DIGITAL IMMUNITY™
STAY PRODUCTIVE, STAY SECURE

DATASHEET

Digital Immunity PROTECT™
Revolutionizing Cyber-Threat Protection

Key Benefits

- ✓ **Prevents advanced threats** including zero-day, APTs and ransomware attacks
- ✓ **Immunizes endpoints** against all file, file-less, known and unknown malware
- ✓ **DI sensor** consumes less than 1% CPU usage - No reboot/downtime needed on deployment
- ✓ **Protection in memory, at run-time** when and where endpoints are most vulnerable
- ✓ **Active protection** - requires no signature updates, no behavioral analysis cycles, no AI algorithms or machine learning
- ✓ **Supports air-gapped environments** - no external or web connection required
- ✓ **Captures deep forensics artifacts** in context at point of attack for rapid incident response.
- ✓ **Built-in multi-tenancy support** and multi-site management – all from one central console

MANUFACTURING CYBER-ATTACKS THREATEN UPTIME & REVENUE

80% of manufacturers will have adopted IIoT by 2021, adding more than 50 million connected devices to their infrastructure, dramatically increasing the attack surface. Vulnerabilities grew 120% in 2017, and 39% of all ransomware attacks targeted manufacturing companies resulting in the loss of hundreds of millions in revenue. You care about keeping your production lines running and protecting your revenues. You can't allow the increased security risk, patch overload and legacy system technology lag, to jeopardize critical production systems.

Digital Immunity™ PROTECT™, a revolutionary cyber-security solution, helps manufacturing companies like yours stay productive and secure. DI PROTECT™ utilizes a bio-inspired patented digital DNA analysis of code executing in memory, at runtime – blocking any code that has a DNA different from that of the original source. This helps prevent even attacks that disguise as legitimate code, tampering and morphing malware, thus hardening operating systems and applications.

Digital Immunity protects your Microsoft Windows devices (desktop, laptop and servers), which are the originating source of over 70% of cyber-attacks from malware attacks (file based or file less, known and unknown) including Zero Day attacks, by preventing malicious code from executing before damage is done. When the integrity of the application is violated, it will terminate the process and notify, or notify only.

Having thoroughly analyzed the challenges faced by their customers and understanding the shortcomings of existing cyber defenses, In-Q-Tell chose Digital Immunity for its unique runtime protection, prevention and detection capabilities as well as for the forensic data it captures in context.

Stay productive. Stay Secure. Choose Digital Immunity!

COMPONENTS & SPECIFICATIONS

DI PROTECT™ Map Manager

- Host Machine: Virtual Appliance
- Processors: Intel/AMD 8 core or higher
- Memory: 32 GB
- Storage: 200Mb (per protected endpoint)
- Networking: Gigabit

DI PROTECT™ Map Generator(s)

- Host Machine: Virtual Appliance
- Processors: Intel/AMD 4 core or higher
- Memory: 8 GB
- Storage: 100 GB
- Networking: Gigabit

DI PROTECT™ Sensors

- Host Machine: Standard workstation
- Processors: Intel/AMD 4 core (x86/64)
- Memory: 4 GB
- Storage: 10 Gb of available disk space
- Networking: 10/100/1000, Wireless

DI PROTECT™ Control Center

- Web Browser:
  - Chrome v68 or later (recommended)
  - Firefox 62 or later
  - Internet Explorer 11
  - Edge 43 or later

ADD-ON MODULES

DI Collector

- Centralized view of multiple production lines
- An aggregated view of OT and IT data
- Full scalability and multi-tiering capabilities
- Forwarding of alerts through a DMZ
- Dedicated dashboard for DI Collector management

DI High Availability

- Mitigates single point of failure
- Clustering and operational load balancing
- Scalable with ability to add unlimited nodes
- Wizard assisted for ease of setup
- Integrates with both local and shared network drives
- Dedicated dashboard for DI High Availability status management

DIGITAL IMMUNITY™
STAY PRODUCTIVE, STAY SECURE

Bioinformatics Methodology Conquers Current Industry Limitations

Protected by three patent family filings, Digital Immunity's bioinformatics methodology is called Digital DNA Mapping, which validates executable code at the individual instruction level. This perfectly secure technique avoids the high computational cost of repetitive run-time re-computation of cryptographic signatures or hashes. It also enables effective protection at the endpoint irrelevant of its patching status.

This methodology enables "adaptive immunity" for foreign code. Through high performance and strong forensics, Digital Immunity maintains an analog of immunological memory on each Endpoint that identifies running software as trusted or untrusted, without resource-intensive behavioural or cryptographic techniques, hash codes or signatures.

The Application Is the New Perimeter

The enterprise network has become increasingly complex and porous as the perimeter has expanded to the endpoint, with applications and end users everywhere. Mobile and cloud-based applications continue to drive demand for anytime, anywhere access. The application is the new perimeter, and ensuring computational integrity is security's next great achievement.

Unique Deterministic Detection

A Digital DNA Map of each instruction within an application is created, generated from a known, trusted source. Published to the DI Map Manager and provisioned to each protected Endpoint, Digital Immunity works in real-time, continually monitoring that the applications haven't been modified in memory. Deep granular data retention on kernel-level activity meets compliance standards and provides actionable, real-time cyber defences. A DI Sensor is used to keep endpoints protected. This is kernel driver which is installed on each Endpoint, delivering a lightweight approach that does not need complex, resource intensive, constant data collection. Our unique deterministic detection and prevention method involve NO signatures, hashes, behavioral analytics, predictive analysis, big data or machine learning.

State of the art countermeasures

For specific alert types and threats, DI PROTECT™ can also neutralize (render inert/core-out) specifically the malicious part of a process without interfering with the legitimate parts of an infected application process. This feature is known as Threat Hollowing and can be applied against these specific threats: Heap Code Execution attacks, Unauthorized Functions threats, Malicious Shellcode attacks, Reflective/PE Injection threats , Malicious Script threats, JavaScript Injection attacks.

Centralize multi-site alerts via DI Collector

The DI Collector provides a single-pane-of-glass view for data collected across multiple sites that are secured by DI PROTECT™. It allows individual sites to send alerts upstream to a central or higher-level DI Collector that would provide a broader view of a large enterprise or global business with multiple business units or departments.
The DI Collector aggregates upstream data sent from existing DI PROTECT™ deployments called 'Sender Sites'. These Sender Sites can be individual DI Map Managers (MMVAs) or part of the DI High Availability clusters located in logical segmentations of the same network, locally distributed sites or geographically remote sites (regional or globally distributed). The Sender site can also be a Collector for other sender sites locally, regionally or globally.

Clustering and operational load balancing vi DI High Availability module

The DI High Availability module provides continuous availability of DI PROTECT™ through the clustering of core DI PROTECT™ components. This module helps mitigate single point of failure by allowing distribution of storage management and other DI Map Managers (MMVAs) roles across multiple High Availability cluster nodes. DI High Availability allows seamless fully automated fail-over across multiple/stand-by cluster nodes, while offering load balancing and distribution of operational load across multiple DI Map Managers (MMVAs) for optimized performance. This offers scalability for Enterprise providing the ability to add unlimited nodes in the High Availability cluster.

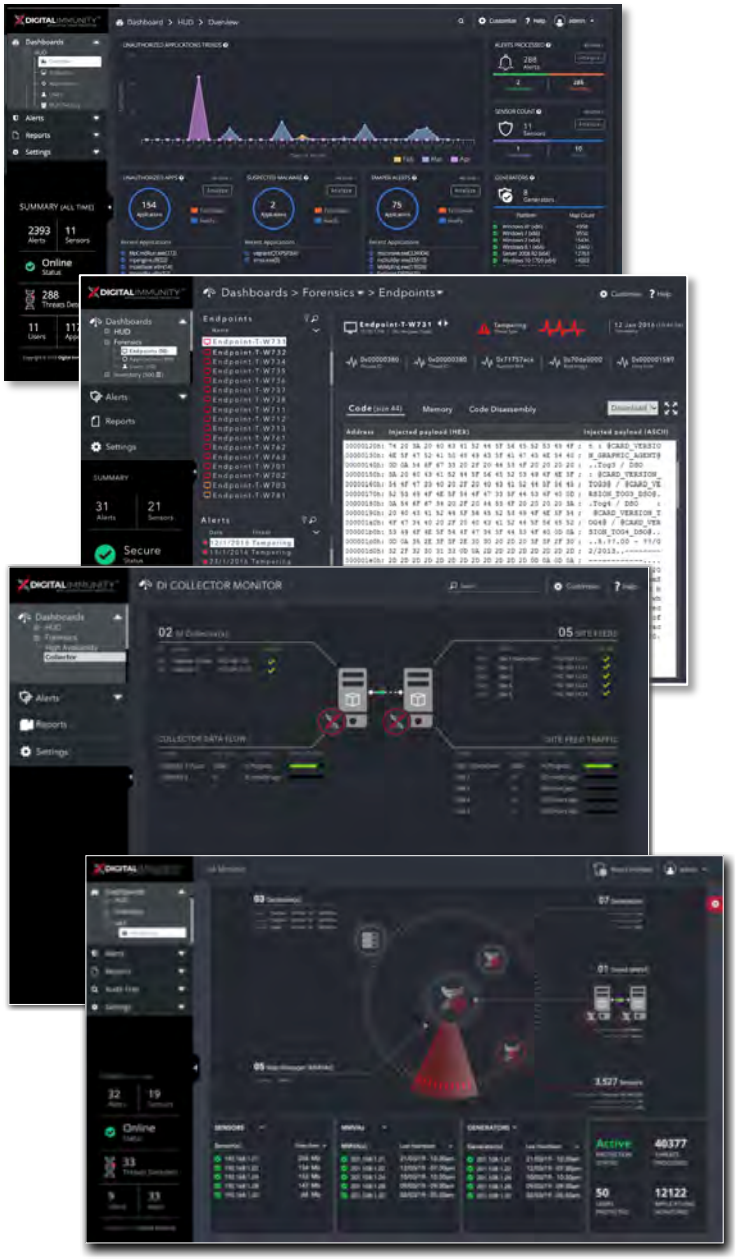
Operating Systems Supported

Server OS

- Microsoft Windows Server 2003 SP2
- Microsoft Windows Server 2008 (including R2)
- Microsoft Windows Server 2012 (including R2)
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

Workstation OS

- Microsoft Windows XP SP2, SP3
- Microsoft Windows Vista
- Microsoft Windows Windows 7
- Microsoft Windows Windows 8
- Microsoft Windows Windows 8.1
- Microsoft Windows Windows 10



About Digital Immunity

Digital Immunity INC, is an IQT Portfolio company that is revolutionizing cyber-threat protection, bridges the gap between real-time threat prevention and 24/7, mission critical environments so security no longer takes a back seat to production.

We provide advanced malware prevention in Operational Technology, as well as controlled, mission critical IT environments with no impact to production or system performance. Our patented Digital DNA Mapping technology prevents advanced threats, including APT's and zero-day attacks, from executing in memory at runtime, hardening your mission critical operating systems and applications.