WHITEPAPER

Trellix Adaptive Defense Model

A Strategic Approach to Integrating Defensive Playbooks and Applied Countermeasures over the Next Decade

Have you ever wondered why we model attackers and threats, but neglect to design comparable systems for defensive strategies?

Think about it.

No global cybersecurity leader to date has been able to establish a simple model that describes what success means for a cyber defender.

Like what we should all be doing before, during, and after an attack. The comprehensive set of phases. Our activities. Our goals and tactics.

It's 2022. Our cybersecurity defensive environment is changing overnight. We need to become intensely adaptive. We won't keep up unless we establish a truly best-in-class, end-to-end defense model.

We have.

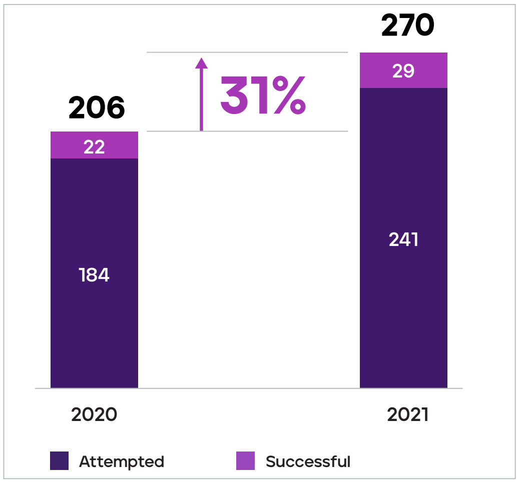
We call it the Trellix Adaptive Defense Model.

Table of Contents

A new approach to modeling cyber defense

According to Accenture, companies in 2021 confronted 270 attacks on average. This represents an increase of 31 percent compared to the prior year. Each of these data breaches, on average, cost organizations $4.24 million.[1]

These are significant numbers. And this trend is likely to intensify.



A changing battlefield

The cybersecurity field is shaped by what traditional defense planners refer to as asymmetric warfare—surprise attacks by small groups levied against larger enterprises whose assets, information, operations, and reputation represent attractive targets.

Cyber attackers are increasingly using tactics that range from "old-school" to "sophisticated" in unpredictable ways. And these tactics are working. Today, malicious actors are able to advance far more quickly and efficiently than in the past through misconfigured defenses, poor security architectures, and excessive privileges.

As a result, the value of your investments in security solutions is at risk and frustration is mounting among your security operations (SecOps) and Security Operations Center (SOC) teams. Low morale then accelerates attrition and places even greater pressure on your access to talent, exacerbating the acute shortage in cybersecurity professionals across the marketplace.

> In 2021, attacks, on average, increased by 31 percent over the prior year.

[1] Accenture, State of Cybersecurity Surveys, Wave 3 and 4 Reports, 2020 and 2021.

Three questions to consider

In recent years, we—the cybercommunity, both private and public—have derived undeniably positive results from modeling attackers and threats. But we've dragged our feet when it comes to modeling equally proactive systems for defensive strategies.

Finding better answers, like any innovative advance, starts with asking questions at the cutting edge of innovation, adaptation, and positive change.

1. A more agile framework: What if you could establish a highly adaptive defensive framework capable of guiding your entire team, from your SecOps and SOC professionals to any security architect, security engineer, and IT administrator helping to manage and operate your defenses?

2. A broader perspective: What if, rather than solely focusing on responding to attacks, you could capture a comprehensive view across the entire attack lifecycle, from prevention to detection and response? Such a perspective would enable a constantly evolving defensive strategy, one that we could continuously retune and recalibrate as we keep pace with the increasing sophistication of today's adversaries.

3. More meaningful impacts: What if this framework could dramatically increase the efficiency and effectiveness of your security experts—and help them become high-performance professionals, with extensive defensive knowledge and a deeply layered understanding of cyber defense, especially as it continues to change?

At Trellix, we have been developing a cohesive response to these questions for several years, a framework that drives living security by embedding expertise throughout the attack lifecycle. We call our solution the Trellix Adaptive Defense Model (Trellix ADM). This white paper provides a brief, executive-level introduction to Trellix ADM and why it represents the new frontline in cybersecurity planning and defense.

At Trellix, we have been developing a cohesive response to these questions for several years...

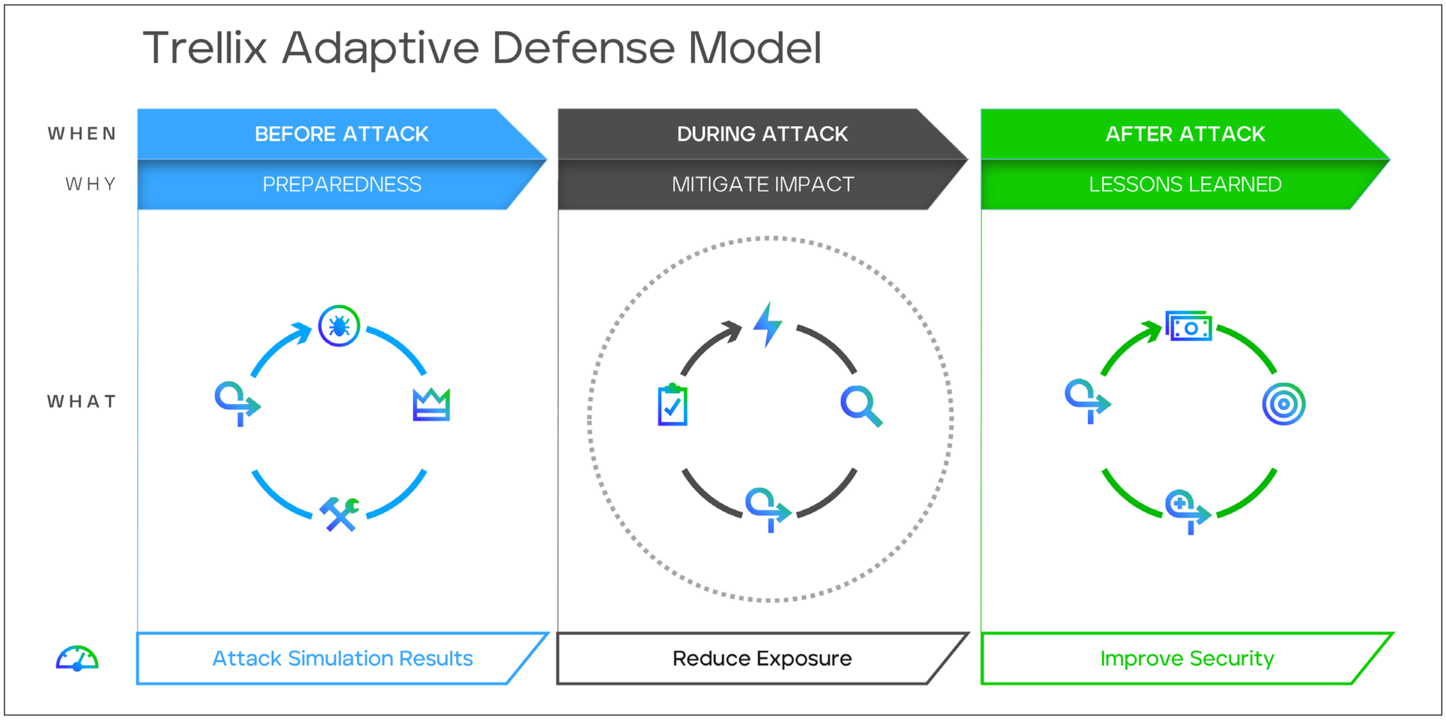


Figure 1: Overview of the Trellix Adaptive Defense Model (displayed without OODA loop detail)

1. Baseline: The limitations of current cyber defense capabilities

1.1 Critical thinking in check

Today's cybersecurity models, from Lockheed Martin's Cyber Kill Chain[2] to MITRE ATT&CK®,[3] tend to focus on the attacker rather than the defender. Despite their effectiveness, these models have assumed that defenders are locked into static and linear mindsets, leaving them at a disadvantage in matching the nimble creativity of today's rapidly mutating adversaries.

// CYBERSECURITY IN 2022

Poor Defensive Visibility Represents a Critical Vulnerability

When cyber defenders can't access a holistic view of the defensive ecosystem, the value and ROI of security investments decline. That's never good, but especially now when boards are increasingly pressing business and IT management for evidence that years of heavy investment have been worth the cost.

With response playbooks automated by the latest machine learning tools and orchestrators, defenders have access to game-changing capabilities and countermeasures. But current approaches to defense hold them in a reactive position.

Defenders can't think critically about the threat landscape and make the logical connections that would lead to proactive pivoting, new syntheses, and data exploration. Defenders are left unable to formulate crucial questions about hypotheses and the broader relationships within the business and assets at risk.

1.2 Too many products, not enough understanding

Compounding this difficulty is the high number of security products cyber analysts have in their arsenals. Many of our clients with 1,000+ employees maintain, on average, 70 security products from as many as 35 vendors.

These crowded product portfolios mean cyber defenders lack familiarity with their defense capabilities and toolkits. In addition to defense misconfiguration, weak security architectures, and excessive privileges, this "battle fog" forces analysts to rely on exhaustingly iterative cycles of manual research and raw guesswork.

[2] According to the IEEE, "The cyber kill chain is essentially a cybersecurity model created by Lockheed Martin that traces the stages of a cyber-attack, identifies vulnerabilities, and helps security teams to stop the attacks at every stage of the chain."

[3] MITRE ATT&CK® is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.

1.3 A firehose of alerts and information

Today, analysts in high-pressured SOC environments respond to attacks by trying to investigate and analyze configuration guidelines, best practices, and documents that are often incomplete, convoluted, and contradictory. They lose precious time manually looking for patterns, doubling-back from dead ends, and trying to figure out what's important in a mass of data.

Other challenges include unclear change control processes and inconsistent terminology that slow down communication between security and IT teams, whose partnership is so critical to effective and efficient cyber defense.

A majority (81 percent) of Chief Information Security Officers (CISOs) admit that staying ahead of attackers is a constant concern. With 70 percent of security stakeholders reporting double the volume of security alerts in the past five years, analysts simply don't have time to respond. Even the artificial intelligence (AI) and machine-learning models that offer so much promise require time-consuming human curation, tuning, and calibration for effectiveness in the long term.

BY THE NUMBERS

35%

Percentage of security analysts who ignore alerts when the queue gets too full.[4]

287 days

Average time to identify and contain a data breach.[5]

20.9 hours

Average time to respond to a global incident. This is more than twice the time it takes, on average (9.5 hours) for a cybercriminal to obtain illici access to a target's network.[6]

[4] The Voice of the Analysts, IDC, 2021.
[5] Cost of a Data Breach, IBM, 2021.
[6] Voice of SecOps, Deep Instincts, 2021

> “A product-centric industry often drives security professionals to focus too much time and energy on learning tools and technologies, without paying much attention to the quality of their analysis.
>
> In fact, one of the most important skills that successful analysts need to acquire is to understand WHEN and WHY certain tools or products must be used. Understanding this can make a difference between ‘winning’ or ‘losing’ the battle against an adversary that is attacking an organization.”[7] (SANS)

2. A New Model: Changing how we think about cyber defense

2.1 A dynamic reference guide for measuring efficacy

The Trellix Adaptive Defense Model is a defensive toolkit that comes embedded with expertise. It’s a new behavioral model for cyber defense that helps defenders make better decisions by providing answers to critical questions like:

- What countermeasures do I need to apply against specific adversaries?
- When do I need to use those countermeasures?
- Why do I need to use them?
- How do I measure their efficacy?

Using a time-based security model, Trellix’s Adaptive Defense Model provides guidance across all phases of the attack lifecycle—extending protection time before the attack, reducing exposure and impact during the attack, and furnishing insight into the tactics that worked and didn’t work after the attack. By highlighting the gaps in security and providing insight into the tools that can improve efficacy, Trellix’s Adaptive Defense Model gives SOC professionals critical insights while aligning with the needs and requirements of all members of the cyber defense community.

[7] https://www.sans.org/webcasts/2021-report-top-skills-analysts-master-118350/

Adaptability requires critical thinking

Every organization is different and calls for a unique defensive posture to optimize control over its assets.

Defenders lose control when they don’t have:

- Visibility or know what assets are at risk
- A threat model
- Insights into how attackers behave
- Clarity on the tools and resources available to respond
- Confidence in projecting how long it will take to enable these capabilities

Despite owning the leading security technologies, organizations struggle today to create defensive models that can contextualize and internalize all this information.

- **Value for cyber defenders:** Empowers cyber defenders by reducing the guesswork and manual assessment behind today’s defensive security, putting the knowledge and capabilities of experts at our fingertips.
- **Value for vendors:** Serves as a reference to map a security portfolio to a specific security outcome or tactic.
- **Value for customers:** Minimizes stress and uncertainty by providing expert guidance curated for their organization’s most relevant cyber defense needs.

At Trellix, we view the new Adaptive Defense Model as essential to driving living security. The model equips security professionals at all experience levels with expert insight into their countermeasures, explaining why they matter, what security outcomes they produce, and when they should be used. Trellix’s Adaptive Defense Model fills a gap in the security industry, providing organizations with a reference to measure efficacy and validate how their security investments help achieve their strategic and tactical goals.

2.2 Expert coaching across the attack lifecycle

With Trellix's Adaptive Defense Model, security professional gain end-to-end adaptive defense coaching across the attack lifecycle. At the intersection of threat knowledge and product performance, the framework amplifies the preparedness, anticipation, and critical thinking of SOC and SecOps professionals, giving them enhanced insight across a suite of customizable defensive tactics. It provides prescriptive metric-based guidance to identify assets at risk, while suggesting mitigating actions that will increase visibility, detection, and response capabilities.

- **Before** the incident, it uses threat modeling to coach IT administrators, security architects, and security engineers on the most effective countermeasures for reducing the attack surface while identifying and defending at-risk assets.
- **During** the incident, it coaches SOC professionals on when to use particular tools—as well as why and how to use them—removing guesswork and manual research while boosting the critical thinking of SOC professionals.
- **After** the incident, it helps defenders measure the effectiveness of their defensive posture regarding prevalent threats and enables continuous improvement.

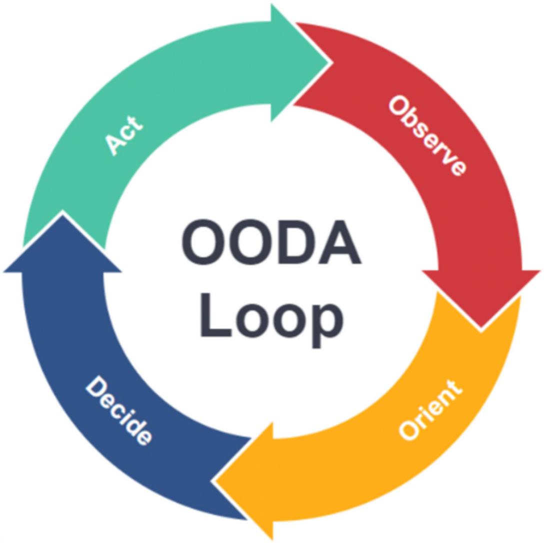
[8] https://online.visual-paradigm.com/knowledge/decision-analysis/what-is-ooda-loop/

3. Frontline Reimagined: Faster OODA Loops for All-Around Defense

3.1 Short-circuiting the attacker

Trellix's Adaptive Defense Model incorporates time through the decision-making approach known as the OODA loop, a four-step iterative process that repeats the cycle Observe-Orient-Decide-Act.[6]

- **Observe:** Sense the environment, gather information, survey the situation
- **Orient:** Analyze the data to form a hypothesis and obtain perspective
- **Decide:** Develop an action plan for a situation based upon the previous phases
- **Act:** Put the decision into motion



Initially developed for aerial combat situations in which decision-making occurs faster than pilots can process all available information, the goal of the strategy is to iterate cycles of OODA loops faster than the opponent. By doing so, the defender effectively infiltrates the opponent's decision-making cycle, short-circuiting their thinking processes and forcing them to react disadvantageously.

These lessons apply to the time-critical aspects of cybersecurity. OODA feedback loops drive progressive and actionable insights with an emphasis on preparedness and continuous improvement. In the security context, both defender and attacker operate under time constraints. By executing faster through OODA loops, the defender amplifies favorable feedback across the dynamic environment and gains the upper hand.

What the Experts Say

"In order to win, we should operate at a faster tempo or rhythm than our adversaries—or, better yet, get inside [the] adversary's Observation-Orientation-Decision-Action time cycle or loop ... Such activity will make us appear ambiguous (unpredictable) thereby generate confusion and disorder among our adversaries—since our adversaries will be unable to generate mental images or pictures that agree with the menacing, as well as faster transient rhythm or patterns, they are competing against."

– John Boyd
U.S. Air Force Colonel + OODA Loop Developer

"The key is to obscure your intentions and make them unpredictable to your opponent while you simultaneously clarify his intentions. That is, operate at a faster tempo to generate rapidly changing conditions that inhibit your opponent from adapting or reacting to those changes and that suppress or destroy his awareness. Thus, a hodgepodge of confusion and disorder occur to cause him to over- or under-react to conditions or activities that appear to be uncertain, ambiguous, or incomprehensible."

– Harry Hillaker

General Dynamics Aeronautical Engineer and "Father of the F-16"

3.2 Orienting for end-to-end control

The Trellix Adaptive Defense Model uses three OODA loops—one before the adversary initiates the attack, another during the attack, and the last after the attack—to empower security professionals to address and cover the entire attack lifecycle.

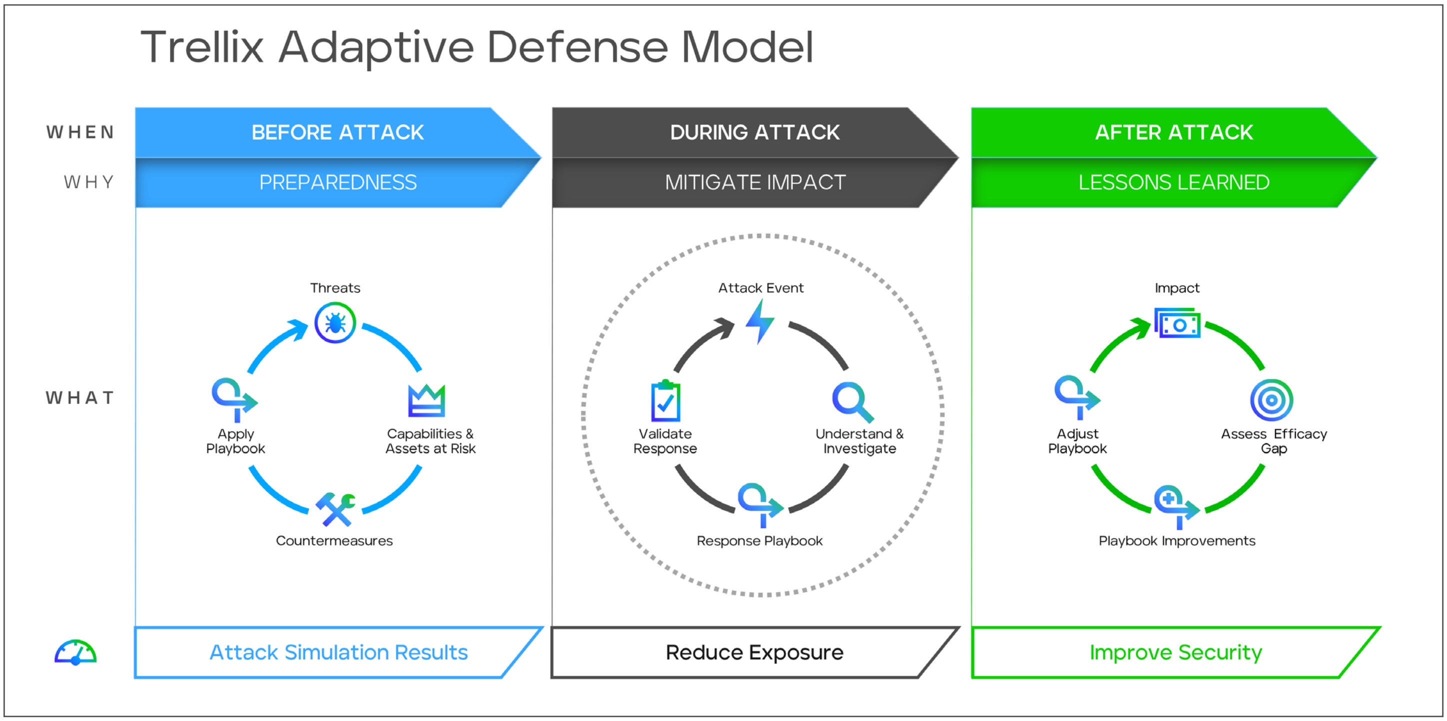


Figure 2: Overview of the Trellix Adaptive Defense Model (includes OODA loop detail)

Before the attack

1. **Observe** your attackers by modeling their behaviors (e.g., using MITRE ATT&CK).
2. **Orient** yourself by internalizing and contextualizing your knowledge, architecting your internal capabilities, and prioritizing your at-risk assets (e.g., using time-based security).
3. **Decide** on your counter-measures by referring to your defensive playbook, which details your efficacy for responding, investigating, detecting, and hunting for attacks.
4. **Act** on what you've learned by updating your product configuration. Continue to measure your efficacy through purple teaming exercises.

During the attack

1. **Observe** events and alerts, gathering data from all sensors (endpoints, network, cloud and applications) to understand what is happening, where, and its priority level.
2. **Orient** to the changing context while using critical thinking to make logical connections that provide a set of options, hypotheses, and assessments.
3. **Decide** (e.g., using an ACH model) among the alternatives identified in the orientation phase. This can help predict or anticipate the adversary's next move.
4. **Act** by carrying out your decision knowing that the adversary might be watching your actions, which is why actions should be rapid, surprising, ambiguous, and everchanging through repeated iterations.

After the attack

1. **Observe** the impact of your actions and assess what worked during the cycle.
2. **Orient** by assessing the efficacy of your performance. Could you have prevented the attack earlier in the attack chain? Were there visibility gaps? Were the response times adequate?
3. **Decide** to carry out concrete steps to improve the defensive playbook by tuning prevention, detection, and countermeasures
4. **Act** by adjusting the defensive playbook in preparation for the next attack.

3.3 Top use cases

Attack Lifecycle	Problem Scenario	Solution	Outcomes
Before the attack Prepare	**CISO asks about particular ransomware protection** • Need to manually research across multiple sources • Information is inconsistent and not actionable • Unclear how much the countermeasures cover the tactics and techniques • Unclear what assets are at risk	**Automated guide coaches defender through the security assessment of ransomware risk** • A single source to assess your ransomware security posture • Ready with actionable insights (why and when to use particular tools) • A guide for assessing, validating, and monitoring required controls	Confident assessment of the ransomware risk; prevention is set in a timely and efficient manner Clear explanation of the value provided by the security solutions deployed in the environment
During the attack Mitigate impact	**Attackers have infiltrated the organization; defenders need to minimize impact** • Limited info on the compromised indicators, requiring manual research • Unclear course of action due to unclear priorities • Attackers may gain control of the entire environment and deploy ransomware	**Automated guide finds, disrupts, and remediates the attack before ransomware makes it into the environment** • Observe events and alerts, gather data from all sensors • Contextualize and make logical connections for situational awareness • Apply critical thinking through AI-assisted investigations for quick containment and eradication	Time-based security extends protection time while hastening detection and response Attack remediated before the attacker deploys ransomware Impact reduced, resulting in lower cost to organization
After the attack Improve detection and prevention	Lacking a planned defensive tactic makes it impossible to measure what worked well; i.e., defenders can't improve what they can't measure	Measure effectiveness of defensive playbook, tune countermeasures, consider new architecture and engineering projects, then validate new implementations	Continuous improvement through Zero Trust and defensible security architectures, plus improved preparedness for next attack

4. A Better Battle Plan: Our defenses must be dynamic

4.1 Empowering your junior analysts

Today's cyber defenders struggle to understand threats. With endpoint security technologies, analysts receive alerts, but they don't necessarily know what those alerts mean. The problem here is that they have difficulty discerning the impact of the attack.

In ransomware cases, early indications that something's amiss are regularly too subtle to see. Or there's a finding that isn't malicious per se, but it takes years of experience to understand how it points to potential persistence or lateral movement. What junior security analysts often lack is the experience to build hypotheses, along with the questions that support those hypotheses or contradict them.

What is "security efficacy"?

The Trellix Adaptive Defense Model's metrics are based on defining security efficacy as an ability to:

- Identify relevant threats
- Determine assets at risk and reduce exposure before an attack
- Protect assets at risk during an attack
- Capture visibility of an attack
- Hunt for an attack
- Detect an attack
- Investigate an attack
- Respond effectively to an attack

This is where the Trellix Adaptive Defense Model comes in—as an expert knowledge system that provides decision support across the attack lifecycle. It's a simple yet powerful framework that explains defensive functions in a visual manner, allowing analysts to select for particular SOAR capabilities while understanding what their deployment will accomplish.

In this way, Trellix's Adaptive Defense Model embeds expertise into the playbook by offering the context and the rationale for which steps to take. Through a visual interface, SOC professionals, security architects and engineers, and IT administrators gain the insights they need to improve strategic and tactical decision-making throughout the incident. Trellix Insights is an example of how Trellix ADM is implemented into a defensive playbook today.

4.2 A senior expert always at your side

Ransomware comes in many different shapes and sizes. And these, of course, keep changing. Analysts are often challenged to identify which capabilities and countermeasures will be most effective in countering one strain or another. Trellix's Adaptive Defense Model eases this burden by providing a standardized taxonomy and supporting metrics that describe and assess both native and non-native countermeasures.

> Trellix's Adaptive Defense Model eases this burden by providing a standardized taxonomy and supporting metrics that describe and assess both native and non-native countermeasures.

In essence, the Trellix Adaptive Defense Model productizes the mind of the senior expert. It gives him or her direct access to the expert-level understanding and information they need to increase their preparedness and resilience in anticipation of an attack.

For CIOs and CISOs, these insights increase situational awareness by explaining more than just what the threats are. The Trellix Adaptive Defense Model measures and explains the efficacy of their products against those threats, while specifying the product's security outcomes and showing how and at what point those products are optimally used during the defensive lifecycle. What's more, the model provides a metric-based argument for investing in particular security products and capabilities, along with the consequences of not doing so.

Today's organizations have tools, but don't fully understand how to use them. Using Trellix ADM, security professionals can better manage their defensive technology arsenal through curated summaries of their relevant attributes, ensuring that they have a holistic understanding of the capabilities at their fingertips.

4.3 Partnering by means of a common language

For many organizations, communication between siloes by championing a common language that, while not new, streamlines the ability of organizations to leverage other industry standards and best practices, such as MITRE D3FEND™, a cybersecurity countermeasure knowledge base.[9]

When changing or adding a capability, for instance, a change control card in the defensive playbook lets security professionals proceed step-by-step through a change procedure. It not only identifies the individual with the skills, experience, and authority to assist, it also indicates what will be required when communicating with that person.

Increasing communication efficiency benefits cyber defense in other ways as well. For security professionals, making a presentation to business leadership on why a particular capability or product is required is a constant challenge. Not only is it time-consuming to prepare, but it draws on a suite of hard-to-come-by communication skills.

With detailed data and measurements on the impact of particular countermeasures, Trellix's Adaptive Defense Model gives security analysts a ready-at-hand way to create proposals in a language that CIOs and CISOs not only understand, but also need when meeting with business leaders further up the chai of command.

When communication improves, defenses strengthen

The Trellix Adaptive Defense Model enables clear communication across stakeholders by providing a common language:

- For vendors communicating with customers
- For SOCs communicating with CISOs
- For CISOs communicating with infrastructure owners and other executives

5. The Time Factor: Building resiliency into defensive architectures

5.1 A lot can happen between yes and no

Today's fixation on ransomware identification has led to the neglect of the critical factor of time when creating cyber defense strategies. Rather than focusing on the "yes or no" of whether the adversary was blocked or not—or detected—Trellix's Adaptive Defense Model keeps the team focused on the bigger picture: the entire attack lifecycle.

- **Before** the attack, the defender uses the data harvested from past experience—from real-time attacks to purple teaming exercises—to configure a defensive architecture most likely to defend the most at-risk assets against the most likely forms of attack.
- **During** the attack, the defender's model uses artificial intelligence and machine learning tools to continuously evaluate sensor data for actionable information on the adversary, strategically responding in decisive yet elusive ways, ideally surprising the attacker and throwing off their strategy.
- **After** the attack, the defender reviews the incident using a visual representation based on telemetry data. By thinking critically through lessons learned, the defender can make adaptations to the model that further optimize its defensive configuration.

Dynamic defense for nonlinear times

An approach to defense that stays proactive, while also aware of its array of deployments, leads to substantially improved architectures for detection, visibility, and response that are more robustly integrated—and also more prepared to adapt to the unforeseen.

Timing is critical—and prioritizing prevention can help defenders estimate how much time they have to react to the adversary. But it also means we have to architect for detection, visibility, and response, ideally ensuring that the sensor goes off before the impact grows too large.

In the end, it's about building better resilience. While we know how difficult it can be to keep attackers outside the environment, we also know that they require time once inside to achieve their objectives—from mapping the environment, to escalating privileges, and gradually increasing access. Given enough time, the attacker will own the environment and have the capacity to detonate ransomware at will.

Before that, however, a temporal progression across an attack chain calls up multiple defense approaches and countermeasures, varying alert levels, and different response configurations depending on how much time the adversary has been inside and the level of access they have achieved. Using this information, the Trellix Adaptive Defensive Model expands on today's standard security models by offering an agile approach to defense configuration that takes time into account.

5.2 Zero trust in action

Imagine a simple video of a cyberattack made up of animated telemetry logs. At first, the attackers move slowly, shifting from place to place but without any clear purpose. But then another attacker appears, moving quickly with coordinated movements. What do we know about this attacker? It's clear they're familiar with the environment. What does that mean? It means they've been here before and have taken the time to map the environment and acquire credentials.

By giving defenders the ability to filter controls by attack phase, the Trellix Adaptive Defense Model gives cybersecurity professionals a different way to look at the attack playbook. By studying attack chains and aggregating data from threat research, we can gather the commonalities of the most frequent ransomware attacks. From here, we can proactively configure our applications and networks to defend against the most common attack vectors as well as protect the most desirable assets.

Thus, if most ransomware attacks take place after attackers have been on the network long enough to elevate privileges, then we know that an effective response will involve reducing excessive privileges by deploying a Zero Trust strategy. If we know the specific privileges most likely to be acquired by attackers, we can configure defenses specifically around eliminating trust for these privileges.

Finally, rather than waiting for ransomware attacks to test these defenses, security professionals using Trellix's Adaptive Defense Model can test, train, and finetune their configurations and architectures in advance with purple teaming exercises. In this way, they can help identify the gaps in the security architecture and deploy the security controls to plug them.

The face of prevention is changing

The complexity of today's security environment has laid bare the limits of a static and linear approach to cyber defense. To respond effectively to the creative deceptions of today's nimble attackers, we need highly adaptive defensive frameworks able to guide not just SOC and SecOps professionals, but also security architects, security engineers, and IT administrators.

The Trellix Adaptive Defense Model, the new adaptive defense model driving living security, meets these demands by coaching the defender through each phase of the attack lifecycle using a playbook of automated guided steps. Based on progressive insights, defenders adjust their strategy in real time while adapting quickly to improve resiliency and mitigate impacts. As a complement to their traditional threat intelligence models based on adversarial behaviors, they now focus on defensive tactics, supported by a simple, visual way to describe what success means.

As the result of 80+ years of threat intelligence, defensive innovation, blue teaming, and applied countermeasures, Trellix's Adaptive Defense Model gives all defenders the ability to measure the effectiveness of their defensive posture against today's most sophisticated threats. At the same time, this game-changing framework gives business executives, CISOs, and SOC managers data-based validation for their security investments, enabling clear insight into how particular products contribute to achieving their specific goals.

That's Trellix's Adaptive Defense Model.

Cybersecurity transformed.

Trellix

Visit Trellix.com to learn more.