MENLO SECURITY

Compliance Brief

Securing organizations with a Zero Trust approach under the NIST Framework

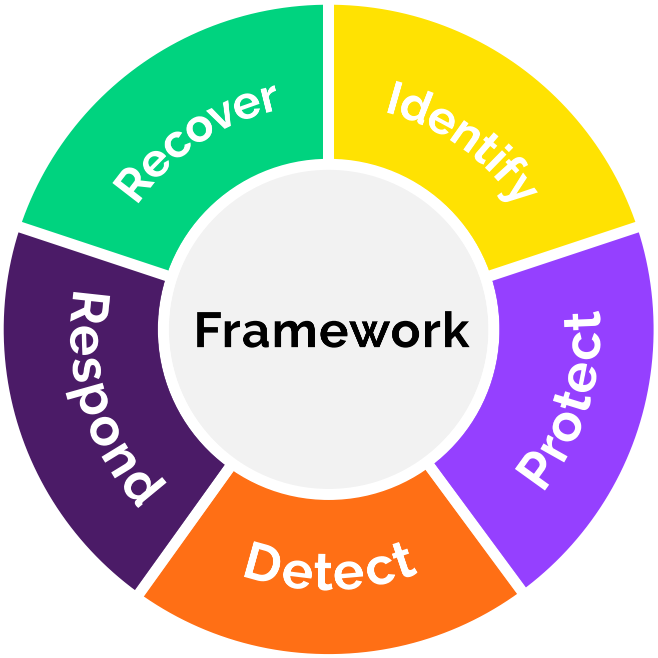
Digital transformation is happening. Remote work is the new normal. With these technology shifts come enhanced access to primary attack vectors. Highly Evasive Adaptive Threats (HEAT) are on the rise.

HEAT attacks are a class of cyberthreats that leverage web browsers as an initial access vector, employ various evasion techniques that bypass traditional cloud security stacks, and deliver malicious web content such as browser exploits, malware files, and phishing pages. Protecting organizations against HEAT attacks requires threat prevention. Traditional methods of cybersecurity that rely on a detect-and-respond approach are no longer enough. Prevention means stopping the attack at the initial access before it reaches the network or endpoint. Aligning with the National Institute of Standards and Technology (NIST) Cybersecurity Framework and focusing on the controls for information protection for your organization builds a Zero Trust model for cybersecurity to prevent HEAT attacks from impacting your users or data.

NIST Framework prevents malware surge

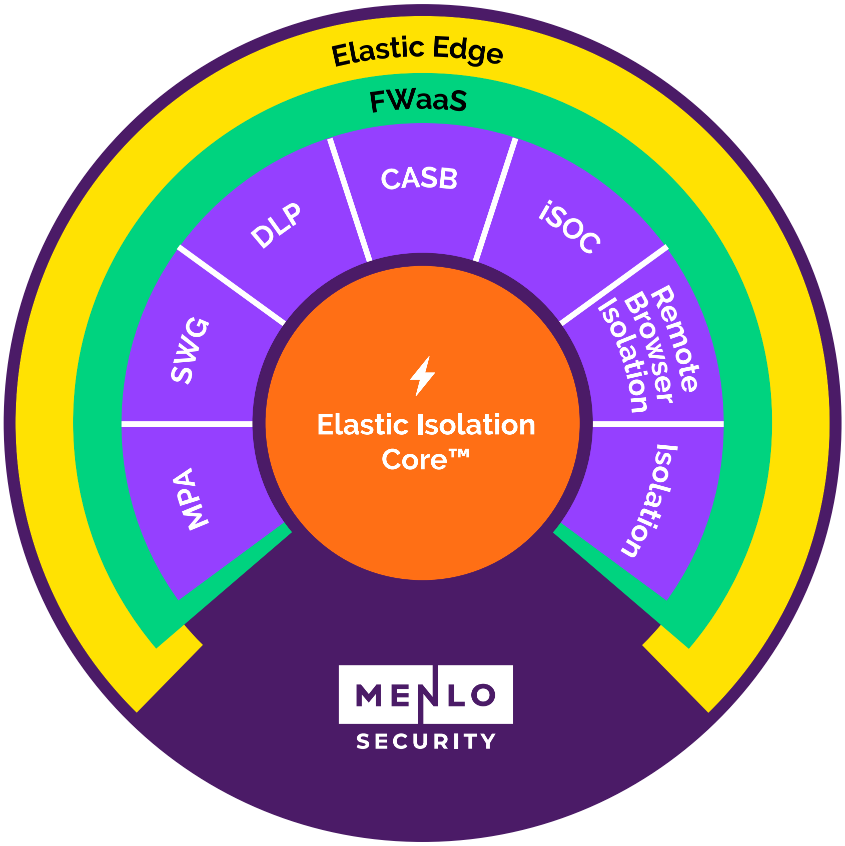
NIST is a unit of the U.S. Commerce Department. NIST 800-53 is a regulatory standard that defines the minimum baseline of security controls for all U.S. federal information systems, except those related to national security. The purpose is to help improve the security posture of systems used within the federal government, but these controls have become the primary framework by which many reputable security organizations measure their solutions.

Originally established in response to former President Obama's executive order for Improving Critical Infrastructure Cybersecurity, the NIST Framework was developed as a collaboration between the public and private sectors to help identify, assess, and manage cyber risk. NIST has become the gold standard framework for organizations to assess their cybersecurity maturity, recognize security gaps, and meet cybersecurity regulations. The NIST Framework integrates a layered approach of five functions necessary for managing cyber risk. These functions include Identify, Protect, Detect, Respond, and Recover. Building a cyberstrategy aligned to the NIST Framework prevents sophisticated threats like HEAT attacks. The Protect function limits or contains the impact of a potential cybersecurity event.



The NIST Framework is highly trusted for many reasons, some of which include:

- FISMA and FedRAMP are based on compliance with NIST SP 800-53 guidelines.
- Following NIST guidelines improves the security rating of an organization.
- Organizations who follow NIST guidelines improve their compliance with other regulations, such as HIPAA (Health Insurance Portability and Accountability Act) and SOX (Sarbanes-Oxley Act).
- Aligning with NIST guidelines helps prevent Highly Evasive Adaptive Threats (HEAT), ransomware, and other highly sophisticated malware from targeting your users.



Menlo Security enables a Zero Trust approach to support the NIST Framework

Zero Trust cybersecurity is now top of mind for organizations. Zero Trust is both a strategy and a mindset. It requires organizations and users to view cybersecurity differently. Zero Trust minimizes risk by assuming all interactions are dangerous until proven otherwise. It also ensures that even after access has been granted, an entity — whether human or automated — should never be considered non-malicious and free of malware.

Just like threats such as HEAT attacks have become more sophisticated, your approach to cybersecurity must do so as well. An approach that is preventative rather than reactive is necessary to stay ahead of these types of attacks. All designed in support of the NIST Framework, Menlo Security's preventive technologies use isolation technology, Secure Web Gateway (SWG), Data Loss Prevention (DLP), and Cloud Access Security Broker (CASB) capabilities combined into a single platform, provide easy management and reporting.

Security that is powered by isolation executes the Zero Trust concept by never allowing web, application, or email content to reside on end-user devices. Instead, the traffic is isolated in the cloud within a disposable container — separated by a virtual "air gap" — which presents to users an image of the content, not the content itself. Isolating at the source of the threat means the attack never happens.

As your organization transitions from reactive approaches to proactive strategies, the Menlo Cloud Security Platform — the only solution powered by an Isolation Core™ — can work seamlessly with your existing security solutions. This will allow you to move quickly to a highly secure, Zero Trust framework that enhances both protection and productivity. The Menlo platform integrates easily into your existing security stack and is designed in alignment with the NIST Framework to help you achieve both the compliance and the protection you need with a Zero Trust model. Adding the power of isolation to whatever security capabilities you already have in place allows you the freedom to work with no fear of the impacts of HEAT attacks.

The Menlo Cloud Security Platform helps organizations achieve NIST Cybersecurity Framework compliance by providing enterprise-grade security capabilities that correspond to Zero Trust and NIST 800-53 guidelines. Our solutions align to the NIST Framework:

- Secure Web Gateway
- SSL Inspection
- Secure Browser Isolation
- Cloud Access Security Broker (CASB)
- Data Loss Prevention (DLP)
- Private Access
- Firewall-as-a-Service
- Threat Insights and Risk Scoring

To find out more, contact us:

menlosecurity.com
(650) 695-0695
ask@menlosecurity.com

About Menlo Security

Menlo Security enables organizations to eliminate threats and fully protect productivity with a one-of-a-kind, isolation-powered cloud security platform. It's the only solution to deliver on the promise of cloud security—by providing the most secure Zero Trust approach to preventing malicious attacks; by making security invisible to end users while they work online; and by removing the operational burden for security teams. Now organizations can offer a safe online experience, empowering users to work without worry while they keep the business moving forward.

© 2022 Menlo Security, All Rights Reserved.