

The background of the entire page is a dark blue color. It is decorated with a pattern of diagonal lines that run from the top-left towards the bottom-right. These lines are in two shades of blue: a lighter, medium blue and a darker, navy blue. Interspersed along these lines are small, solid blue circles of varying sizes, creating a sense of movement and a modern, technological feel.

OPSWAT.

WHITE PAPER

A Guide to Critical Infrastructure Protection

Understanding the processes and technologies essential to managing modern-day cybersecurity

SECTION 1.0

Introduction

It's been a decade since Stuxnet put critical infrastructure cybersecurity on the map. Since then, all 16 critical infrastructure sectors identified by the U.S. Department of Homeland Security have been forced to adapt to the new normal of maintaining mission-critical operations and business continuity under constant threat of cyberattack.

Despite the expanded focus on risk reduction, including advanced technology implementation, employee training and the adoption of enforceable industry and federal security regulations such as NRC, NERC-CIP and HIPAA, attacks targeting critical infrastructure sectors continue to accelerate in both complexity and frequency. In 2018, 90% of professionals in industrial control system (ICS) and operational technology (OT) environments reported that their organizations had been negatively impacted by at least one cyberattack in the past two years, according to the Ponemon Institute.

The control systems that act as the “brain” within mission critical environments are both inherently and increasingly vulnerable to actions of nation state threat actors, hacktivists and insider threats. Unlike Fortune 500 companies, attacks on critical infrastructure are sometimes, but not always motivated by financial gain. Reputational and operational disruption, as well as fear, nation-state espionage, antipathy and ideology are often the drivers.

Within critical infrastructure sectors, cyber risk is most commonly amplified by:

- Flawed IT/OT integrations
- Complexities of legacy SCADA systems
- Lack of asset visibility
- Insufficient number of skilled workers
- Ineffective people, process and technology policies
- Inadequate or unenforced remote worker and bring-your-own-device (BYOD) policies




In far too many situations, more than one of these vulnerabilities is present, threatening the systems that inherently run our day-to-day lives.

SECTION 2.0

Critical Infrastructure Protection – Trust No File. Trust No Device.TM

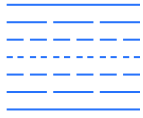
With the proliferation of zero-day attacks and the rapid expansion of the attack surface, to say CIP cybersecurity professionals are extraordinarily busy is an understatement. To help prioritize workload and mitigate backlogs, both current and prospective workers must be efficient in the responsibilities and technical proficiencies most applicable to critical infrastructure environments.

Such responsibilities include, but are not limited to:

 <p>Creating and maintaining secure data exchange processes between segregated networks</p>	 <p>Ensuring proper device posture checks to determine which devices can access which organization assets and segregated networks</p>	 <p>Disarming content that has potential for carrying malware from application files or emails</p>
---	---	--

A summary of the 11 technologies required to protect your critical infrastructure is provided on the following pages.

Critical Infrastructure Protection Technology - Trust No File.™



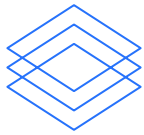
Deep CDR

Content disarm and reconstruction (CDR) breaks a file into its smallest components and removes any and every potential threat. The technology scrubs away hidden files or messages maliciously embedded within any file type, leaving the final disarmed file to look and behave exactly as the file should.



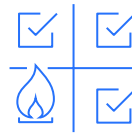
Proactive DLP

Data Loss Prevention (DLP) technology is used to detect and block financial or personally identifiable information (PII). Rather than blocking files and leaving teams high-and-dry, Proactive DLP technology suppresses sensitive information with automatic document redaction, metadata removal, or watermark addition.



Multiscanning

Multiscanning technology provides advanced threat detection and prevention. Multi-scanning exponentially increases malware detection rates, decreases outbreak detection times, and provides resiliency to anti-malware vendor issues by deploying up to 30 anti-malware engines.



File-based Vulnerability

This technology detects application and file-based vulnerabilities before they are installed. It allows organizations to correlate vulnerabilities to software components, product installers, firmware packages, and many other types of binary files which are commonly collected from a vast community of users.



Threat Intelligence

Effectively and intelligently analyzing patterns of malicious content is paramount to preventing outbreaks or stopping them in critical infrastructure environments. Threat intelligence technology analyzes data from thousands of devices, analyzing data points for binary reputation, vulnerable applications, malware analysis reports, Portable Executable or PE info, static and dynamic analysis, IP/URL reputation and, most importantly, the correlations between them.



Sandbox

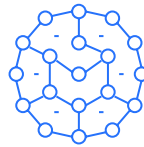
Due to the criticality of maintaining operational efficiency in critical infrastructure environments, sandboxes are often used to run third-party software and untested code as a means to reduce risk. This allows CIP cyber pros to test content without giving it access to mission critical networks and servers.

Critical Infrastructure Protection Technology - Trust No Device.™



Endpoint Compliance

Enables organizations to detect, assess and remediate device applications that do not comply with a set of security and operational policies created and enforced. It helps to minimize the spread of a malware infection and decrease the probability of data loss in the organization.



Endpoint Vulnerability Assessment

Strengthens the security of endpoints by confirming all applications are running on their most updated versions. Once vulnerabilities are identified, automatic patching can remediate them as soon as possible. This can also be done manually by retrieving the available remediations and choosing the update which best suits the organizations' needs.



Endpoint Malware Detection

Examines the running processes and their loaded libraries in order to provide quick assessment of the endpoint and to determine if any suspicious processes are currently running. This is especially important for remote facilities with many third-party visitors.



Endpoint Application Removal

Allows for the removal of security applications like AV and firewalls as well as the removal of potentially unwanted applications (PUA). It allows systems admins to prevent users from accessing some popular and legitimate applications that are not compliant with the work environment



Data Protection

Incorporating removable media protection, anti-keylogger and anti-screen capture technologies, data protection technology helps organizations prevent data loss and file-based attacks on endpoints. It does so by blocking users' access to removable media, such as USBs or smart phones, or allowing access to only whitelisted processes.



BEC Attack Detection and Prevention

Increase threat detection rates up to 99%, and prevent BEC attacks by deploying an advanced email gateway security layer with zero-day prevention technology. Deploy spam filtering and anti-phishing to protect against malware outbreaks.

SECTION 3.0

Effective Technology – and a Well-Trained Staff.

But perhaps no critical infrastructure protection (CIP) vulnerability is greater than the cybersecurity skills gap – an unprecedented predicament at a time when there is projected to be up to 3.5 million open cybersecurity jobs worldwide by 2021, according to Cybersecurity Ventures.

Why is lack of people such a vulnerability? Within all 16 critical infrastructure sectors, the confidentiality, integrity and availability of networks, systems and equipment is of the utmost importance. Unexpected downtime is not only unacceptable, but it can be dangerous, destructive and costly. The same can be said for unauthorized access, as it can be very difficult to find an adversary's footprint and root them out once they have bypassed security controls and entered into a system or network. ICS environments can also serve as a gateway into enterprise and government IT networks, which frequently maintain incredibly sensitive IP, company and customer data, as well as classified national security information.

Simply put, it is because of such high stakes that critical infrastructure organizations need an abundance of qualified, highly-skilled cybersecurity pros 24/7/365 to help identify, mitigate and remediate threats of all types.

Within critical infrastructure specifically, there is no universally accepted number of current or projected job openings; however, an aging OT workforce of non-digital natives combined with the increase in threat frequency and sophistication suggests that there's no shortage of opportunities. In fact, a very basic search of Indeed and LinkedIn provides thousands of open positions.

SECTION 4.0

The CIP Cybersecurity Status Quo Can No Longer Suffice

To date, several non-profit and company-driven certification and professional training courses have been introduced to help educate aspiring CIP cybersecurity professionals and retrain the existing workforce with the skills necessary to protect industrial environments from cyber threats. Unfortunately, such educational opportunities aren't producing enough job-ready workers or properly empowering those already in the workforce with empirical knowledge.

One reason is that many existing programs are sector specific. For example, the ISO 28000 certification is specific to the supply chain, meaning that such distinction would be of little to no importance to a cybersecurity role in the energy sector. Certifications that aren't industry specific, like the Global Industrial Cyber Security Professional (GICSP), tend to focus too much on concepts and theories and not enough on practical workforce training and development.

With demand for skilled critical infrastructure cyber pros at an all time high and growing, the cybersecurity industry must evolve how it trains the future and existing workforce by focusing more on teaching the practical applications of technologies, processes and procedures and less on abstract theory and concepts.

To prepare workers for a career in CIP cybersecurity and to help continuously educate existing workers, training programs must evolve to focus on the practical processes and technologies, as well as interoperability with existing IT security infrastructures, particularly access control.

The OPSWAT Academy provides a modern-day education and training program to help address the CIP cybersecurity skills shortage through courses that promote the best practices and practical approaches successfully implemented in the most secure critical infrastructure environments.

The Academy provides a comprehensive curriculum that is essential to a modern-day CIP cybersecurity training program.

SECTION 5.0

OPSWAT™ CIP Cybersecurity Solutions

At OPSWAT™, our philosophy is Trust No File. Trust No Device.

OPSWAT offers a proven and comprehensive suite of products and services to manage a broad range of CIP use cases – including Cross-Domain, File Upload, Secure Access, and Secure Storage. All OPSWAT Products are powered by the advanced technologies covered in this guide. In addition to our industry-leading products, we also offer CIP training through the OPSWAT Academy and cybersecurity readiness assessments delivered by our global team of experts.

To learn more about the OPSWAT Academy, visit opswat.com/academy and register for your first session.

Ready to take the next step in enhancing your critical infrastructure? Contact us at opswat.com/contact to learn more about our solutions and how we can help take your cybersecurity protection to the next level.



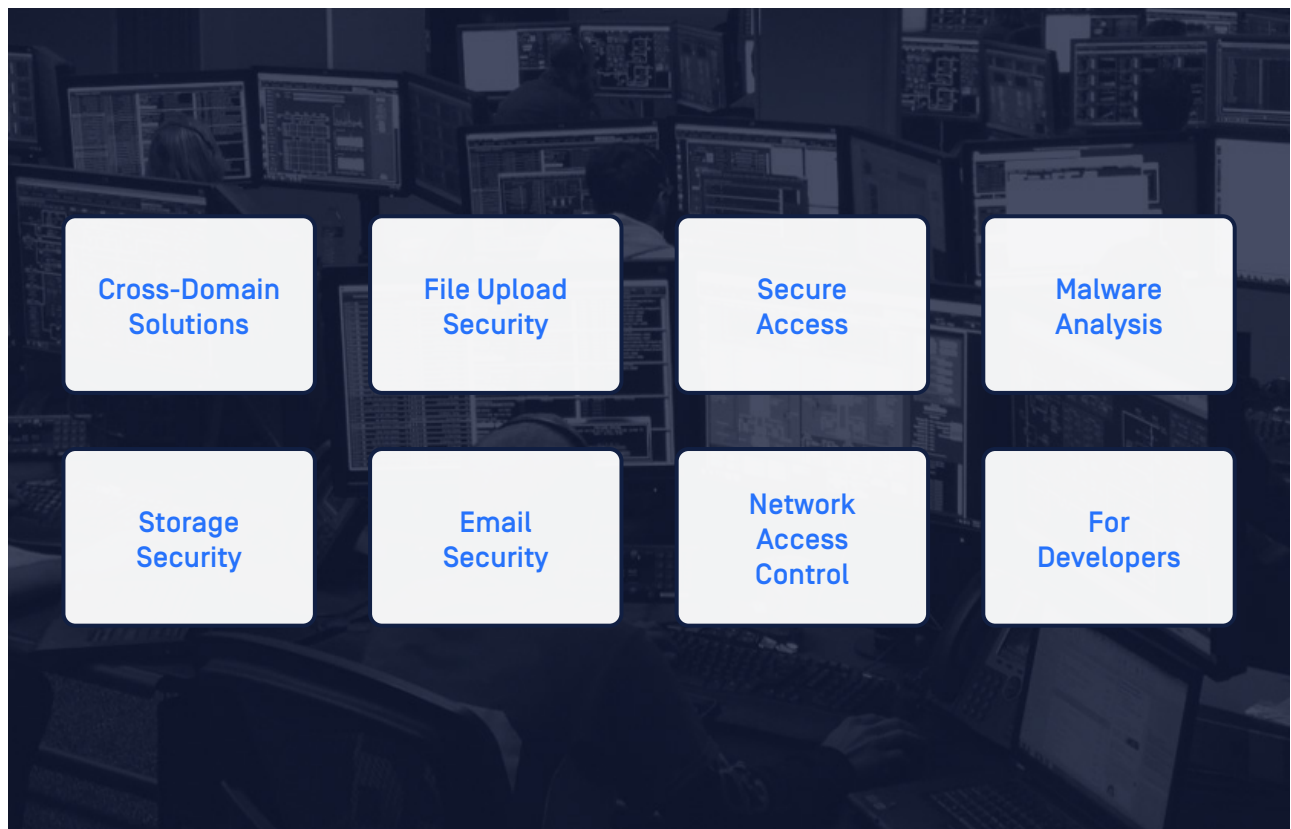
OPSWAT.
Academy

SECTION 6.0

About OPSWAT™

OPSWAT is a global leader in critical infrastructure cybersecurity that helps protect the world's mission-critical organizations from malware and zero-day attacks. To minimize the risk of compromise, OPSWAT Critical Infrastructure Protection (CIP) solutions enable both public and private organizations to implement processes that ensure the secure transfer of files and devices to and from critical networks.

More than 1,500 organizations worldwide spanning Financial Services, Defense, Manufacturing, Energy, Aerospace, and Transportation Systems trust OPSWAT to secure their files and devices; ensure compliance with industry and government-driven policies and regulations; and to protect their reputations, finances, employees and relationships from cyber-driven disruption. OPSWAT. Trust no file. Trust no device.™



Visit us on [LinkedIn](#), [Twitter](#), [Facebook](#), and [YouTube](#).



OPSWAT.

Trust no file. Trust no device.

©2020 OPSWAT, Inc. All rights reserved. OPSWAT, MetaScan, MetaDefender, MetaDefender Vault, MetaAccess, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file. Trust no device, are trademarks of OPSWAT, Inc. All other brand names may be trademarks of their respective owners.