VIDERITY
STRATEGIC, CREATIVE, TECHNICAL

Industrial Cyber Security

CYBERVANTAGE MANAGED SECURITY SERVICES

24/7 Expertise to Reduce Operational Downtime and Lower Cyber Risk

“Viderity provided the cyber security knowledge base required to protect our refinery’s control system. We have 24/7 coverage regardless of what is happening in the plant.”

Lanny Gibson, Process Control Supervisor Total Port Arthur Refinery

“With Viderity Managed Security Services our security updates are today better managed and kept up to date. We are working to attain the next level of cyber assurance and we are looking to Viderity’s support to drive towards the objective.”

Lương Thái Hà, Deputy General Manager, Binh Son Refining and Petrochemical Co. Ltd.

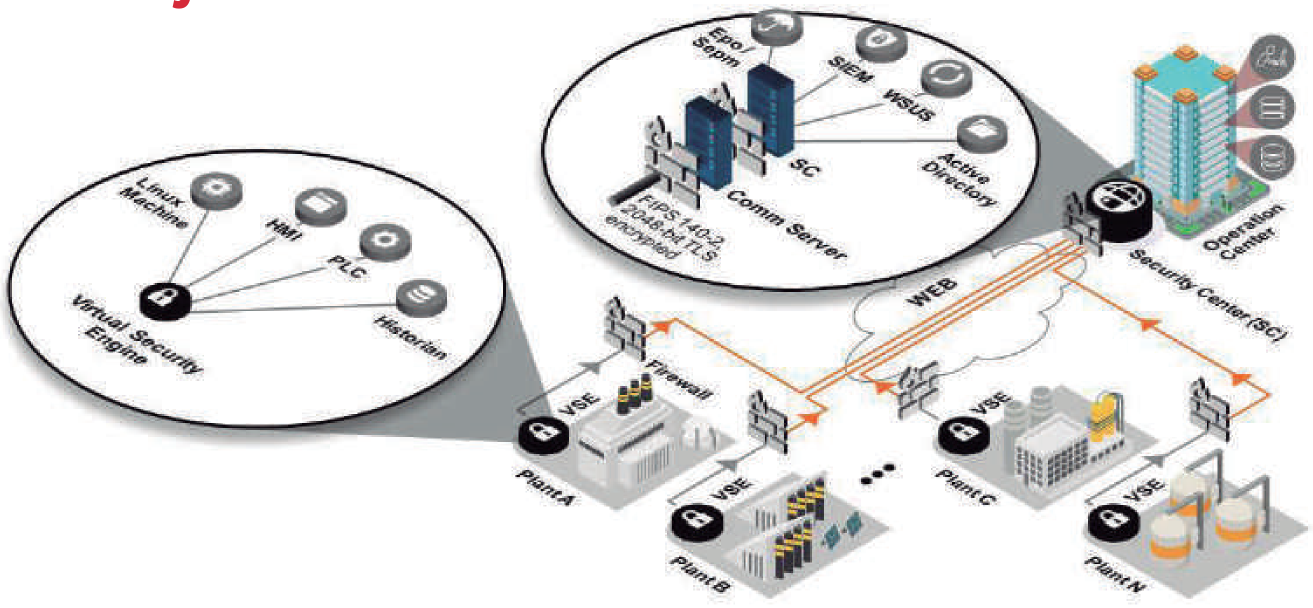
Save Time and Effort While Improving Operational Integrity

Around the world, industrial firms and critical infrastructure operators partner with Viderity to address the unique requirements of cyber security in process control environments. Viderity's broad expertise encompasses automation assets and their integrated communication networks – a distinct advantage in control system security.

In today's world, cyber security is necessary to ensure critical automation systems remain safe and fully operational. However, implementing cyber security controls is a technical and labor intensive task. Viderity's CyberVantage Managed Security Services are designed to take off the task list of process control engineers and put it into the hands of industrial cyber security experts, at a fraction of the financial investment.

Having a team of experts dedicated to these activities will not only save time and resources, it also ensures security controls are implemented in an efficient and standardized fashion. The quickest way to get your systems secure and to prevent unnecessary outages due to cyber events is to contact Viderity.

Introducing CyberVantage Managed Security Services



ICS Shield – the Core Enabler for CyberVantage Managed Security Services

Over the past 10 years Viderity has grown its Managed Industrial Cyber Security Services to a customer base for more than 40 customers across multiple industries. Viderity's new CyberVantage Managed Services today encompass all the traditional Managed Industrial Cyber Security Services, such as Secure Remote Access & Support, Automated Patch & Anti-Virus Delivery, and Continuous Security & Performance Monitoring, and Interactive Activity & Trend Reporting. However, to address customers' new and more advanced cyber requirements, CyberVantage Managed Services also provides new cutting-edge services such as Security Device Management Service, and now these services over multiple vendors' control system.

With the advent of Industry 4.0, industrial operators are increasingly adopting digital transformation strategies towards smart manufacturing and Connected Plants. Connected Operations today entails integrated operations with real-time connectivity to corporate head-offices for complete end-to-end supply-chain management. This revolutionizes the use of information in everything from manufacturing plants to pipelines and transmission systems to provide the business with the big-data and analytics never been available before. As companies continue to embrace this digital transformation, they recognize an increasing need for industrial cyber security capabilities embedded as part of the technology platform.

Recognizing this new requirements, Viderity today offers both new customers and existing subscribers to our Managed Industrial Cyber Security Services the option of establishing their own Security Centers through the use of ICS Shield, the same technology platform employed in Viderity's Managed Security Centers.

Viderity's ICS Shield provides a top-down operational technology (OT) security management solution for securing connected industrial control system environments with multiple sites and multiple automation vendors. It also enables secure management of remote field assets through a single security operations center. Viderity has integrated and enhanced this product after its acquisition of Nextnine in 2017 and it has become the ICS Cyber Security platform of choice with more than 6,000 installs globally.

Distributed architecture and secure tunnel from plants to center

- Install SC at the data center | Install VSEs at each plant
- Establish a secure tunnel, outbound, using port 443, TLS encrypted | One FW rule to manage all remote connections

Encompassing Managed Industrial Cyber Security Services and Beyond

For those companies that may not have the people and expertise to seffectively implement the required ICS/DCS security controls, CyberVantage Managed Security Services offers a set of managed services to ensure you get the most out of your software investment. The following outlines the full set suite of services in CyberVantage Managed Security Services offerings:

Secure Remote Access and Support

This service is provided to customers that desire a single secure solution for all remote connectivity. Viderity's secure access solution has the following enhanced security features:

Highly Secure

- Individual accounts must be pre-approved for site access and authorized for specified devices
- Two-factor authentication required
- Request for access must be submitted and approved for each session
- Screen sharing allows monitoring of all activity
- Access can be disabled at any time
- Alerts sent for all sessions starts and stops

Exceptional Audit Capabilities

- Comprehensive, detailed reporting of all activity
- Audits logs stored in two isolated locations
- Video recording and playback of user activity

Automated Patch and Anti-Virus Delivery

Viderity's software updates undergo extensive application testing on systems emulating a customer's production environment. Testing and qualification of newly released patches and anti-virus files adds to system stability by identifying and restricting potential ICS conflicts before implementation on site. This helps assure customers that installing Viderity-approved releases will add to the reliability and security of their system.

Viderity's secure connection approach is used to provide automatic, encrypted delivery of all patches and anti-virus files. This method is designed to reduce the potential for tampering, contamination, or modification of files from email transmissions or compromised portable media.

Virus Protection

McAfee and Symantec anti-virus programs are a critical piece of control systems' defenses. These applications function to identify and block harmful code from running on operating systems, and work in conjunction with signature files identifying specific viruses, worms, rootkits, and trojans.

It is imperative that anti-virus programs remain up-to-date; each and every workstation and server should employ the latest release of anti-virus signature files to help prevent unintentional failures or deliberate application malfunction of the PCN. A single unprotected piece of hardware has the potential to spread malware and jeopardize other networked devices, with some malware enabling backdoors for unauthorized access to the system.

Operating System Patch Management

Operating System (OS) patches are necessary to update a software program to fix problems, or to address security vulnerabilities discovered. These vulnerabilities are akin to an open door that allows malware or an attacker to enter. Patch installation closes this door and complements anti-malware program defenses.

Suppliers of operating systems such as Microsoft release patches regularly. Too often, however, patch installation takes a lower priority at industrial sites due to time and personnel constraints. Viderity's automated patching solutions eliminates the need to visit each device while leaving you in control of exactly when patch installation will occur. This quick and standardized method of patch delivery will help to ensure secure and continuous operations.

Control System Patch Management

DCS updates are custom-built and based on each site's configuration. Our industrial controls experts determine the specific software needed for each customer location, and only that selected software is sent. This custom software load has no extraneous elements or unnecessary code. The result is a reduced cyber attack profile, and improved system efficiency, reliability, and security. These software updates along with others can be delivered on the schedule determined by software development.

Continuous Security and Performance Monitoring

Comprehensive system health & cybersecurity monitoring

Monitoring the controls network, including all attached devices, is crucial not only for process orchestration, but also for the security of the entire site. The difference between a minor security incident and a major one is early detection. Compromised security opens a plant to modification of processes and production mixes, potentially affecting the quality of the produced product. These modifications, ultimately stemming from poor ICS security, can result in reduced plant output, unsaleable products, or even far worse consequences.

24x7 alerting against predefined thresholds

Viderity provides continuous monitoring of the performance and health conditions of the PCN including controllers, servers, workstations, applications, and even safety systems. If an event is detected, or if thresholds are exceeded, an alert is automatically generated. The alert thresholds are different for each system and device to provide accurate and useable event information. Should an alert condition be detected, an email or SMS text alert message will automatically be sent to the site contact 24/7 as part of the service.

Interactive Activity & Trend Reporting

Viderity's advanced intelligence technolo gy transforms masses of system statistics into actionable trends. This management reporting solution provides both critical site information and predictive hardware analysis, as well as details on current cyber security vulnerabilities and attacks.

Viderity's reporting capabilities help you stay ahead of potential attacks and take quick protective action when needed. Leveraging statistics presented by Viderity's monitoring capabilities, the reports include summaries and charted trends of network and system events.

Viderity has developed a complete portfolio of Industrial Cyber Security products and services specific to the needs of your control network. These solutions form a cyber defense foundation and operate to safeguard both the business and human interests of the process control environment.

Reduce overall cyber security risk, improve system performance, reduce operational cost and expertly manage the essential elements of your process control infrastructure with CyberVantage Managed Security Services.

The reports also identify degrading conditions, and predict hardware vulnerabilities.

The report in HTML5 format allows customers' engineers to quickly find the status of the system down to the most granular details, to compare, interpret, analyze and built upon the collected performance and security metrics.

Fully stand-alone and compatible with all current version web-browsers, it requires no connections to Internet or to Viderity Security Service Centers to work. It is available on daily, weekly, or monthly basis, or online on-demand accessible at Viderity's secure portal through two factor authentication logins.

The information also functions as a key source of compliance-related data, with quick, timely assessments to improve site and network security, performance, and management. Reporting information provides highlighted parameters, trends, and number of events per device for fast scanning and identification of equipment issues and possible threats. Reported information includes the following alerts and availability conditions for controllers, HMIs, safety devices, firewalls, switches, workstations, servers, and virtual hosts:

- Network Activity Logs
- ACL Rules, Utilization Spikes, Passwords/ Strings
- System Audit Logs
- Unauthorized Access, Disabling Controls, Configuration Changes
- System Availability/Performance
- Application Health, CPU Utilization, Hardware Errors
- Administrative Changes
- Security Policy Modifications, Group Additions, Enabling USB Devices
- Software Update Compliance
- Aging for Virus Signatures, Security Patches, Software Updates
- Virus Infections

Viderity's Activity and Trend Reporting highlights system and network actionable information from masses of equipment and network statistics to help plants optimize PCN management and security.

Security Device Management

It is important to remember that security utilities only work when properly configured, consistently maintained, and continuously monitored. Viderity works with customers to provide the approved configurations, custom definitions, and ongoing monitoring required for the industrial manufacturing environment—adding real security to plant systems and operations.

Protecting the productivity, reliability, and safety of the plant is paramount. Firewalls are a front line of defense to keep unwanted traffic and potential attackers out of the ICS network. With improved processing speeds and reduced latency, today's high-performance firewalls can now also be deployed between process control levels or zones as additional defensive elements around the process equipment core.

An Intrusion Prevention System (IPS) complements firewalls by examining traffic that has made it onto the internal network. It analyzes both the data packets and the network traffic flow and compares these to the patterns, or signatures, commonly seen with cyber-attacks. Utilizing sophisticated behavior analysis, an IPS monitors and protects the internal network from threats or attacks that may have been well hidden in other legitimate applications. Ideally, firewalls and IPSs should be used together to block and remove security threats from process control networks.

Our offering of CyberVantage Managed Security Services complement the Industrial Cyber Security Risk Manager solution. As Risk Manager identifies risks and notifies you of vulnerabilities, and help you implement countermeasures. In addition, Risk Manager can optionally be co-managed as a service to improve your situational awareness.

Threat Detection & Vulnerability Identification

Outsourced Security Monitoring & Response Support

- Installation & Maintenance of log collectors; support for deployment and configuration
- Streaming data into a hosted SIEM
- Centralized logging for Correlation and Analysis
- Monitoring/Alerting/Reporting
- Threat hunting & Incident Response support
- Data collection for incident investigations

ICS Shield Services

ICS Shield software installation and support

- Initial install – of all ICS Shield software components to ensure operation
- Asset support – making sure all assets/nodes are configured in system properly
- On-going maintenance and software support (e.g. VSE patch updates)
- Monitoring of software (e.g. VSEs and service center software to ensure it is all working correctly)

ICS Shield Hosting & Operations

- Option to host Customer's ICS Shield in one of Viderity's Managed Security Centers.
- Continuous Administration – Viderity 's extensive experience can be used to operate and maintain all aspects of the system
- User support – ensuring proper user access and connection restrictions to various sites/assets
- Anti-virus and patching configuration support (ePO, SEPM, WSUS) for PCN systems
- Secure file transfer support in moving files in and out of ICS environment
- Active reporting/alerting- monitor alerts 24/7 and notify of potential threats to their environment

Customers Case Experiences

With over 400 customers' sites managed around the world, Viderity has extensive experience providing industrial cyber security managed services. The following are just some of the real-world case studies where we have helped customers improve their cyber security posture (names withheld for cyber security reasons)

Viderity Performance Materials and Technology

- Cyber Security Vulnerability Assessments helped locate gaps, and associated risks; and Profiler to help establish an overview of the cyber posture
- Automated patch and anti-virus definition delivery employed to significantly increase server and workstation security

North American Refinery

- Viderity reduced the risk of security breaches and manage the security posture of process control infrastructure
- 24/7 monitoring and alerting of the site's PCN, including controllers, servers and workstations
- Intelligence reporting services to transform system statistics to actionable trends

Asian Petrochemical Plant

- Active monitoring and secure remote access provided to multiple remote sites for over 8 years
- Due to success of this work, the company has expanded investments on Viderity cyber security
- PCN security updates are better managed and constantly kept up to date
- Downtime has been reduced and the business is more responsive to issues before further deterioration
- Secure remote support with full recordings and audit trail of all activities

Benefits of Viderity's Cyber Security Solutions

Viderity's Industrial Cyber Security combines leading engineering analysis with the industrial expertise essential in process control environments.

Continuous Maintenance

- Receive new features and capabilities as soon as they become available
- Have problems corrected as they occur

Experience

- Eliminate the need to train personnel or learn through trial and error
- Viderity has extensive experience and has defined best practices

Staffing

- No need to hire dedicated personnel to perform infrastructure services tasks
- Viderity has a growing team of experts and analysts

Constant Support

- 24x7 answers to questions or issues

Extended Team

- Leverage a global team of ICS security experts who have multi-vendor experience

"With the increase in threats and capabilities of cyber attackers targeting the industrial sector, we needed to add tools to address these specific concerns and complement our established cyber security framework. Viderity's Risk Manager and ICS Shield® offerings helped us provide more oversight and improve our detection and protection functions."

Scott Francy, Viderity PMT Lead Automation Engineer

Additional Viderity Products and Services

Viderity provides a full range of products and services to help customers manage and secure their industrial control systems and critical infrastructure and bolster the Industrial Internet of Things. Leveraging our industry leading process control and cyber security experience, our expertise, and technology, Viderity delivers proven cyber security solutions designed for the specific needs of process control environments. In addition to CyberVantage Managed Security Services our portfolio includes the Industrial Cyber Security Risk Manager solution, which proactively monitors, measures and manages industrial Cyber Security risk and the award-winning Secure Media Exchange (SMX) which actively protects against current and emerging USB-borne threats. We also offer consulting and remediation services including security assessments and audits, architecture and design, network security, endpoint protection, situational awareness, and response and recovery. These solutions are enabled by innovative technology and delivered by a global team of cyber security experts.

For More Information

To learn more about Viderity's Managed Industrial Cyber Security Services, visit www.becybersecure.com or contact your Viderity account manager.

Viderity Process Solutions Viderity
1250 West Sam Houston Parkway South
Houston, TX 77042
Viderity House, Arlington Business Park
Bracknell, Berkshire, England RG12 1EB
Shanghai City Centre, 100 Junyi Road
Shanghai, China 20051
www.viderityprocess.com

VIDERITY
STRATEGIC, CREATIVE, TECHNICAL