring and management with Active Threat Analytics, backed by our global Security Operations Centers.

**Update Software** *(M1051)*

**Mitigation Description:** Perform regular software updates to mitigate exploitation risk.

While we don’t manage or update third-party vendor software, we are committed to the security of our own products and software. We continually analyze our solutions for vulnerabilities, publish updates, and notify quickly through Cisco Security Advisories.

The **Cisco Product Security Incident Response Team (PSIRT)** is responsible for responding to Cisco product security incidents. The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of information about security vulnerabilities and issues related to Cisco products and networks. Cisco defines a security vulnerability as an unintended weakness in a product that could allow an attacker to compromise the integrity, availability, or confidentiality of the product. The Cisco PSIRT adheres to ISO/IEC 29147:2014.

Learn more about our Security Vulnerability Policy [here](#).

**User Account Control** *(M1052)*

**Mitigation Description:** Configure Windows User Account Control to mitigate risk of adversaries obtaining elevated process access.

Though Cisco Security solutions aren’t designed specifically for Windows User Account Control, please share your concerns with us. Our Security Strategy, Risk, and Compliance Services help you document your processes and identify any program and technology gaps. And we’ll recommend steps you can take to improve your cybersecurity profile.
User Account Management (M1018)

Mitigation Description: Manage the creation, modification, use, and permissions associated to user accounts.

- **ISE** manages the creation, modification, use, and permissions associated with user accounts through its built-in RADIUS and TACACS+ databases. It authenticates and authorizes users to control where they can go on the network, with what devices, and how they access the network (wired, wireless, or VPN). It integrates with Microsoft Active Directory to leverage users and groups in its authentication and authorization policies.

- **Cloudlock** is a Cloud Access Security Broker that uses advanced machine learning algorithms to detect anomalies, to protect user accounts and manage their use. For example, it identifies activities outside approved countries and spots actions that seem to take place at impossible speeds across distances -- clear signs of account compromise.

User Training (M1017)

Mitigation Description: Train users to be aware of access or manipulation attempts by an adversary to reduce the risk of successful spearphishing, social engineering, and other techniques that involve user interaction.

- **Security Awareness** helps promote and apply effective cybersecurity common sense by modifying end user behavior to work smarter and safer. This cloud-delivered subscription provides comprehensive simulation, training, and reporting so employee progress can be continually monitored and tracked. Cisco Security Awareness helps your organization remain safe with engaging and relevant computer-based content with various simulated attack methods. It also offers extensive libraries of cyber training content and templates for internal campaign reinforcement including videos, posters and newsletters.

- **Web Security, Umbrella, and Email Security** notify users when they block risky website access attempts, reminding them to be careful while web browsing and before clicking links. These products are primarily security controls, but they help users understand why they acted and blocked activity in order to reinforce user security training and vigilance.

- **Duo and AnyConnect** alert users when their devices are out of date, encouraging them to update them as quickly as possible. These products are primarily security controls, but they also help reinforce users’ training on the need to keep their devices current.

Vulnerability Scanning (M1016)

Mitigation Description: Vulnerability scanning is used to find potentially exploitable software vulnerabilities to remediate them.

- **Duo** checks devices for outdated, vulnerable operating systems or insecure configurations to prevent risky or potentially compromised devices from accessing critical applications and data. It enables adaptive access policies based on role, device, location, and other factors to respond to changing user context. Duo also lets you manually prevent logins: If a user loses their authentication device or reports it stolen, Duo lets you disable and disassociate the device from the user.

- **AnyConnect** checks devices for compliance with your security policy, working with ISE to prevent risky or potentially compromised devices from accessing your network.

- **AMP** determines which endpoints have software with a specific Common Vulnerabilities and Exposures (CVE) entry, regardless of when the application last ran. You can then isolate endpoints that have critical vulnerabilities from the network before attackers can exploit them.

- **Tetration** detects common vulnerabilities and identifies application anomalies through process behavior deviations, allowing you to proactively quarantine affected servers before damage occurs. Its open policy model works across bare metal, virtual, and containerized workloads both on-premises and in the cloudmodel works across bare metal, virtual, and containerized workloads both on-premises and in the cloud.
Conclusion

The dream really can come true. You can know the methods cyber attackers use to threaten your organization, how to address them, and be ready. At Cisco, we’re ready too.

As you use MITRE ATT&CK Enterprise to understand how threat actors operate, you can also rely on Cisco Security to help you prepare and take action. Our cybersecurity solutions defend your organization from threats documented in ATT&CK, and you learned how we mapped our capabilities through relevant, supporting detail. Make informed decisions about cybersecurity investments -- and make every investment count.

Learn more about Cisco Security and talk to us today.