TECHNOLOGY BRIEF

ViON - Cyemptive Implementation

To protect the network, applications, and data, Cyemptive uses the following components:

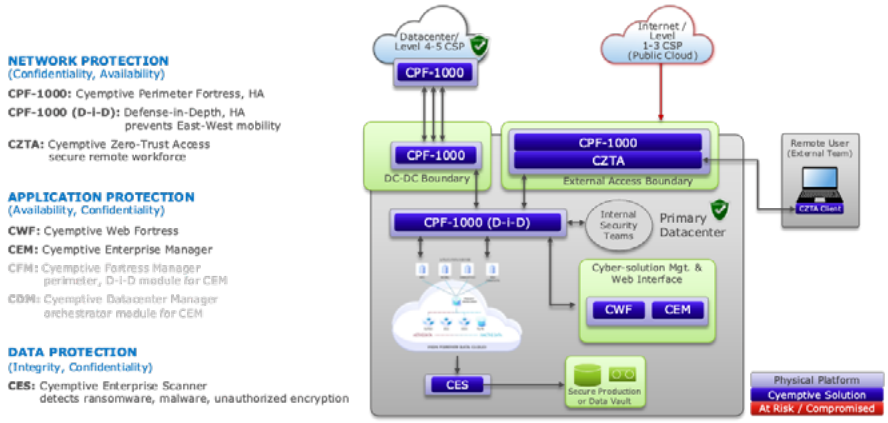
- Cyemptive Perimeter Fortress (CPF)
- Boundary and Defense-in-Depth
- Cyemptive Zero-Trust Access (CZTA)
- Cyemptive Enterprise Manager (CEM)
- Cyemptive Web Fortress (CWF)
- Cyemptive Enterprise Scanner (CES)

With the recent string of security breaches, pre-emptive cybersecurity is more important than ever. There are record numbers of network breaches and an explosion of ransomware / malware attacks. Current cyber defense technologies are simply NOT working!

ViON is partnering with Cyemptive to provide revolutionary, disruptive solutions, using patented and patent-pending technologies to achieve new capabilities around cybersecurity never seen before. All the Cyemptive technologies follow Zero Trust Blueprint's (ZTB) to enable pre-emptive protection.

Cyemptive's approach utilizes a unique combination of technologies that does not seek to identify and stay ahead of known threats, but rather use the patented technology to "pre-emptively" prevent all attacks regardless of being known or unknown. Cyemptive has built protections leveraging multiple automated defense techniques, deep zero-day intelligence, honeypots, sensors, and revolutionary Cyemptive State technologies working together. The combination of Cyemptive solution technologies makes environments nearly impenetrable.

Cyemptive's Cybersecurity Solution Components



Cyemptive Perimeter Fortress

The **Cyemptive Perimeter Fortress (CPF)** is a revolutionary perimeter defense solution which stops today's most advanced global hackers. It does this in seconds and prior to compromise. The CPF handles root level attacks and firmware attacks with ease as the underlying technology does not wait for a compromise to occur. The CPF platform uses the highest levels of encryption, multiple tunnels, and Cyemptive technology to ensure the policies and operations are always in a known, good state. By integrating Zero-Trust capabilities at ALL layers, malicious attackers must defeat MANY levels of protection. This platform is capable of preventing and / or detecting known and unknown attacks like Zero-Day (Discovered) and Zero-Day (NOT Discovered) attacks. Cyemptive re-defines perimeters into two areas: Boundary Perimeters and Internal Defense-in-Depth Perimeters.

By integrating Zero-Trust capabilities at ALL layers, malicious attackers must defeat MANY levels of protection.

Boundary - Protect the Internet/Public Cloud Connection

It is regularly agreed that the Internet/Public Cloud is not secure by default. Attacks are being concealed and passed through in network payloads and many of these attacks are undiscovered. It can be argued that most of the current perimeter solutions are NOT preventing or eliminating attacks. The CPF-1000 in a Boundary Service mode prevents North-South attack vectors and secures boundary access into a datacenter.

An add on module to the CPF, the **Cyemptive Zero-Trust Access (CZTA)**, allows for remote users to securely communicate to the corporate environment. VPNs and Certificate Authorities (CA's) HAVE been compromised, allowing bad actors easy access to corporate networks and data. Static certificates are especially "At Risk" and have been "Compromised." To combat this threat, Cyemptive created the CZTA. This is a defensive technology that adds Zero-Trust Isolated Channels to endpoints. CZTA uses the highest legal levels of encryption and dynamic non-permanent keys to ensure communications are secure.

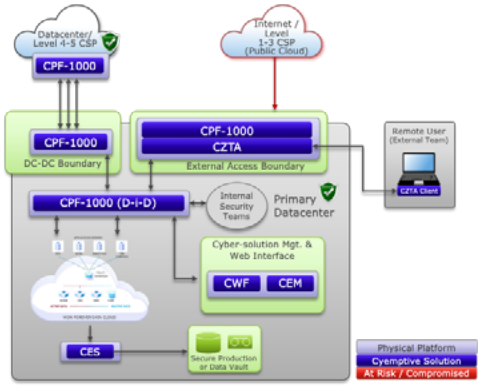
Cyemptive's Perimeter Fortress

NETWORK PROTECTION
(Confidentiality, Availability)

CPF-1000: Cyemptive Perimeter Fortress, HA

CPF-1000 (D-i-D): Defense-in-Depth, HA prevents East-West mobility

CZTA: Cyemptive Zero-Trust Access secure remote workforce



Boundary - Provide Secure Tunnel Between Datacenters Or Private Cloud Providers

Many customers today have multiple sites and require the ability to protect the traffic between them. These remote datacenters or CSPs can be vulnerable to Man-in-the-Middle attacks and session hijacking when bad actors insert themselves in between the reliable source and the destination network traffic. The CPF-1000 solution can be deployed at each of the sites to provide site-to-site control. Multiple tunnels can be configured between the sites to provide higher throughput and greater security.

The CPF-1000 solution can be deployed at each of the sites to provide site-to-site control.

Internal - Defense-In-Depth Measure Within The Datacenter

The CPF-1000 (D-i-D) is installed within the datacenter to prevent East-West mobility and insider threats.

Cyemptive Enterprise Scanner

In most environments, data is already compromised with no visible symptoms. Look at the following staggering facts:

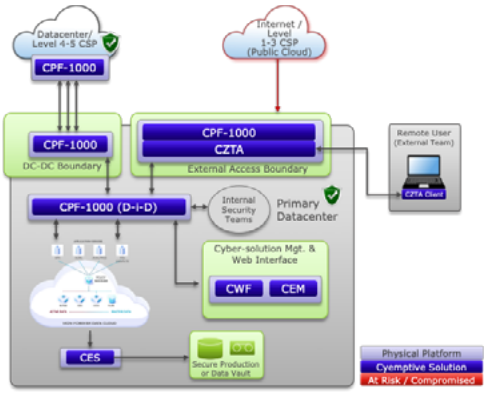
- Hackers are developing 560,000 new malware variants daily*
- Every minute four companies fall victim to ransomware attacks*
- 75% of companies infected with ransomware were running up-to date endpoint protection**

It is difficult to determine the actual effectiveness of antivirus scanners with a record number of infections reported. With the number of variants growing exponentially, the effectiveness of scanners that rely on signatures drastically drops.

Cyemptive's Enterprise Scanner

DATA PROTECTION
(Integrity, Confidentiality)

CES: Cyemptive Enterprise Scanner
detects ransomware, malware, unauthorized encryption



The CES can detect both known and unknown forms of encryption applied to files to several orders of magnitude more than other solutions on the market today.

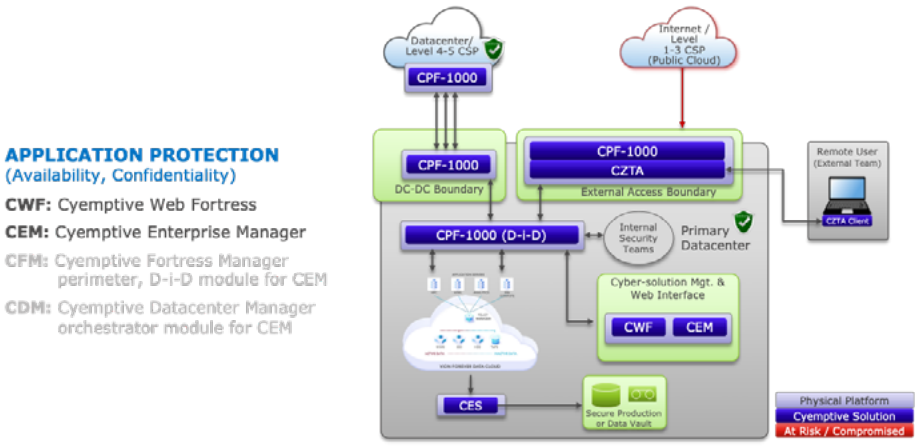
The **Cyemptive Enterprise Scanner (CES)** detects and prevents ransomware before it encrypts files within the operating system or network. In addition, CES detects and prevents many other forms of malware and unwanted encrypted files before they enter and harm the operating system or network. The CES can detect both known and unknown forms of encryption applied to files to several orders of magnitude more than other solutions on the market today. The CES also incorporates highly efficient cluster scalability for efficiently scanning massive datasets including any level of backup file systems.

- CES Comes in multiple flavors and can be sized to meet a customer's environment from 1 TB to Exabytes of data.
- CES runs in a "Shared Nothing" cluster and uses an extremely efficient Cyemptive optimizer for processing data as fast as possible (near real-time) for some customers.
- CES implements "zones" or boundaries within the platform to prevent unauthorized access to processes validating and auditing data.

How the CES works:

1. CES ingests files that have changed in a primary data store via read-only connectivity
2. CES will Scan, Log, Audit, Isolate if needed, Alert, Report on the actions
3. The scanned data is moved, if determined a "Good" file, into a Data Vault for Backup, on-site / off-site storage (Gold Copy), or provided to original or different servers as a "Verified" production copy
4. If CES Recovery nodes are used, they perform the same operations in reverse with an additional capability of auditing the files from ingest, Data Vault, and in recovery
5. OPTION: CES can provide an optional "Chain of Custody" for automated legal or forensic operations from start to recovery whether the file is one hour or 10 years old.

Cyemptive's Web Fortress



Cyemptive Web Fortress

Applications are being compromised and hacked daily in record numbers. Many technology companies constantly send patches and updates to attempt to stay in front of these attacks but are failing. The **Cyemptive Web Fortress (CWF)** takes the place of a single or clustered, physical or virtual webserver. It provides High Availability to consumers internal, external, world and protects the webserver and keeps it in a known, good / Cyemptive hardened, locked-down state.

The CWF protects webservers against real-time attacks on a pre-emptive, immediate basis, as opposed to the reactive, extended time approaches being attempted in the market today. If your application needs a boost in web security, CWF is the only protection in the market today which can truly pre-emptively protect you. This new approach can stand up to the latest slew of Zero-Day exploits, sophisticated AI and quantum computing persistent threats in real time and handle them within seconds to minutes.

CWF is the only protection in the market today that can truly pre-emptively protect you.

Cyemptive Enterprise Manager

The **Cyemptive Enterprise Manager (CEM)** is the control center of the combined Cyemptive platform that enables and manages the on-premise platform as well as the global multi-cloud control, provisioning, cross cloud deployments, compliance checking, security controls, cyber scanning and report consolidation.

There are currently two management modules associated with the CEM:

The **Cyemptive Fortress Manager (CFM)** module provides overall intelligent management control for all CPF's within your environment. The CFM automatically detects and prevents unauthorized changes applied to CPFs while alerting administrators per notification policies ensuring the systems in a known, good state. The CFM centrally manages both INBOUND and OUTBOUND configurations of the CPF for boundary and Defense-in-Depth security layers.

The **Cyemptive Datacenter Manager (CDM)** module is the execution engine providing scalable sizing for all application deployments. The CDM manages and deploys secure hypervisor templates for use with CWF (as an example). It integrates existing dev-op tools to perform repeatable, predictable, scalable application deployments, all while maintaining top level security.

ViON Cyemptive Implementation

An integrated ViON and Cyemptive solution will provide the highest levels of protection and cybersecurity posture using the trusted C-I-A Triad of Confidentiality, Integrity, and Availability in a Zero Trust Blueprint model.

It integrates existing dev-op tools to perform repeatable, predictable, scalable application deployments, all while maintaining top level security.

Confidentiality	Integrity	Availability
Cyemptive Perimeter Fortress (CPF) Cyemptive Zero Trust Access (CZTA) Cyemptive Enterprise Scanner (CES) Cyemptive Web Fortress (CWF) Cyemptive Enterprise Manager (CEM)	Cyemptive Enterprise Scanner (CES)	Cyemptive Perimeter Fortress (CPF) Cyemptive Zero Trust Access (CZTA) Cyemptive Web Fortress (CWF) Cyemptive Enterprise Manager (CEM)

ViON can work with customers to determine their security needs and integrate the entire array of Cyemptive solutions, or parts of the solutions. These solutions can replace an existing security solution, or work in conjunction with most legacy solutions.

With over 20 years of experience supporting sophisticated environments, ViON has the resources to address your most complex security challenges. We support all stages of implementation, including Proof of Concept (POC) testing, staging and on-site installation services, along with Professional, Managed and Support Services to ensure our customers get the solution that meets their exact requirements.

ViON®
Building your enterprise solutions

About ViON Corporation

ViON Corporation is a cloud service provider with over 40 years' experience designing and delivering infrastructure as-a-Service for government agencies and commercial businesses. The company provides a large portfolio of IT as-a-Service, including infrastructure, multi-cloud and artificial intelligence (AI) solutions that extend from the edge to the core to the cloud. Focused on supporting the customer's IT modernization requirements, ViON's Cloud Services is changing cloud management for the market, providing a streamlined platform to audit and control technology in an evolving multi-cloud world. **The ViON Marketplace™** allows customers to research, compare, procure, manage and report a full range of everything as-a-Service solutions from leading manufacturers via a single platform. ViON delivers an outstanding customer experience at every step with professional and managed services, backed by highly trained, cleared resources. A veteran-owned company based in Herndon, Virginia, the company has field offices throughout the U.S. (**vion.com**).

To learn more, go to vion.com/cloud or email us at **info@vion.com**