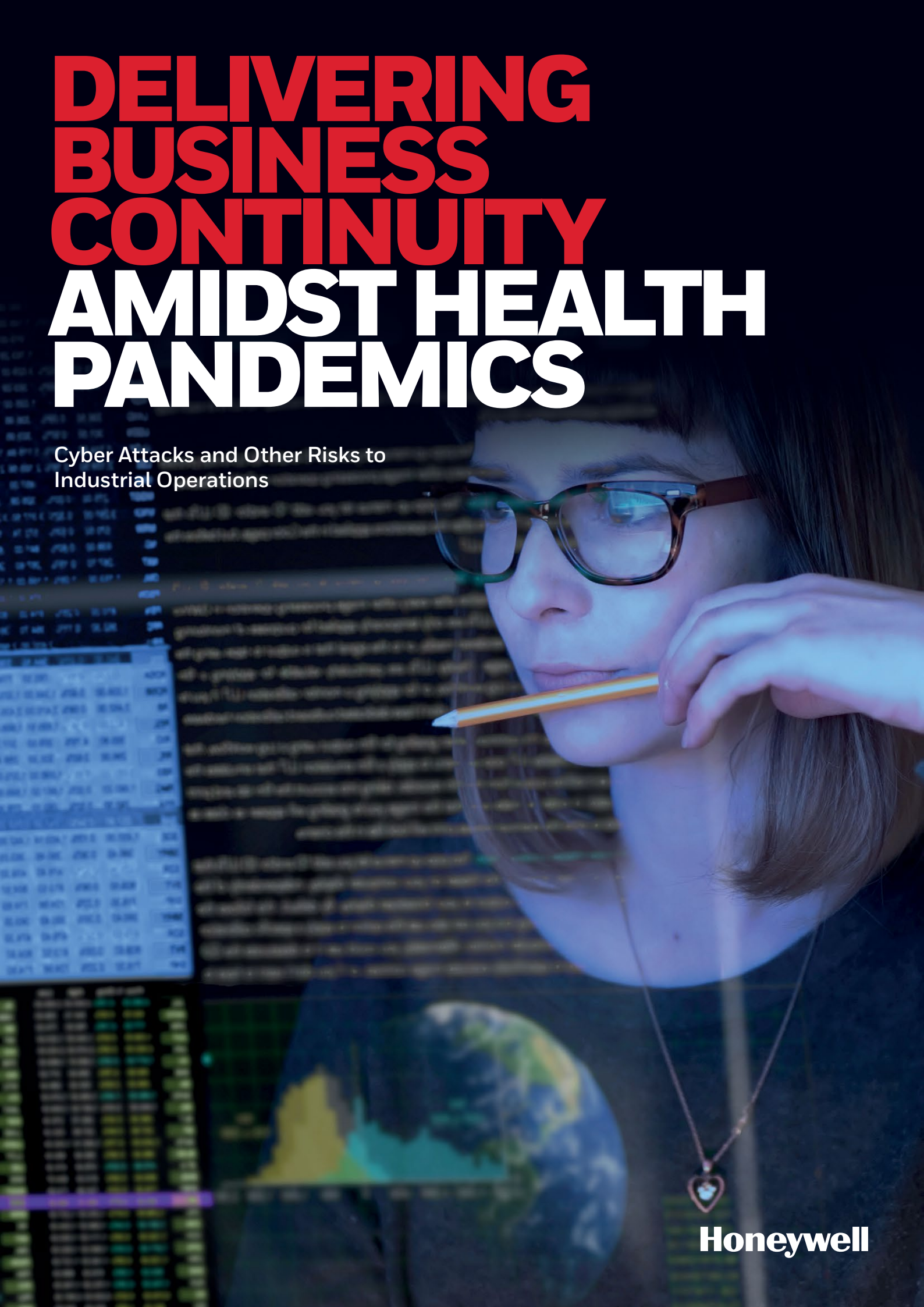
DELIVERING BUSINESS CONTINUITY AMIDST HEALTH PANDEMICS

Cyber Attacks and Other Risks to Industrial Operations



Honeywell

TABLE OF CONTENTS

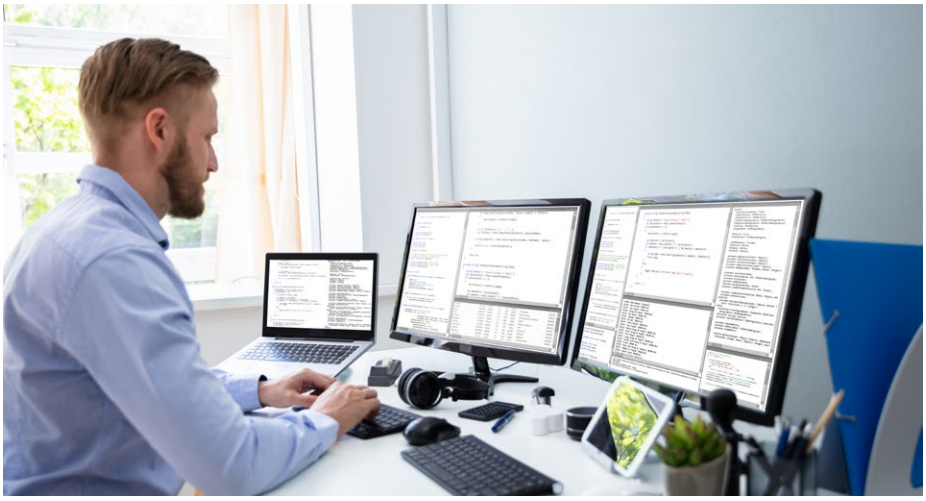
MANAGEMENT SUMMARY

Industrial-Grade Remote Access in a World of Physical Risks

Global risk factors today for an industrial enterprise, whether health pandemics or cyberattacks, are placing an urgent emphasis on the need for flexible control and management over operational assets. Business continuity remains a strategic priority, as new worldwide complexities and uncertainties arise. A March 2020 Forrester report notes that provisioning employees with remote access technologies is a key continuity strategy at 88 percent of organizations surveyed (1), while Gartner recommends to "accelerate the development of a technology infrastructure that can support alternative types of working."(2) In the same timeframe, the US government's Cybersecurity and Infrastructure Security Agency (CISA) issued an advisory to critical infrastructure companies to prepare for remote work scenarios in light of the Covid-19 health pandemic (3).

While some office personnel have the ability to work remotely, manufacturing and industrial operations must keep the lights on. This includes a reliance on highly specialized technicians to monitor, diagnose and regularly operate capital-intensive assets, whether turbines, pulp machinery or gas and water pumps. Such privileged access is critical to keep operations running and requires a specialized approach.

Fortunately, industrial software innovations have increased in pace and scale. More options exist today for how and where an industrial enterprise runs and services its operations remotely, together with updated security controls. By designing and implementing robust digital operations, with the proper safeguards in place, industrial enterprises can manage through unplanned downtime and even increase efficiencies and performance. Specific to the needs of industrial operators, advanced secure remote access technologies go beyond the scope of traditional IT VPN requirements to enable a safer and more controlled approach to running and maintaining processes from a distance. Although a part of disaster planning and recovery in increasing resilience, industrial-grade secure remote access also represents a strategic investment that can help grow a company's operational excellence and capabilities.



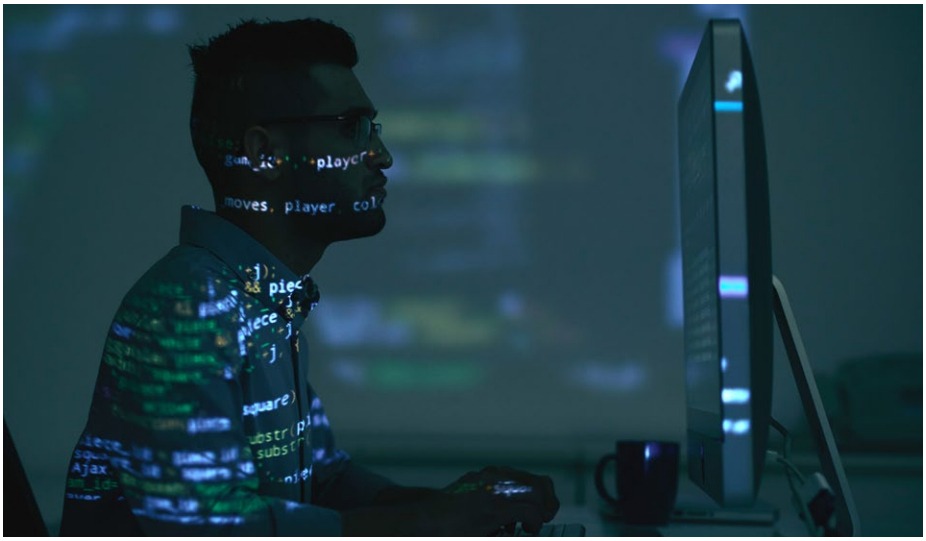
IT AND OT REMOTE ACCESS REQUIREMENTS ARE NOT THE SAME

A critical starting point in approaching remote operations is to recognize the major considerations unique to industrial environments that rely on operational technologies (OT). A common mistake at the business level is to assume that assets are not differentiated – yet an IT business PC is a far cry from an engineering workstation PC, let alone a station that is tied to multiple critical operational processes. These stations may control processes that impact furnace temperatures, flow settings, and other physical attributes. Any disregard for verified OS patches, critical infrastructure hardening per Center for Internet Security standards, or other customized configurations and systems can result in the loss of human life, irreversible environmental impact and other serious physical dangers. This is easier said than done, especially in times of crisis when top-down decisions can be made under pressure and amidst false or changing information. **Before deploying any remote access solutions, it is essential to ensure careful review by operational leaders and specialists, including any OT technical provider partners.**

In this OT context, remote connectivity may be best described as secure machine-to-person communication and access, rather than person-to-person. IT solutions are not typically the safest option in machine-to-person remote access situations, focused more on protecting data alone than ensuring industrial process integrity.

The technical requirements list to determine safe remote access for industrial operations may include specific items to protect uptime and process integrity, such as:

- Understanding of industrial-specific protocols, some of which may be greater than 20 years old or unique to a set of assets which are critical to operations.
- A vendor-agnostic solution to ensure mixed vintage and mixed provider assets can be managed.
- Governance controls for flexibility based on the site specifics, such as allowing the local plant manager to authorize or deny remote access requests or establish thresholds for the time duration of each remote access session.
- Ability to connect to a remote asset without requiring the endpoint asset to install any agents or local software. Such unverified agents can represent risk of disruption, not limited to freezing the asset, causing a reboot, or otherwise interfering with a process driven by that asset.
- Ability to terminate, record and playback remote sessions, including any actions taken by the operator to troubleshoot or maintain the system.



Use Cases for Industrial-Grade Secure Remote Access:

It is estimated that at least a 35% efficiency gain can be achieved through automation (4), and improvements in cybersecurity risk management can help mitigate an estimated $75M in cyber attack damage (5). Asset discovery and inventory alone can reduce labor costs by approximately $200,000 a year (6), depending on organization size, location and asset composition. In business continuity situations, the benefits of secure remote access technology become immeasurable because you are keeping operations running, even with limited staff or no local staff.

The uptime of facilities processing or producing goods and services is constantly impacted, whether by market, technical, human or other conditions that continually change. An essential component of a robust OT architecture is the ability to connect to operating assets, whether on site or remotely. This capability is especially useful to operating personnel, who bear the burden of actively managing assets day in and day out, yet who are frequently short-staffed and tasked with a wide range of work responsibilities. The same person accountable for cybersecurity may also be called on for updating standard operating procedures and for managing budget and staff planning, for example.

Use cases for industrial-grade secure remote access can include:

Staff on Medical Leave

In situations where it is difficult to allow staff to access a site, or one in which the usual supporting staff are not available due to situations such as medical leave, remote access provides an option for business continuity. Consider a refinery with operations in Argentina and on the Norwegian Continental Shelf: if local staffing is limited, secure remote access can allow technicians at Canadian headquarters to view and act on regional assets. Through the playback of these sessions, operational leaders at both sites can even refine their approaches. They may learn new ways of troubleshooting an asset based on the specific staffer's expertise, or they may update policies to prevent a resolved issue at one site from occurring again elsewhere (e.g. a worker brought in a USB that carried malware). As staff situations change, the remote access solution can enable rotating shifts from multiple geographic locations, as well as from different organizations (e.g. a partner vendor or third-party specialist). New staff who are onboarding to backfill medical leave personnel can leverage the secure remote access recordings as real-world training and can do so while maintaining mandatory social distance. This access and management flexibility increases the ability to consistently staff operations despite personnel disruptions.

Exploitation of Connectivity

Cybersecurity is an on-going concern that affects remote operations as malicious actors leverage unmanaged or poorly monitored connection points. Secure remote access solutions that centralize and control activities at a granular level can help mitigate risk of this exploitation. Closely controlling and monitoring connections, together with logs and recorded sessions, can help with cybersecurity threat mitigation as well as compliance.

Particularly in times of crisis, hackers prey on panic and human emotions. They deploy social engineering efforts and other scams that trick employees into allowing access or otherwise breaking security policies. Policies established and enforced through a secure remote access solution can raise alerts and automate actions to rapidly act on discovered threats or attempts at exploitation. Establishing secure remote access can also positively influence network segmentation, and related privileged access rights assigned to specific personnel. Together with solutions such as threat monitoring, these safeguards can increase the OT network's resilience both short term and long term.

Centralized Operations

A common use case for industrial-grade secure remote access includes situations where operations have already been centralized across multiple sites, to improve cost efficiencies or offset the challenges of staffing offshore or isolated physical locations. In these cases, centralized solutions can help standardize how secure remote connections are managed across assets at any number of locations. Considering there could be dozens of technicians from multiple vendors maintaining a globally distributed OT environment on any given day, a centralized view into all connectivity helps tighten control and reduce inefficiencies. All requests are funneled through the same secure tunnel, including verification of the technician, session authorization by the local plant owner/operator, and logging of the recorded session for oversight and staff training purposes. Rather than allowing the risky conditions of disparate and ad hoc verification of important plant connectivity, operational leaders can unify and simplify oversight of remote connections. In the case of a pulp and paper company, as one example, more than 80 non-standard solutions were consolidated down to a single remote access solution for over 140 sites (7).

Vulnerability Patching

Another common use case for secure remote access across operations is the need to rapidly deploy software patches due to discovered security vulnerabilities. The same architecture used to remotely access assets can be used as a secure data transfer tool, logging and monitoring what patches were deployed where and when. Leveraging global resources is also possible with secure remote access, allowing patches to be verified by staff in one location such as Poland, for example, before deploying the patches to sites in the Middle East. This leveraged coordination between remote access and patch distribution is a competitive differentiator that OT companies too often overlook.

Considering recent high-profile cases of companies skipping or poorly documenting patch processes, what was once a more back-end set of tasks is becoming painfully visible up the leadership chain and is under scrutiny by regulators to determine cybersecurity compliance. Patching compliance can impact whether or not a company passes security audits, and failures to comply can run into the millions of dollars. That does not include costs should an unpatched vulnerability be exploited and become known to the general public. In those cases, legal costs become an issue, together with severe company reputation issues.

Security Operations Center

A growing use case is allowing a third-party Security Operations Center (SOC) provider, specific to operations, to handle all monitoring and maintenance across plants. This can increase mean-time-to-resolution by ensuring 24/7 access to expertise anywhere, as part of the service level agreement (SLA). For specialized skills such as OT cybersecurity threat monitoring, these services can expand bench strength while keeping operations up, especially amidst heightened threat levels. Considering the significant and high-impact differences between IT and OT noted earlier, an industrial operations SOC can lend the required expertise as well as geographic coverage needed by many global enterprises. In the case of Honeywell, experts are often already well versed on the operational environment of customers and regularly provide service remotely. The SOC can typically manage multiple vendor technologies while providing regular monitoring and reporting for compliance needs if a capable solution is deployed.

WHY WE NEED TO THINK BEYOND VPN SOLUTIONS

ASSESSING SOLUTIONS

At the outset, when determining an appropriate architecture for your organization, it can be helpful to work with a secure remote access solution that has already been approved by operations and IT for use in an industrial operations organization. The Honeywell Forge Cybersecurity Suite, for example, provides controlled secure remote access, successfully deployed across Honeywell services teams, and has been used by many providers in the industrial operations space. Thus, Honeywell Forge is often already a pre-approved solution at many customer sites based on its existing use for support contract fulfillment. This saves the time, effort and coordination involved in securing approvals to expedite use of the solution, which is particularly helpful during unexpected situations such as staff health crises or malware outbreaks.

Industrialized Feature Set

Going far beyond a typical IT VPN, an industrial secure remote access solution should layer in security for OT networks in support of a defense-in-depth strategy. Most security professionals recognize that delaying attackers, complicating their attack path, or incurring upon them excessive costs are all barriers to mitigating risk of complete malicious outsider penetration and access to critical assets. Technology feature sets should include:

- A single, outbound-initiated remote connection between protected industrial assets and the centralized communication server, to provide robust security similar to a “data diode,” but with all the additional benefits of bi-directional communication.
- The ability for plant personnel to have the final say in granting remote access to any system. Remote access requests can be configured to require approval by an authorized operator in the plant, who is able to supervise and video record the remote activity.
- Extensive granular controls, such as permissions for each user, preventing them from executing specific remote activities or granting them view-only permissions that prevent them from performing any other remote activity.
- Advanced encryption, using Transport Layer Security (TLS) v1.2 and higher, with 2048bit encryption. FIPS 140-2 validated cryptographic modules are also important. (Federal Information Processing Standards (FIPS) is a US-government computer security standard put in place by the National Institute of Standards and Technology.)
- Use of certificates for authentication, following standard public key/private key cryptography protocols, including to negotiate and transfer symmetric key for data encryption.
- Support for two-factor authentication with customized access controls.
- Password vaulting that allows the use of mapped accounts without disclosing internal shared credentials to less trusted third parties.

ACCOMMODATING FOR SCALE

Another consideration for laying this foundational technology is the ability to scale and grow capabilities as operations evolve. Modular software, or global subscription options, can provide flexibility should another plant experience a sudden shift in staffing, or if malware strikes different locations and requires remote expertise to troubleshoot.

For plants with mixed vendor technologies or varied asset vintages, as well as multiple geographic locations, a provider with expansive resources can better support secure remote access usage. Global providers such as Honeywell, add value by providing hands-on centers that simulate your plant conditions. By leveraging these global centers of excellence, customers can ultimately save time, budget and costly security mistakes as they improve their organization's industrial cybersecurity maturity. As financial markets experience unpredictable volatility, partnering with a global public vendor who has decades of experience inside operations can be a safe choice to ensure your technology investment delivers both long- and short-term value.

CONCLUSION

Managing Dynamic Risk Conditions
In recent years, cybersecurity attacks have increased against industrial operators, and the nature of risks remains dynamic. Implementing a centralized, streamlined remote access solution lays the foundation for agility as needed to deploy patches, check for malware, and other cybersecurity best practices.

In addition, more recent concerns such as health pandemics may have longer-reaching consequences that are difficult to predict. Implementing a robust architecture that allows for flexible staffing and ongoing operations despite personnel disruptions can represent a wise investment.

HONEYWELL OT CYBERSECURITY EXPERTS AND SOLUTIONS CAN HELP

Honeywell is the leading provider of cybersecurity solutions that help protect OT-based assets, operations and people from digital-age threats. With more than 15 years of industrial cybersecurity expertise and more than 50 years of industrial domain expertise, Honeywell can help your company make sense of today's IT-OT cybersecurity complexity and reduce your cyber risk. We provide innovative cybersecurity software, services and solutions to protect assets, operations and people at 1000's of industrial and critical infrastructure facilities around the world. Our solutions are vendor neutral, meaning they go far beyond Honeywell proprietary devices and assets to help protect assets across your industrial network. For more detailed and specific technical support of your OT cybersecurity objectives, engage with Honeywell by contacting your local sales representative or visiting www.becybersecure.com.

1. Wired Magazine: High-Stakes Security Setups Are Making Remote Work Impossible - Mar 13, 2020
   Forrester: Prepare Your Organization For A Pandemic - Feb 7, 2020
2. Gartner: With Coronavirus in Mind, Is Your Organization Ready for Remote Work? - Mar 3, 2020
3. CISA: Risk Management for Novel Coronavirus - Mar 6, 2020
4. SecurityWeek.com Feb 4, 2019
5. CPOMagazine.com Aug 2, 2019
6. & 7. Based on Honeywell project experience - 2019

Honeywell Process Solutions
1250 West Sam Houston Parkway South
Houston, TX 77042

Honeywell House, Skimped Hill Lane
Bracknell, Berkshire, England RG12 1EB UK

Building #1, 555 Huanke Road
Zhangjiang Hi-Tech Industrial Park
Pudong New Area, Shanghai 201203

www.honeywellprocess.com

THE FUTURE IS WHAT WE MAKE IT

Honeywell

6762 Secure Remote Access WPR | 04/20