Illumio Adaptive Security Platform® (ASP) and NIST

Executive Summary

The NIST Cybersecurity Framework ("Framework" or "CSF") has become an essential tool for organizations taking steps to manage cybersecurity risk. The Illumio Adaptive Security Platform (ASP) helps organizations implement the Framework by providing advanced technology that addresses four of the five core Framework Functions: Identify, Protect, Detect, and Respond.

Identify (ID)

This Function supports developing an organizational understanding of cybersecurity risk to systems, assets, data, and capabilities.

Illumination, a core component of Illumio ASP, provides real-time application dependency mapping as a first step toward defining and enforcing micro-segmentation policy. Illumination maps workloads, applications, and flows to clearly show connections between all the systems and applications within its scope. Illumination remains accurate even in highly dynamic and complex cloud and data center environments and can be used to identify critical high-value assets and opportunities to reduce the attack surface. Illumio ASP is relevant to the following NIST Identify Subcategories:

ID	Description
ID.AM-3	Organizational communication and data flows are mapped
ID.BE-4	Dependencies and critical functions for delivery of critical services are established
ID.GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
ID.AM-1	Physical devices and systems within the organization are inventoried
ID.AM-2	Software platforms and applications within the organization are inventoried
ID.AM-4	External information systems are catalogued
ID.BE-5	Resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations)

Protect (PR)

This Function supports implementing appropriate safeguards to ensure the delivery of critical infrastructure services.

Illumio ASP enforces least privilege functionality, imposing granular and tailored micro-segmentation and eliminating unneeded communications between hosts and applications. All traffic between hosts and applications can be encrypted, including communications within an organization's networks and across public networks. Illumio ASP is relevant to the following NIST Protect Subcategories:

ID	Description
PR.PT-3	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
PR.AC-5	Network integrity is protected, incorporating network segregation where appropriate
PR.DS-2	Data-in-transit is protected
PR.AC-3	Remote access is managed
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
PR.DS-1	Data-at-rest is protected
PR.DS-5	Protections against data leaks are implemented
PR.DS-7	The development and testing environment(s) are separate from the production environment
PR.MA-2	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
PR.IP-7	Protection processes are continuously improved

Detect (DE)

This Function supports the timely discovery of cybersecurity events.

Illumio ASP identifies system communications, establishing a baseline of operations and data flows; once a baseline is established, security policies are defined and enforced. Illumio ASP provides real-time data on workload communications and the impact of any workload or application becoming unavailable. The understanding and control offered by micro-segmentation also enables adaptive capabilities in the area of incident response. Illumio ASP is relevant to the following NIST Detect Subcategories:

ID	Description
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed
DE.CM-1	The network is monitored to detect potential cybersecurity events
DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events
DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed
DE.AE-3	Event data are aggregated and correlated from multiple sources and sensors
DE.AE-4	Impact of events is determined
DE.DP-5	Detection processes are continuously improved

Respond (RS)

This Function supports implementing appropriate activities to detect, respond to, and contain the impact of a potential cybersecurity event.

Illumio ASP helps to quickly change or restrict communication paths between workloads, preventing lateral movement until the attackers are removed from the systems. Illumio ASP also helps organizations build and enhance understanding about what systems hold critical data or provide critical services. Once in place, it can validate this mapping by showing how systems communicate in real time. Additionally, systems can be configured to respond automatically during an event. Illumio ASP is relevant to the following NIST Respond Subcategories:

ID	Description
RS.RP-1	Response plan is executed during or after an event
RS.AN-3	Forensics are performed
RS.MI-1	Incidents are contained
RS.MI-2	Incidents are mitigated
RS.AN-1	Notifications from detection systems are investigated
RS.AN-2	The impact of the incident is understood

Conclusion

Illumio ASP reduces cybersecurity risk by helping organizations optimize the Identify, Protect, Detect, and Respond Functions of the NIST Framework. It gives cybersecurity decision makers and implementers the necessary knowledge to best use the product's features and capabilities in an environment where the NIST Framework is central to the overall risk management of the organization.

About Illumio

Illumio, the leader in micro-segmentation, prevents the spread of breaches inside data center and cloud environments. Enterprises such as Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite use Illumio to reduce cyber risk and achieve regulatory compliance. The Illumio Adaptive Security Platform® uniquely protects critical information with real-time application dependency and vulnerability mapping coupled with micro-segmentation that works across any data center, public cloud, or hybrid cloud deployment on bare-metal, virtual machines, and containers. For more information about Illumio, visit www.illumio.com/what-we-do or follow @Illumio.

Illumio, Inc. 920 De Guigne Drive, Sunnyvale, CA 94085 Tel (669) 800-5000 www.illumio.com