DIGITAL IMMUNITY™
STAY PRODUCTIVE, STAY SECURE

DI PROTECT™

Operational Technology Engineers Benefit by Deploying Digital Immunity

DIGITAL IMMUNITY

Stay Productive. Stay Secure.

OT Engineering and Digital Immunity

These days, many of us want to know more about a product or service before engaging a vendor. To that end, Digital Immunity is creating a collection of concise documents - an Education Series - to educate and engage potential customers. During this learning process, you may want to engage with our staff to delve deeper into the product, delivery models, licensing and more. Once you contact us, we will ensure the right team members are engaged to help you finalize your assessment and demonstrate the associated Return-On-Investment.

This document is focused on the Operational Technology (OT) and Industrial Control System (ICS) space and the benefits of implementing Digital Immunity's DI PROTECT™ technology.

AVAILABILITY – INTEGRITY – CONFIDENTIALITY (AIC)

One of the models designed to guide policies for Information Security is the Confidentiality-Integrity-Availability (CIA) Triad. Confidentiality tends to come first because breaking into computer systems to steal intellectual property (IP) has represented a common and growing concern.

For most manufacturing organizations, however, **availability** tends to be the primary concern. If a manufacturing plant is not running well, the potential to short the market and lose market share is a very real concern.

Because of the capital and expense intensive nature of manufacturing, management strives to optimize plant output by seeking automation, running multiple shifts, and continuously seeking improvements to improve yield and safety. Availability, therefore, is of utmost importance, and cybersecurity controls must both protect assets from cybersecurity consequences while simultaneously supporting the mission of plants - to make product safely, cost-effectively, and protect the environment.

OT ENGINEERS ARE ALREADY BUSY

Management and engineers understand the importance of implementing cybersecurity controls. However, the challenge is balancing this workload with all the other competing priorities.

Cybersecurity controls, many times, are adding responsibilities and complexity to an engineer's workload. This additional workload adds up and can cause frustrations for engineers, their management, and families/friends.

PATCHING

In the last couple of years, per published statistics, the number of new malware continues to increase for both Windows and ICS-specific systems. This is translating into negative impacts to manufacturing plants, and these impacts are increasingly being made public by mainstream media.

Cyber-Hygiene, specifically patching, has become more important across the enterprise and in manufacturing. However, it is one thing to push a patch to an office worker's PC and another thing to push a patch to an Industrial Control System or Quality Control System for manufacturing. These machines many times run 7x24 or can be running assays that take hours to complete. Disruption to these processes can cause lost product, lost revenue, and resource churn.

Pushing for emergency patching cycles creates many challenges for manufacturing personnel trying to meet site production objectives. Thus, reducing the need for emergency patching cycles creates return-on-investment (ROI).

By implementing DI PROTECT™ in Protect Mode, virtually all the time spent on emergency patch cycles will no longer be necessary. Patching the plant site can wait until normal maintenance windows, whether that is for the next scheduled downtime window or for the next functionality software upgrade.

Imagine getting weekends and holidays back. Imagine not having to explain to site management why another emergency patch is requiring downtime. Imagine focusing on plans to improve, to upgrade.

MANAGEABILITY

Another important consideration is the overhead associated with running various Cybersecurity management consoles. DI has been architected with manageability in mind. To highlight a couple of features:

- **Reference Platforms**
    - Ability to define a one-to-many relationship of reference platform to devices (servers, HMIs, engineering workstations)
    - Each OS requires a reference platform (e.g. Windows 7, Windows 10 build x.x.x)
    - Updates, such as patches, can automatically be generated and made available
    - Sensors on the devices pull down updates when available
- **Alerts**
    - In Protect Mode, the alerts will be brief because malware will not get a chance to fully execute
    - In Notify Mode, the forensics details will be very rich. The malware was allowed to execute and DI gathers great detail about the incident which can be used for forensics analysis. This feature can be used to set up Honey Pots inside manufacturing.
    - Basic alert information can be forwarded to your SIEM
    - Detailed information will be available within DI's management console
    - A multi-tiered architecture is possible for large organizations wanting to roll-up information for various security groups.

- **USBs**
  - Many companies struggle with controls for USBs
  - DI PROTECT™ will check the binary code on the USB before allowing this code to run.
  - Endpoints can be placed in Notify Mode to allow non-approved code to run when necessary and then place back into Protect Mode. Better yet, if the code on the USB needs to be run frequently, then run this good code through DI's generator and ensure only this good code is able to run via the USB.
  - DI's development team is working on further improvements for USB control. Stay tuned.

RETURN-ON-INVESTMENT (ROI)

As this document illustrates, the opportunity to realize a positive ROI, as a result of implementing DI PROTECT™, is very real.

Management can once again plan upgrades and patches. Engineering teams can focus more attention on new opportunities (e.g. yield improvements, upgrades, etc).

Engineers can be insulated from the emergency patching fire drills and focus time on the improvements management wants and rewards while also regaining some quality of life to be with friends and family.

DI PROTECT™ is a win-win for management and engineers.

About Digital Immunity

Digital Immunity, 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.

"Revolutionizing cyber-threat prevention in Operational Technology environments."

Founded in 2015 and headquartered in Burlington, MA, Digital Immunity provides revolutionary cyber-threat prevention solutions, DI PROTECT™, for modern cyberwarfare. 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 no disruption of good processes or production. Using Digital Immunity's Control Center you can mobilize your security team with real time actionable alerts and forensics artifacts in context.

What Makes Digital Immunity Different?

- In memory at run time prevention
- Works in air-gapped environments - completely self-contained
- Real prevention, unlike traditional AV detection - no preexisting knowledge of threats needed
- Hardening of OS and Applications
- No false positives
- No patch fatigue
- No extraction of data for analysis in the cloud
- Provide threat intelligence in context via the Control Center dashboard
- Remediation takes place on the device
- Works on "gray" systems as well due to DNA mapping process
- Doesn't need to learn or update – not dependent on AI or machine/behavioral learning

Contact Us

60 Mall Road, Suite 309,
Burlington, MA 01803

Phone: (781) 425-8655
Email: Sales@digitalimmunity.com
Web: www.digitalimmunity.com