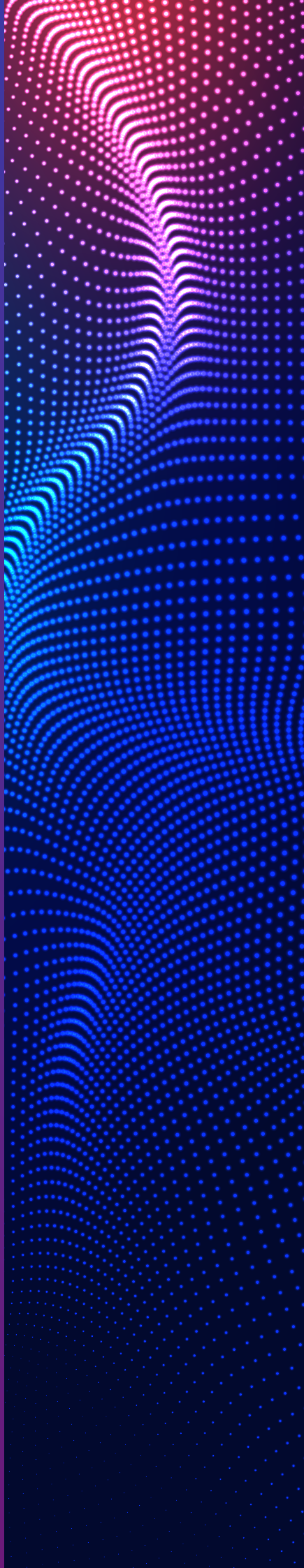
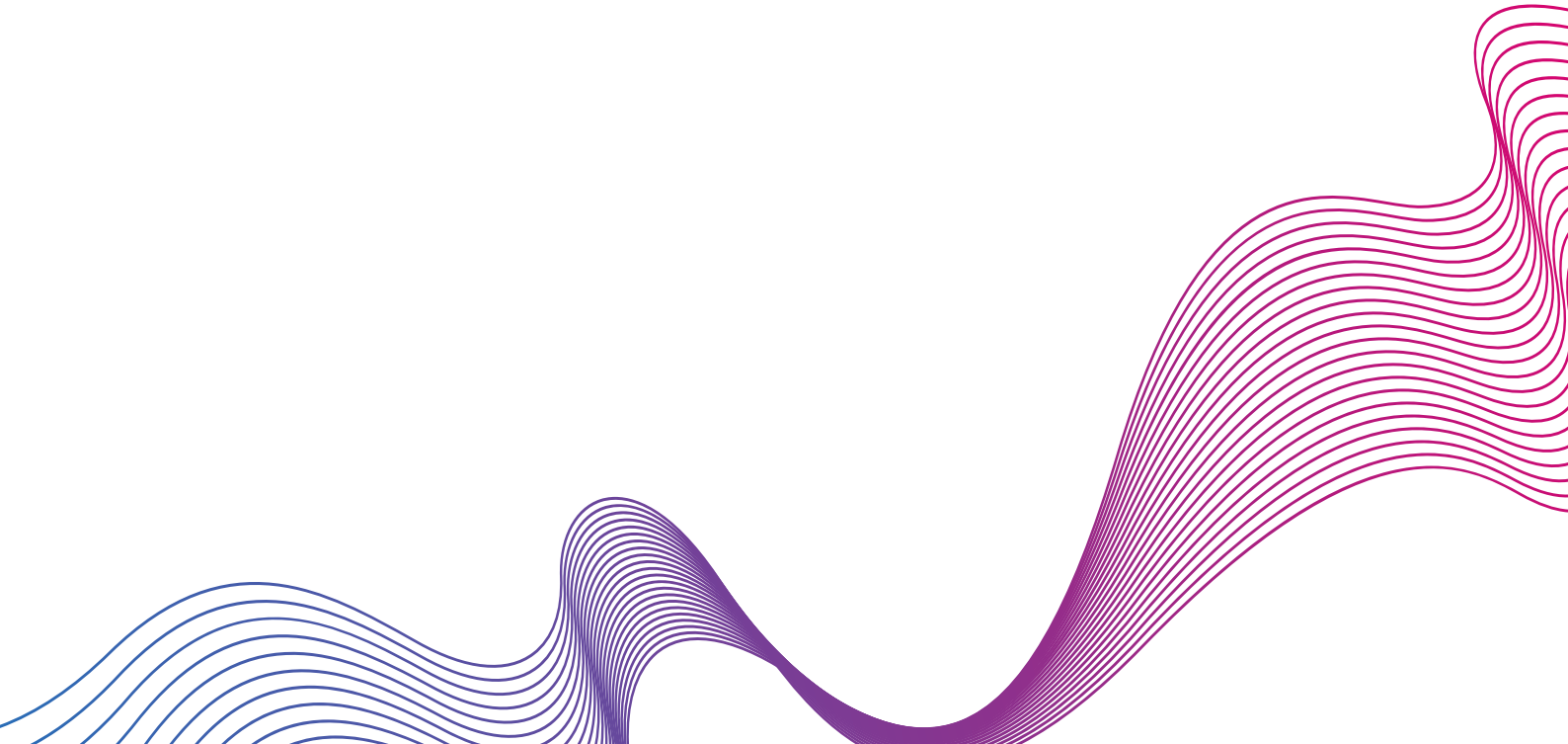
ManageEngine
AD360

5 imperatives
for an adaptive
security architecture



www.manageengine.com/active-directory-360

TABLE OF CONTENT



INTRODUCTION

THE WORLD OF CYBERSECURITY IS CHANGING FAST.

New challenges are arising as the old ways of protecting networks and data no longer suffice. The threat landscape changes by the minute, and adversaries are becoming more sophisticated every day. IT security teams can no longer focus on monitoring only endpoints, but must adopt a more integrated and proactive approach to security to remain effective in the coming years.

Adaptive security architecture (ASA) has been gaining traction in recent years as the need for a new approach to cybersecurity becomes more apparent. In this e-book, we will learn about an ASA and why you should consider implementing it as part of your defense strategy moving forward.

WHAT IS ADAPTIVE SECURITY ARCHITECTURE?

An ASA is a security model that emphasizes the need for security to be constantly evolving to keep up with the changing threats.

It is designed to be flexible and adaptable so that it can quickly respond to new threats as they emerge. An ASA relies on a variety of security controls, such as firewalls, intrusion detection and prevention systems, and anti-malware software. It involves a number of proactive measures, such as regular security audits, and vulnerability assessments.

ASA enables real-time monitoring and rapid responses to security issues, ensuring that organizations provide their customers and employees with peace of mind about data protection.

Many IT security teams focus on preventing cyberattacks and tend to embrace the incident response mentality instead of the continual response mindset that an ASA promotes. What is the difference between incident response and continual response? They both sound similar, but there are actually some key distinctions. Here's a closer look at each:

- Incident response is usually initiated in response to a specific event or threat. It's a more reactive approach that's taken when something has already happened. The goal is to contain the damage and minimize the impact of the incident.

- Continual response is a proactive approach taken on an ongoing basis. It's about consistently monitoring your systems and being prepared to respond to incidents before they happen. The goal is to prevent incidents from occurring in the first place, or at least minimize their impact if they do occur.

Many organizations need to shift from incident response to continual response. With this shift, security defense systems can preempt and monitor existing and potential threats, provide real-time feedback, and rapidly adjust existing security policies to secure an organization's networks. While these actions are still necessary, security teams should embrace adaptive security platforms, which are capable of adjusting to emerging threats and employing dynamic defenses and response mechanisms. As cyberattack strategies become more sophisticated through the use of automation and other tactics, organizations must adjust their methods for handling them.

COMPONENTS OF AN ADAPTIVE SECURITY ARCHITECTURE

There are four key components of **adaptive security architecture**

Visibility

The ability to see what is happening in the network and identify potential threats. This can be accomplished through tools like network monitoring and intrusion detection systems.

Automation

The ability to take action based on the information from the intelligence component. This could involve automatically blocking IP addresses that are known to be associated with attacks or quarantining files that contain malware.

Intelligence

The ability to understand what the data from the visibility tools are telling us. This requires analysts who can interpret the data and determine what it means in terms of security threats.

Response

The ability to quickly react to incidents when they occur. This includes having a plan for how to deal with an attack and being able to execute that plan quickly and effectively.

THE FOUR STAGES OF GARTNER'S ADAPTIVE SECURITY ARCHITECTURE

Gartner's adaptive security architecture is a framework that organizations can use to design and implement their security strategies. The framework is based on the principle of "defense in depth", a security strategy that leverages numerous security measures to protect an organization's assets from cyberattacks. Gartner's adaptive security architecture focuses on focuses on speed and agility, and it is designed to provide organizations with a flexible and scalable approach to security.

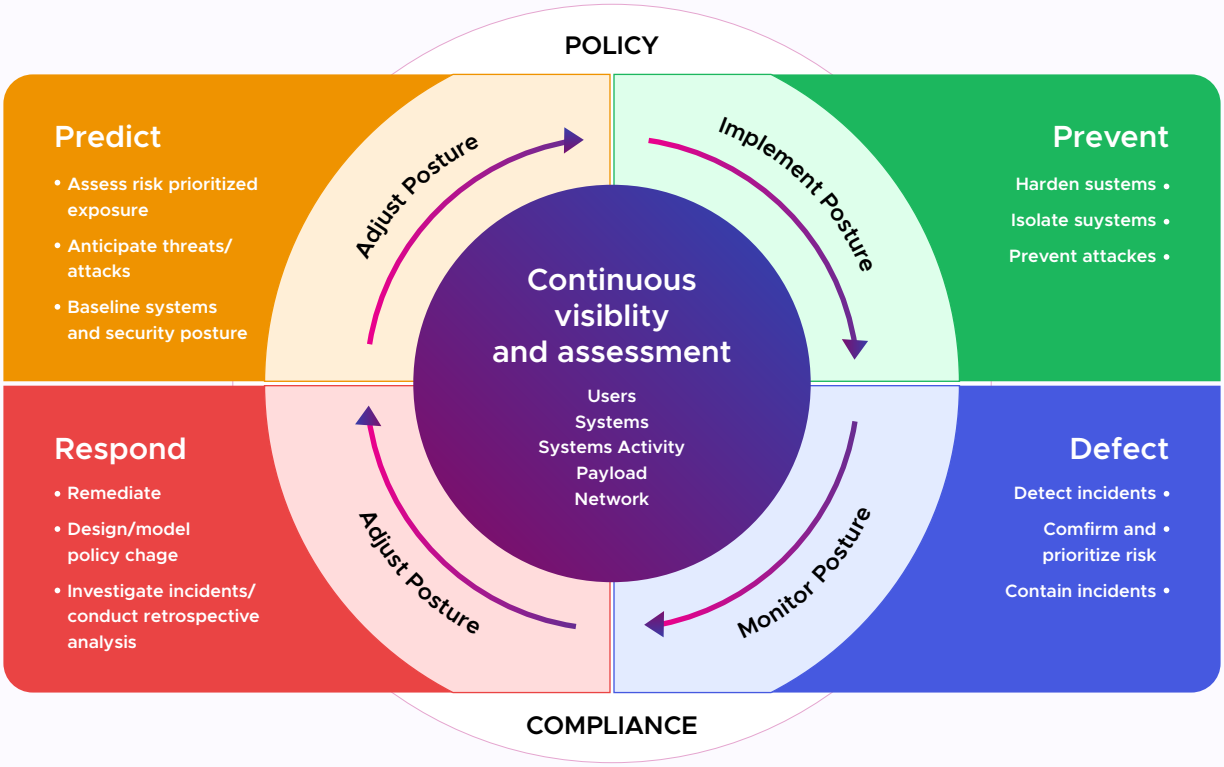
Gartner recommends a four-phased approach:

1. Detect: Security teams need to have visibility into all aspects of the IT environment to identify potential threats.

2. Respond: Once a threat has been identified, security teams need to be able to quickly assess the impact and take appropriate actions to mitigate the risk.

3. Predict: Security teams need to anticipate future threats proactively and take steps to prevent them from happening in the first place.

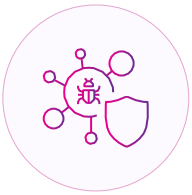
4. Prevent: In the event of a successful attack, security teams need to be able to harden and isolate systems to prevent security breaches, recover operations rapidly, and minimize business impact.



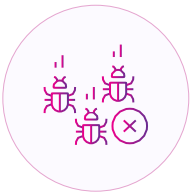
OBJECTIVES OF AN ASA

1. Bolstering security:
To provide a high level of security for the information and systems that are critical to the organization.

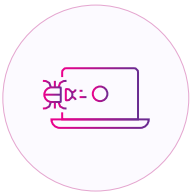
2. Adaptability:
To be able to rapidly adjust to changing security threats and vulnerabilities.



3. Reduce threat propagation:
To restrict the potential spread or lateral movements of a threat within a network.



4. Decrease attack velocity:
To reduce the rate of the attack when multiple assaults are taking place.



5. Narrow down the attack surface:
To make the target of an attack smaller.

6. Real-time response:
To be able to quickly and easily respond to new security threats and vulnerabilities.

CHALLENGES FACED BY ORGANIZATIONS AND HOW TO OVERCOME THEM WITH AN ASA

Organizations are challenged with discovering threats when they occur, addressing vulnerabilities swiftly, and continually improving their security posture, all while protecting critical data and their businesses.

Organizations need secure access to sensitive and confidential data, while improving their ability to analyze security data and identify attacks as they occur. With the fast-paced adoption of IoT, big data, and analytics, security risks are increasing, leading to the need for new strategies beyond the traditional approach of security.

By adopting the strategy to predict a threat before it happens, IT security teams can protect their organization's data, well before damage is done. The intent behind using a reactive security design approach is to anticipate threats before they occur. Unlike conventional approaches, the adaptive response model integrates alerts and threat information from multiple security domains and technologies. ASAs identify methods and techniques used by cybercriminals, and, in turn, leverage that information to prevent attacks.

An ASA integrates your organization's data across various security measures, such as anticipating threats, and providing full protection to the network and endpoints. It enables us to keep up with cybercriminals, build and enhance a security framework according to the current state of the threat landscape, and avoid massive losses to businesses.

An ASA is a mix of integrated tactics that helps organizations stay ahead of cybercriminals, triggering agile security measures that secure data and systems as nimbly as possible, instead of relying on legacy perimeter security strategies. Ideally, the most feasible security architecture helps to build a cybersecurity system that adapts continuously to the evolving challenges of the digital world. Your ASA autonomously learns from previous successes and failures in order to reach higher rates of success in terms of data protection and detection.

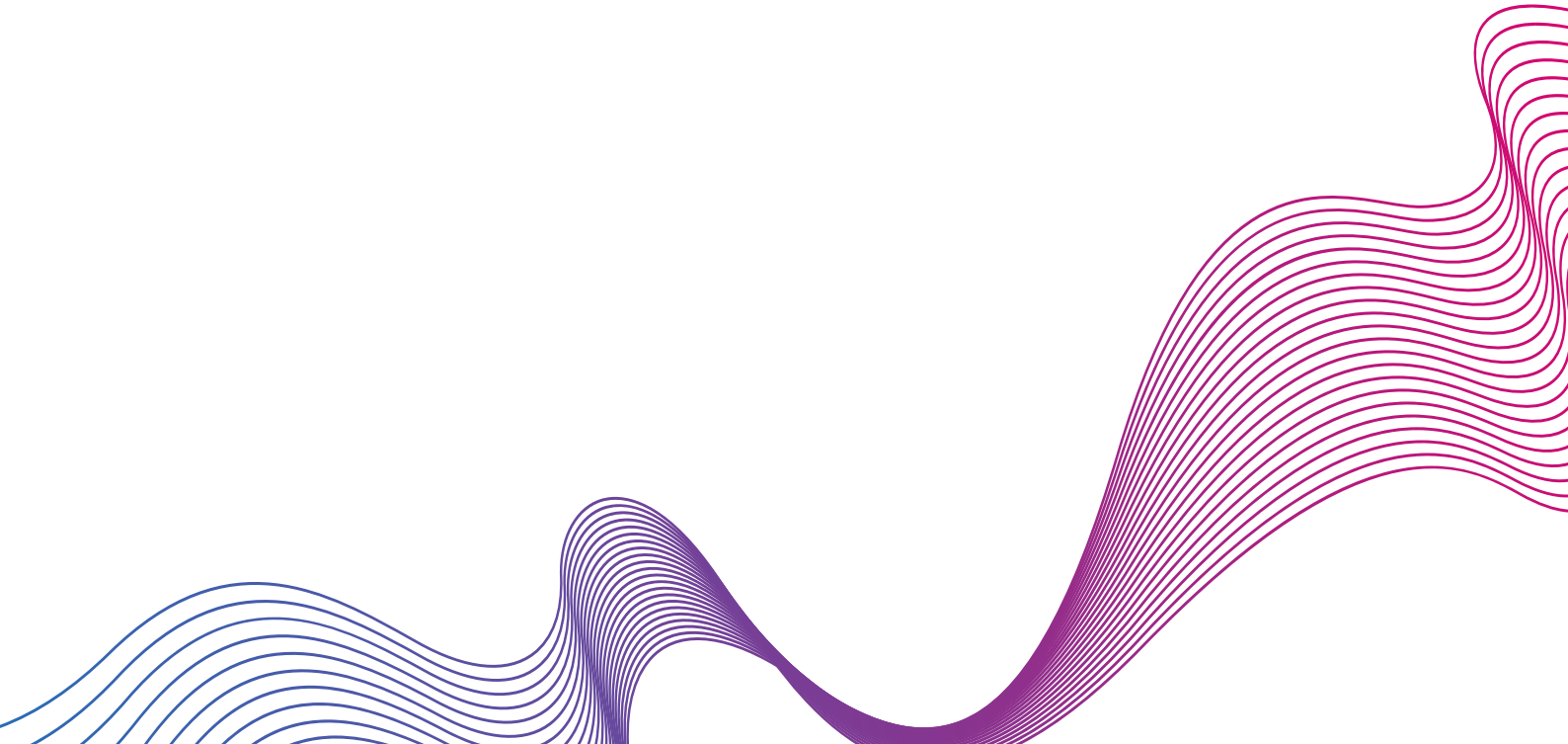
While traditional SIEM systems will still be needed to handle the detection of threats in real time, businesses need to begin to include systems focused on the domain-specific intelligence produced by an ASA. Innovations, such as artificial intelligence algorithms, can help cybersecurity products be more adaptive and learn when data and patterns in the systems behaviors are identified. Analytics-driven security can help organizations adjust to threats faster and react to them.

Advanced analytics can identify security breaches that are not apparent from monitoring a system on your own. It helps uncover ongoing patterns in user behavior, network, application behavior anomalies, fraudulent transactions, and other changes, by which real-time insights can be gained and future security threats can be countered. To enhance our technologies, we need to leverage data captured from pen tests and analysis of our current IT security infrastructure.

The results from assessments can be used to refine the security mechanisms, including adjustments in the machine learning processes. Machine learning can help a security team by automating many processes, such as the pattern recognition used in analytics. An ASA is efficiently illustrated with a system called user and entity behavior analytics (UEBA), which profiles users and network devices to understand what constitutes normal behavior, then highlights abnormalities as they arise. Adaptive security solutions study patterns and behaviors, instead of simply reviewing log files, monitoring checkpoints, and responding to alerts.

An ASA must be able to protect the organization's critical assets from a variety of threats. It must be able to detect and respond to new threats as they emerge. And it must be able to continuously improve the security posture of the organization. Achieving these objectives requires a comprehensive approach that includes people, processes, and technology.

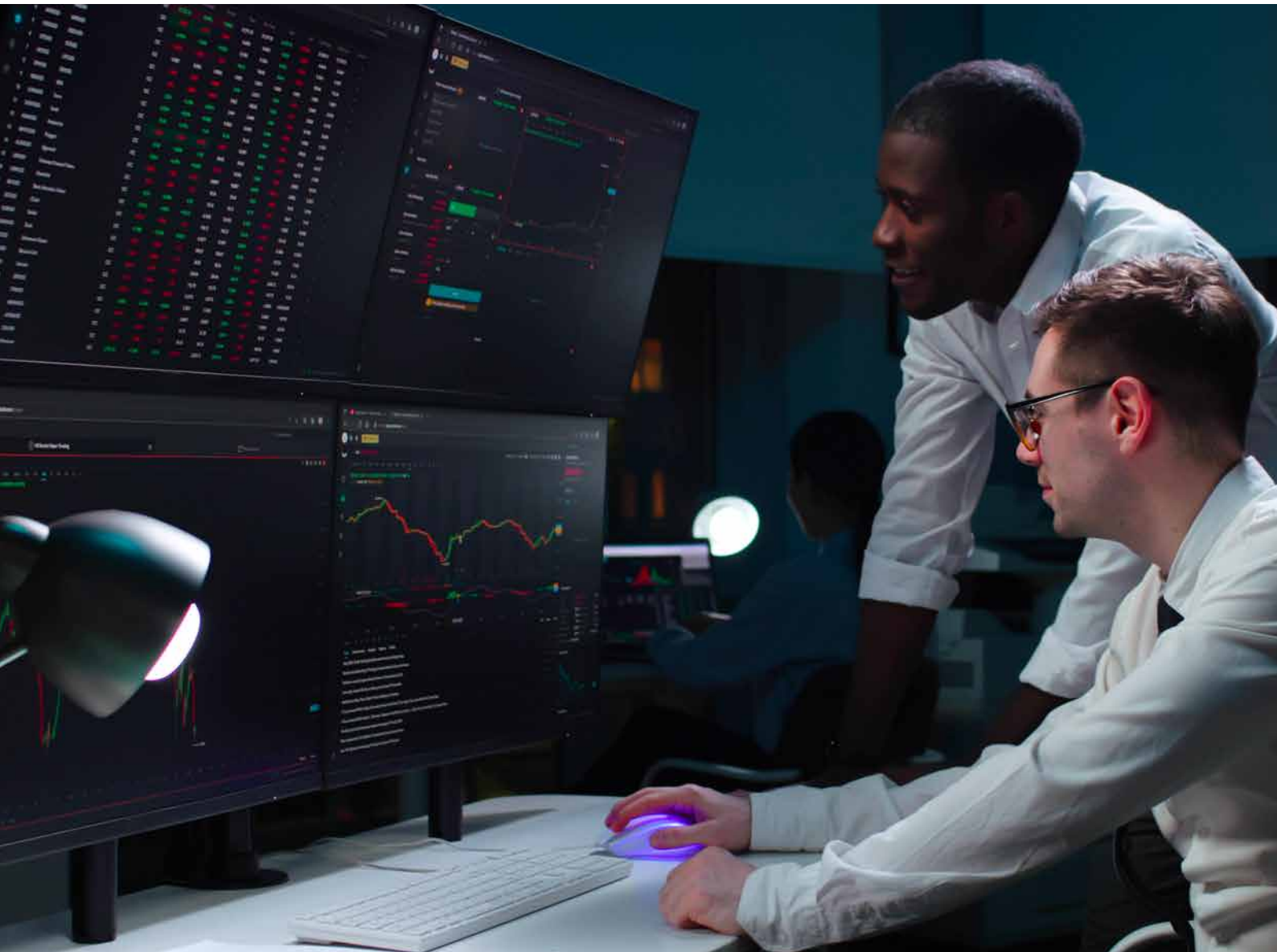
People are the most important element of an ASA. They are responsible for identifying and protecting the organization's critical assets. They are also responsible for detecting and responding to security threats. Processes are needed to ensure that people follow the proper procedures for identification, protection, detection, and response. Technology is needed to automate and improve the efficiency of these processes.



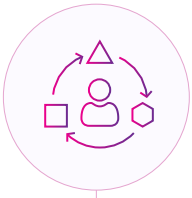
DETERMINING WHAT NEEDS PROTECTING

The first step toward developing a robust security architecture for an organization is to understand what needs protecting and the associated risk. The most basic question you should ask is which assets need to be protected and where they are located? This question defines what is included in the scope of the security architecture and helps to identify the key players that are responsible for providing protection.

Assets can be both tangible and intangible; they can be data, people, or organizations. Depending on the business, different assets are likely to be more important than others. In addition to the type of assets, you should also consider the risk associated with each asset and the impact that loss of the asset would have on the business.



5 KEY ELEMENTS TO CONSIDER WHEN IMPLEMENTING AN ASA



1. Adaptability

A key challenge to security is the constant threat of an attack. A security solution that is tightly integrated and highly customized may not be able to respond to the constantly evolving threats as quickly. This is where the concept of adaptability is important. The ability to be able to identify and to integrate components that can be easily modified or shifted to meet new threats is essential. The security architecture should have the ability to respond to threats by adding new functionality, removing components that are not needed, and shifting the relationships between components. To achieve this, the security architecture should use open, modular, and standardized components. Open components are components that can support a wide range of functionality. Modular components are self-contained units that perform a specific function and can be used in a variety of different contexts. Standardized components are components that are built to a standard specification.

2. Resilience

Business continuity and disaster recovery are important aspects of security architecture. In the event of a disaster, the systems should have the ability to recover from the incident. This requires a detailed understanding of the impact of a disaster, such as a power outage or data breach, and how an organization will recover from it. The impact of a disaster could be the shutdown of a specific system, the unavailability of data, or the loss of critical resources. The business continuity and disaster recovery requirements drive the selection and implementation of the security features. The security architecture should have a strategy to protect against events that could disrupt business continuity. The architecture should also have a strategy to recover from incidents that disrupt business continuity.

3. Governance

A well-designed security architecture is built on solid foundations. It has the right components, is well-integrated, and can protect against attacks. However, if the governance of the architecture is not well-implemented, the architecture will not be as effective. The governance of the security architecture includes the processes, standards, and controls that are used to manage the architecture. It is important to have a governance model that clearly identifies who is responsible for what part of the security architecture. It is also important to ensure a consistent approach to managing the architecture across the organization by having a common set of standards. A consistent approach enables the architecture to be managed more effectively, reducing the risk of misconfiguration or errors.

4. Visibility

The security architecture should be built with an understanding of how it all works together, as well as how it comes together. An important part of this is to understand which components are used, how they are configured, what data flows between them, and how data is transformed as it passes between components. The visibility into the security architecture provides an indication of how effective the architecture is. A visual representation of the architecture can be useful in understanding which components are used, how they are configured, and the data flows between them. The visibility should be monitored continuously to identify any issues or risks that may arise and to understand any changes in the system.

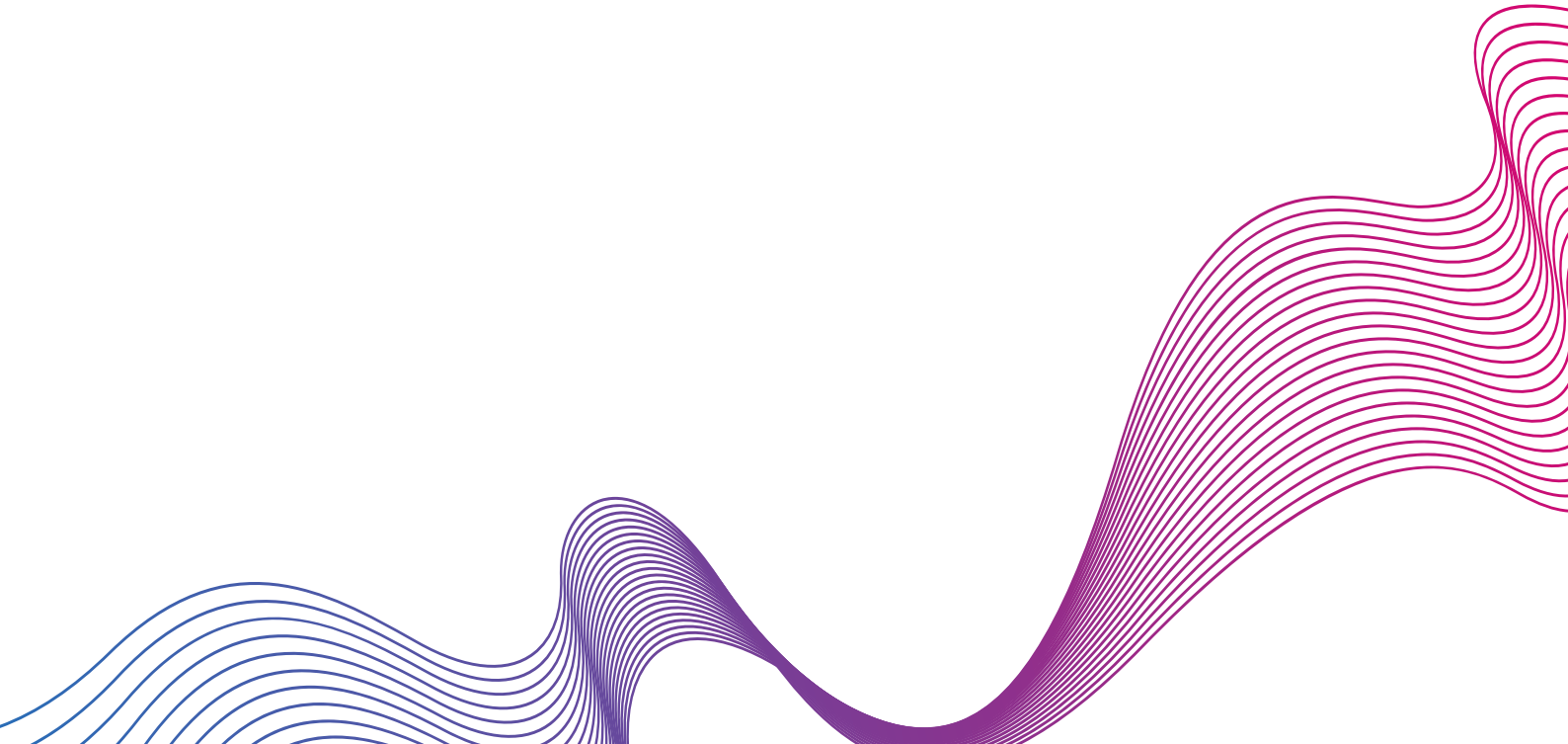
5. Unified view of the environment

A unified view of the IT environment is essential for understanding how it all works together. This includes understanding the relationship between the assets, the security controls, and the risks they face. A unified view of the environment provides a high-level overview of the assets and risks in the environment, as well as the key relationship between them. It also enables you to identify areas that could be improved or modified.

The most efficient way to achieve a unified view of the environment is through modeling.

Modeling is the process of using a visual representation of your environment to identify assets, dependencies, risks, and interconnections between hardware and software components. It provides a view of the entire environment, including its people, processes, and technology. There are many types of modeling that can be used for this purpose, such as diagramming and modeling the environment. Diagramming is the process of creating a visual representation of an environment that helps to understand the key relationships between the different components.

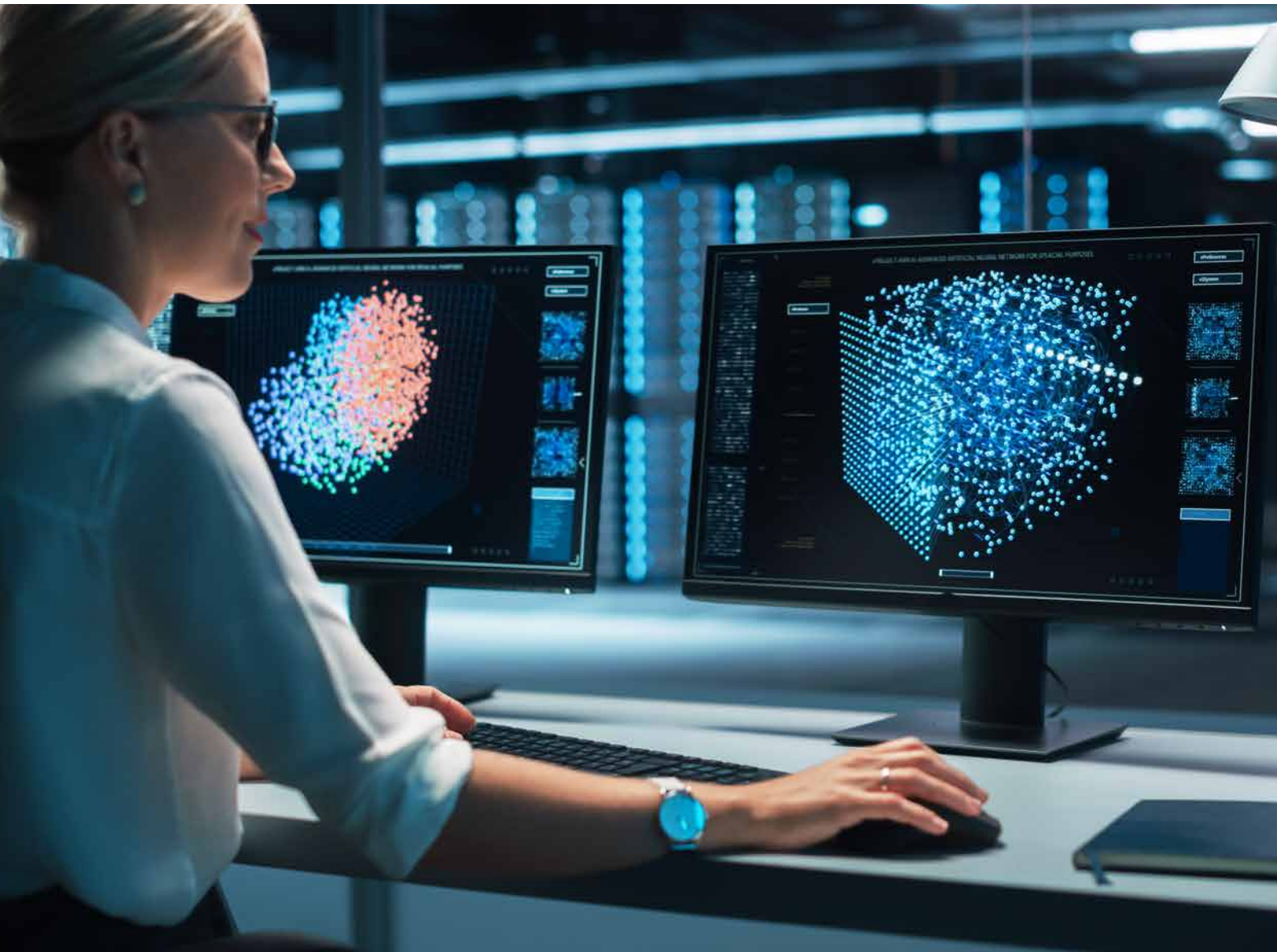
As we have seen, an ASA is more than just implementing specific security features within a system. The main objective of adaptive security is to establish a feedback loop of threat awareness, threat detection, and prevention, a process that continually becomes more effective. It involves developing a detailed blueprint of how the system's security features should be implemented and configured to provide specific security services. While many organizations recognize the importance of good security architecture, not all are fully aware of what is necessary to build a truly secure system. By understanding the above five elements of ASAs, you can create a blueprint for a secure system that is able to meet evolving threats and challenges.



IMPLEMENTING AN ASA WITH THE HELP OF MANAGEENGINE AD360

AD360 is a holistic identity governance, security, and access management solution. From managing your user identities, governing access to resources, user provisioning, self-service password management, UEBA, adaptive authentication, and SSO, the solution helps organizations build an adaptive security architecture which can be managed by a simple, easy-to-use web interface.

Various systems, such as Windows Active Directory, Exchange Servers, Office 365 and more can be governed, monitored, audited, and secured with AD360.



15 Gartner recommended IAM critical capabilities in AD360:

1

Identity lifecycle management & fulfillment

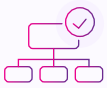
Assets can be both tangible and intangible; they can be data, people, or organizations. Depending on the business, different assets are likely to be more important than others. In addition to the type of assets, you should also consider the risk associated with each asset and the impact that loss of the asset would have on the business.

2

Entitlements management

Eliminate redundancy and human errors, and improve business processes by automating entitlements management with context-aware privilege delegation.

3



Approval-based workflows

Capability to build purpose-oriented business workflows. Create the required levels of approval—requester, reviewer, approver, and executor— for the right stakeholders.. Define the approval flows for business processes such as user account creation, modification, permissions management and more.

4

Real-time change auditing

Get audit reports for privileged user activity, insider threat detection and root cause analysis. Monitor and get notified on logons activity, ACL and password changes. Also, audit Azure AD, removable storage, workstation, server, file & folder. Generate out-of-the box reports for GDPR, SOX, PCI, HIPAA, FISMA, GLBA.

5

Policy and role management

Supports role-based access control which lets admins define and assign granular roles for stakeholders, enforce policy of least privilege, and segregate duties on privileged accounts to prevent privilege escalation.

6

Access Certification

Review user access rights using detailed reports and ensure that the access complies with internal security policy.

7

User Authentication Methods

Avoid impersonation attacks using biometric, and other advanced authentication methods. Step up your security by implementing MFA to end points and applications.

8

Adaptive authentication

Risk-based adaptive authentication using factors such as user location, IP address, time of previous logon, device footprint and more.

9

SaaS Application Enablement

Supports SAML 2.0-based SSO to hundreds of enterprise SaaS applications like Salesforce, ServiceNow, Slack, and more.

10

Nonstandard Application Enablement

Supports custom scripts that facilitate identity provisioning for in-house applications. Go beyond mainstream target systems like Active Directory, Azure AD, Office 365 and extend AD360's IAM capabilities to ServiceNow, Salesforce and other third-party applications.

11

Access requests

Supports self-service group management through which users can request membership to AD groups to gain access to a set of specific IT resources. By enabling approval workflow rules for self-service group management, application and resource owners can control who gets to be a member of a particular group.

12

Reporting and ML-based user behavior analytics

Review user access rights using detailed reports and ensure that the access complies with internal security policy.

13

Ease of deployment

No prerequisites or complicated deployment. Start managing identities in your on-premises, cloud, or hybrid IT environment within minutes.

14

API Target Enablement

The AD360 REST APIs facilitate sharing of data between AD360 and any third-party application or web service.

15

High availability

It supports high availability in case of system and application failures. High availability is achieved through automatic failover; when the AD360 service running on one machine fails, another instance of the AD360 service running on a different machine will automatically take over.

ManageEngine
AD360

AD360 is an integrated identity and access management (IAM) solution for managing user identities, governing access to resources, enforcing security, and ensuring compliance. From user provisioning, self-service password management, and Active Directory change monitoring, to single sign-on (SSO) for enterprise applications, AD360 helps you perform all your IAM tasks with a simple, easy-to-use interface. With AD360, you can just choose the components you need and start addressing IAM challenges across on-premises, cloud, and hybrid environments from within a single console.

For more information about AD360, please visit www.manageengine.com/ad360.

$ Get Quote Download