anjuna

Anjuna Delivers a 77:1 Advantage Against the MITRE ATT&CK MATRIX

Executive Summary

The MITRE ATT&CK MATRIX delivers a framework that enables CISOs to assess and improve their ability to detect and mitigate a wide range of attacks on the enterprise. This knowledge base of adversary tactics and techniques is founded on real-world observations. It aids in developing specific threat models and methodologies across the business, government, and cybersecurity arenas.

However, this approach results in a constant, ongoing game of "whack-a-mole" as enterprises continuously adjust their technology, processes, and people to respond (albeit belatedly) to rapidly changing attack surfaces and threat profiles.

Confidential Cloud Software Raises Security Quality and Effectiveness Against MITRE ATT&CKS

To address this situation and enhance the effectiveness of attack interception and mitigation, all major cloud vendors have implemented technology that transforms the public cloud to deliver Confidential Cloud Computing environments using public cloud infrastructure. This approach employs secure enclave technology to enable the creation of a trusted execution environment (TEE), which is based on hardware security features provided by CPU vendors. This encompasses technologies such as encryption/decryption within the CPUs, memory and data isolation, or additional security features that vary by CPU vendor.

By converting your public cloud leveraging these Confidential Computing technologies, entire classes of MITRE attacks are no longer possible, as the entire attack surface is shut down by default. For example, many attacks maintain a command line in their attack chain. With a Confidential Computing-secured cloud environment, there is no command line. Thus, any command line-based attack (no matter how ingenious) is ineffectual.

77 Attacks: Anjuna MITRE ATT&CK MATRIX Security Analysis

Anjuna Security evaluated the complete MITRE ATT&CK MATRIX and discovered 77 MITRE attacks that Confidential Computing can shut down forever through secure enclaves. This supersedes and surpasses conventional mitigation to deliver total prevention by default.

How many other actions can an entity take to completely eliminate all 77 potentially devastating attacks in perpetuity? Anjuna's Confidential Cloud Software can perform this feat in minutes.

Hardware-Grade Security Becomes the New Standard

Given the recent availability of unprecedented levels of hardware-grade protection, today's enterprises are increasingly turning to Confidential Computing (secure enclaves) as the future of security on the public cloud. Now, Anjuna Confidential Cloud Software makes it easy to deploy secure private environments that are built on public cloud infrastructure from AWS, Microsoft Azure, Intel, AMD, and others.

That means enterprises can ensure trust by protecting sensitive workloads on any cloud, anywhere. Anjuna's software implements Confidential Computing technology in minutes to create private environments that protect sensitive applications and data from unauthorized insiders, threat actors, and malicious processes, including an actual physical machine breach!

Preemptively Mitigating the Top Five Attacks

Before diving deeper into the details of how Anjuna Confidential Cloud Software stops attacks, let's explore the fundamentals—the most virulent, top attacks that can be mitigated for an enterprise. If the attacks here concern you, read on—there are 72 more! As stated, Anjuna can provide 72 additional examples. Every security organization needs to protect itself against the many variations of these attacks that are constantly released.

Deployment of Anjuna Confidential Cloud Software means that enterprises—protected by default—no longer need to be concerned about these attacks or their thousands of iterations. Implementing Anjuna's software delivers the highest possible return on security investment to the enterprise.

Attack	Public Attack Examples	How CC stops the Attack	References	MITRE Ref
Command shells can invoke virtually any executable on the system to launch attacks, including ransomware	2016 attack on Brazil Olympics; commonly used in ransomware	Anjuna ensures that only intended applications & data can be executed	ZeuS Panda FiveHands Ransomware	T1059: Command and Scripting Interpreter
Adversaries modify client software binaries to establish persistent access to systems that evade virus scanners	Stuxnet is the most famous example of this attack. It was used by the U.S. on Iranian nuclear PLC machines. Also used to attack the UK National Health Service and 100 online gaming companies	Anjuna enforces policies that ensure only trusted binaries can run	Stuxnet | CovidLock: Android Ransomware Walkthrough and Unlocking Routine | Computer Virus Cripples UK Hospital System | Chinese Antivirus Firm Was Part of APT41 'Supply Chain' Attack	T1554: Compromise Client Software Binary
Attackers may place files on a host that appear to be legitimate application files by naming them the same as regular application files	Attacks on International Atomic Energy Agency, Korean Government. All major U.S. cell phone carriers, etc.	Anjuna Isolates the OS from an application and its data. Even if a machine is attacked, both the data and application running in a confidential compute environment on that machine are not accessible	North Korean APT Is Targeting South Korean Officials With AppleSeed Backdoor | Trickbot | New Ramsay malware can steal sensitive documents from air-gapped networks	Masquerading
Adversaries may exploit software vulnerabilities in client applications to execute code locally and remotely	Log4J (notoriety speaks for itself). Over 200 of these exploits have been cataloged	Anjuna isolates the application from both the hardware and OS	A Study of RATs	Exploitation for Client Execution
Modifying boot sequence of a machine gives the attacker boot-level access	Well-known in numerous attacks with many variations	Anjuna separates the protections of a machine from that of an application. An isolated environment is created by the hardware—not the software	What is a Boot Sector Virus?	BootHole GRUB bootloader bug lets hackers hide malware in Linux, Windows

Fundamentals of the MITRE ATT&CK MATRIX

The MITRE ATT&CK MATRIX is a catalog of strategies and tactics used by adversaries against computer systems. By cataloging the attacks, MITRE not only provides a comprehensive list of attacks but also organizes them by attack type most relevant to security professionals. Forewarned is forearmed. The MITRE ATT&CK MATRIX is a valuable resource for evaluating threat campaigns confronting your organization and the most effective strategies for responding to them.

Anjuna examined all of the attacks in the MITRE Matrix and determined which of them are completely eliminated by default. Chapter 5 catalogs all 77 of them, including the five described above.

How Anjuna Confidential Cloud Software Eliminates MITRE Attacks

Anjuna Confidential Cloud Software does not merely mitigate MITRE attacks—it halts them permanently by default before they start, no matter how cleverly they are implemented or adapted. This fact speaks to the core value of Confidential Computing; it's why hardware vendors are adding the capability to their latest offerings and why cloud vendors deploy that hardware. By separating the protections of a machine from those of an application, Anjuna's software enables isolated environments on the public cloud that provide hardware-based attack mitigation for the first time.

An attacker with access to a machine may stop an environment from being started—but once it is created by hardware, the attacker cannot change the contents. Anjuna uses hardware attestation to measure an application and ensure it has not been tampered with. After the environment is created—even with root access to the machine—the attacker cannot access the data or application running in the isolated environment. This fact highlights the total security transformation enabled by Anjuna.

Anjuna Confidential Cloud Software Advantages

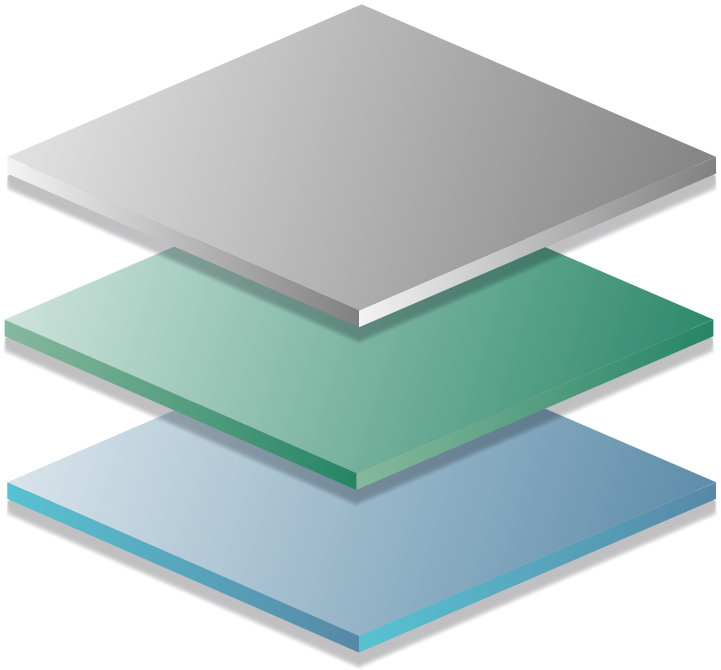
Anjuna delivers software that creates isolated environments on any cloud. By taking advantage of cryptographic and isolation capabilities in the latest CPUs and hardware, Anjuna allows enterprises to isolate their applications and data from other applications and data in ways that were previously available only on custom hardware. Using these special compute environments, enterprises can eliminate whole classes of attacks, keeping effective protections in place even if a machine is compromised.

Mitigate Risk with Data Protection-in-Use

Anjuna leverages the Confidential Computing capabilities provided by CPU enhancements, also known as protection-in-use. In addition to protection-at-rest and protection-in-motion, this allows for integration with other enterprise security software, including key management systems, SIEMs, cloud monitoring systems, and others. Taken together, these capabilities allow Anjuna to separate the ability to access an application or its data from the ability to run an application.

This represents a major shift in how we think about computer architecture to mitigate attacks. Anjuna's Confidential Cloud Software simply and automatically enables enterprises to build isolated private environments across every major cloud and hardware vendor infrastructure. Investing in Confidential Computing software delivers the highest possible attack prevention ROI: one simple software implementation covers 77 attack categories and thousands of individual attacks.

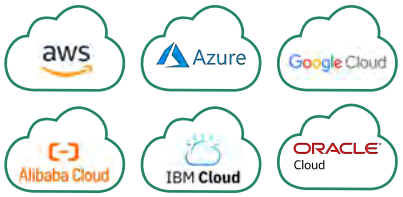
Anjuna Confidential Cloud Software Operational Configuration



Any Application
Traditional | Cloud-Native

anjuna

Any **Infrastructure, Cloud,** Or **Secure Enclave**



Intel SGX | AMD SEV
AWS Nitro Enclaves

Appendix: Techniques That Anjuna Mitigates

The following is a list of the MITRE attacks that Anjuna mitigates by default. Each attack has many different implementations, so in practice, these 77 cover thousands of attacks in the real world.

To understand in more detail how Anjuna mitigates these attacks, please contact us at info@anjuna.io or www.anjuna.io

T1003: OS Credential Dumping
T1011: Exfiltration Over Other Network Medium
T1020: Automated Exfiltration
T1021: Remote Services: Distributed Component Object Model
T1027: Obfuscated Files or Information
T1036: Masquerading
T1040: Network Sniffing
T1046: Network Service Scanning
T1047: Windows Management Instrumentation
T1052: Exfiltration Over Physical Medium
T1059: Command and Scripting Interpreter
T1068: Exploitation for Privilege Escalation
T1070: Indicator Removal on Host
T1072: Software Deployment Tools
T1078: Valid Accounts
T1080: Taint Shared Content
T1091: Replication Through Removable Media
T1092: Communication Through Removable Media
T1098: Account Manipulation
T1106: Native API
T1110: Brute Force
T1114: Email Collection
T1119: Automated Collection
T1127: Trusted Developer Utilities Proxy Execution
T1129: Shared Modules
T1133: External Remote Services
T1136: Create Account
T1137: Office Application Startup
T1176: Browser Extensions
T1189: Drive-by Compromise
T1190: Exploit Public-Facing Application
T1200: Hardware Additions
T1203: Exploitation for Client Execution
T1204: User Execution: Malicious Image
T1205: Traffic Signaling
T1210: Exploitation of Remote Services
T1211: Exploitation for Defense Evasion
T1212: Exploitation for Credential Access
T1213: Data from Information Repositories
T1216: Signed Script Proxy Execution
T1218: Signed Binary Proxy Execution
T1219: Remote Access Software
T1220: XSL Script Processing
T1221: Template Injection
T1505: Server Software Component
T1525: Implant Internal Image
T1530: Data from Cloud Storage Object
T1539: Steal Web Session Cookie
T1542: Pre-OS Boot
T1546: Event Triggered Execution
T1547: Boot or Logon Autostart Execution
T1548: Abuse Elevation Control Mechanism
T1550: Use Alternate Authentication Material
T1552: Unsecured Credentials
T1553: Subvert Trust Controls
T1554: Compromise Client Software Binary
T1555: Credentials from Password Stores
T1556: Modify Authentication Process
T1557: Adversary-in-the-Middle
T1558: Steal or Forge Kerberos Tickets
T1559: Inter-Process Communication
T1562: Impair Defenses
T1563: Remote Service Session Hijacking
T1564: Hide Artifacts
T1565: Data Manipulation
T1566: Phishing
T1574: Hijack Execution Flow
T1599: Network Boundary Bridging
T1601: Modify System Image
T1602: Data from Configuration Repository
T1609: Container Administration Command
T1610: Deploy Container
T1611: Escape to Host
T1612: Build Image on Host
T1613: Container and Resource Discovery

About Anjuna

Anjuna Security makes the public cloud secure for business. Software from Anjuna Security effortlessly enables enterprises to safely run even their most sensitive workloads in the public cloud. Unlike complex perimeter security solutions easily breached by insiders and malicious code, Anjuna leverages the strongest hardware-based secure computing technologies available to make the public cloud the safest computing resource available anywhere.

anjuna.io | info@anjuna.io | 650-501-0240