DIGITAL IMMUNITY™
STAY PRODUCTIVE, STAY SECURE

DI PROTECT™

Operational Technology Critical Assets and Digital Immunity

DIGITAL IMMUNITY

Stay Productive. Stay Secure.

OT Critical Assets 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 identifying and better protecting the Critical Assets that are running your business.

IDENTIFY YOUR CRITICAL ASSETS

The first two controls in the SANS Top 20 Critical Security Controls is to inventory and control your company's hardware and software assets. For large companies this can be a very challenging task. Outsourced network management, outsourced server management, outsourced administrative computers, and more, can result in multiple inventory systems managed by multiple vendors. However, for cybersecurity purposes, a complete and integrated view is needed to know where assets reside, what software and patching levels are installed, and to map vulnerabilities against this inventory to prioritize updates and patches. This can be a daunting task.

To make this large task more manageable, companies prioritize systems based on the criticality of the asset to the business. These systems, if impacted by malware, could cause negative consequences such as putting precious data at risk and negatively impacting day-to-day operations.

Examples of critical assets differ by industry. For example, key systems for a Pharmaceutical company can be:

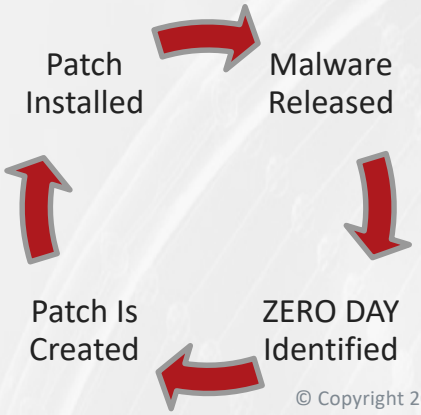
- R&D: External Collaborations; Pre-Patent IP; Toxicology
- Medical/Regulatory: Clinical Trial Management; NDA/NLE Management
- Manufacturing: ICS/OT systems; Manufacturing Execution Systems
- Quality Control: Laboratory Information Mgt Systems; various lab systems (Chromotography, TOC, IR, …)
- Legal: Patent Management System

Other manufacturing industries may have a differing list of critical systems.

WINDOWS SYSTEMS

Operational Technology (OT) critical systems running on Windows operating systems (OS) are what Digital Immunity's DI PROTECT™ is designed to protect.

Because of the large installed base of Windows systems, the bad actors creating malware/ransomware are incentivized to target Windows OS-based systems. Microsoft is working to address these vulnerabilities with regular patching and companies race to apply these patches. In addition, other software vendor products that are running on Windows have their own set of security vulnerabilities to address.



Everyday, as we read the news, yet another type of malware has been identified and is impacting companies and institutions. The merry-go-round of malware being released, identified, a patch is created, then companies work to get the patch installed, consumes valuable resources. In addition, at the end of each cycle, companies know full well that their systems are still vulnerable. It is just not clear when and what will impact their system.

LOCK-OUT MALWARE/RANSOMWARE

Anti-virus (AV) and Next Gen Anti-virus (NGAV) software provide an important layer of protection in a defense-in-depth strategy, especially for administrative laptops. In large corporations, maintaining a balance of security with flexibility to support the diverse needs of the workforce makes an AV/NGAV solution a good fit for more dynamic, general-use PCs.

However, AV/NGAV are insufficient for critical systems. This is made clear as companies continue to be hit with malware. Companies are aware of AV/NGAV's limitations and as a result, implement other countermeasures such as network segmentation, admin privilege managers, etc. This, too, is helpful, but insufficient. In addition, these countermeasures create complexities to data flows, support, and remote access.

DI PROTECT™ provides a new way to truly protect critical systems, by hardening the OS and it's related applications. The OS and applications, custom developed or purchased packages, are protected by DI's patented DNA Mapping technology. DI analyzes the binary code to create a DNA Map that is then used by a lightweight sensor on the running system which constantly monitors the integrity of the code during launch, run and exit. Only valid code is allowed to execute, preventing system tampering or the execution of foreign or malicious code.

The DI PROTECT™ cyber-threat prevention solution is an ideal architecture for Industrial Control System/Operations Technology (OT) environments. Three keys are:

1. Very Lightweight Sensors on the running system:
   - Ideal for resource challenged OT systems
2. Security Patching can be planned:
   - Only valid binary code runs preventing malware from negatively impacting a system, reducing the risk of malware impacting a protected device so significantly that emergency patching will likely not be needed.
   - Engineers quality of life improves as emergency patching cycles may no longer be necessary.
3. Manageability:
   - Setup common reference platforms to deploy to like systems (e.g. packaging line A)
   - Rollup alerts from sites to regions to corporate
   - DI becomes part of the code management process

SUMMARY

Key points to keep in mind. DI PROTECT™:

1. is not targeting general use, administrative PCs. This is better provided by AV/NGAV and other tools.

2. currently provides protection for Windows-based systems. Note: Linux is on the horizon.

3. provides that final layer of protection for critical assets. Malware is like water, it finds cracks and conduits to spread. By bubble wrapping your critical systems, your ability to operate and/or time to recover improve.

4. improves the quality of life for support staff. Applying emergency security patches will, in almost all cases, not be necessary for critical assets protected by DI PROTECT™.

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