DIGITALIMMUNITY™
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 Map Manager

- Host Machine: Virtual Appliance
- Processors: Intel/AMD 2 core or higher
- Memory: 8 Gigabytes
- Storage: 2 Terabytes
- Networking: Gigabit

DI Map Generator(s)

- Host Machine: Virtual Appliance
- Processors: Intel/AMD 4 core or higher
- Memory: 16 Gb
- Storage: 100 GB
- Networking: Gigabit

DI Sensors

- Host Machine: Standard workstation
- Processors: Intel/AMD 1 core (x86/64)
- Memory: 1 Gb
- Storage: 5 Gb of available disk space
- Networking: 10/100/1000, Wireless

DI Control Center

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

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. No access to source or executable code are required, and this perfectly secure technique avoids the high computational cost of repetitive run-time re-computation of cryptographic signatures or hashes.

This methodology enables "adaptive immunity" for foreign code. Through high performance and strong forensics, Digital Immunity maintains an analog of immunological memory on each Device that identifies running software as trusted or untrusted, without resource- intensive behavioral 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 device, 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 Map Manager and provisioned to each Device, 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 DNA Sensor kernel driver is installed on each Device, 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.

About Digital Immunity

Digital Immunity, LLC, 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 on mission critical devices in Operational Technology 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 with DI PROTECT™, our flagship solution. DI PROTECT™ will also capture forensic artifacts in context and present them in the DI Control Center for further analysis.