DriveLock
securing your digital tomorrow

Cyber Security in Operational Technology/IIoT

Whitepaper

DriveLock
securing your digital tomorrow

Contents

1. Management Summary

The manufacturing industry is in a process of evolution. Industry 4.0 stands for the constantly growing intelligent networking of machines and processes throughout the industry by means of digitalization. The range of opportunities will include new value creation models. Among other things, the production of customer-specific and self-designed products is made possible, and delivery times can be predicted precisely. On the other hand, quality and efficiency in the production cycle are increased.

On the downside, however, security solutions are often still insufficient. More and more companies are realizing that without the right security measures, highly automated production facilities are an easy target for cyber-attacks. Digitization will not end with the smart factory, but will extend beyond the factory boundaries through networking of the plants with external suppliers. A double-edged sword that increases both productivity as well as the risks. Companies require comprehensive and cost-effective IT security without compromising the production performance in order to take full advantage of integrated manufacturing systems, while minimizing risks at the same time.

A smart factory needs smart security and we can help you with the implementation. DriveLock offers consulting support and solutions: Application control and device control to protect against malware and to control mobile data mediums, endpoint detection tools, and software that will enable data encryption for hard drives, directories, files, and external data media. In addition, plant technicians, IT and production personnel can be continuously trained and educated with information campaigns directly at the workplace through our Security Education module.

We will glad to answer any additional questions you or your staff may have.

Please contact us at www.drivelock.com.

2. Introduction: Cyber-attacks on ICS are on the rise

Systems for manufacturing and process automation - summarized under the term Industrial Control Systems (ICS) - are used in almost all infrastructures which control a mechanical process. This ranges from energy generation and distribution, gas and water supply to factory automation, traffic control technology and modern building management.

Attacks on production facilities, critical infrastructures or devices that are not part of classic office IT system, but rather belong to operational technologies, are no longer future concerns, but a reality in everyday business life. Industrial Control Systems (ICS) or SCADA (Supervisory Control and Data Acquisition) systems are increasingly subject to the same cyber-attacks as conventional IT.

Operators urgently need to address this issue in view of the increasing frequency of incidents, and newly discovered vulnerabilities. Industrial cyber security has become a necessity.

2.1 IT vs. OT - the merger of IT and OT

Market research companies and analysts (such as Gartner) have explained the term Operational Technology (OT) as follows: It consists of hardware and software for monitoring and controlling physical devices, as well as their processes and events in the company. In a more general fashion, industrial production & control systems (ICS) and related networks and endpoints are often referred to as Operational Technology (OT).

In the past, the majority of OT systems were manufacturer-specific and separated from the information technology (IT), and most of the devices were not Internet-ready. Today, through digitalization, many ICS systems and subsystems are a combination of OT and IT. The responsibility for industrial cyber security is therefore also somewhat blurred: We refer to this as IT-OT convergence, or the Industrial Internet of Things (IIoT).

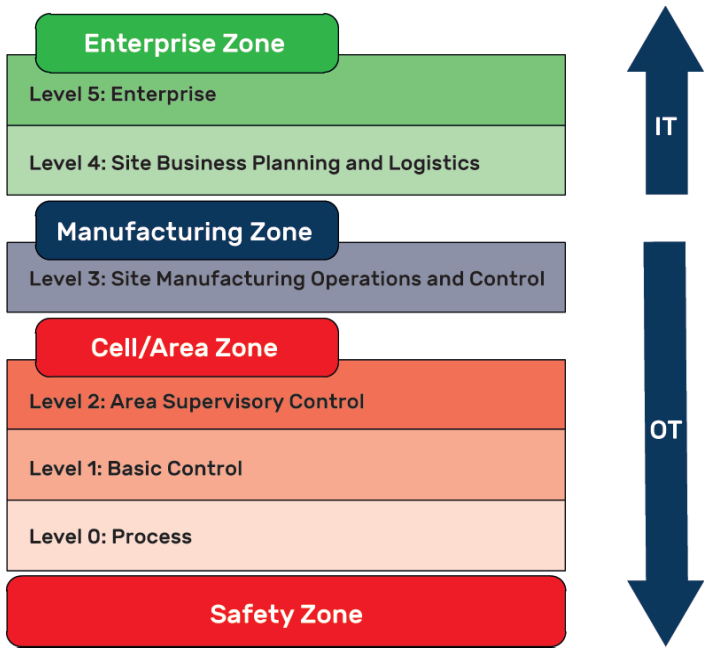
The Industrial Internet of Things (IIoT) represents the industrial form of the Internet of Things (IoT). In contrast to IoT, it does not represent consumer-oriented issues, but rather focuses on the application of the Internet of Things in the manufacturing and industrial environment.

Some analysts prefer the term "universally connected devices". The boundary between the IT and OT domain used to be very clear, yet it is becoming less delineated as the two are fusing together.

IT components and IT technologies from office IT are increasingly used in OT and are now exposed to comparable risks. This development is being accelerated by the trend towards optimizing manufacturing processes to increase competitiveness within the framework of Industry 4.0.

IT organizations typically have managed industrial workplaces (Figures: levels 4 and 5 below). IT has generally been concerned with securing systems that store data such as financial and customer information, intellectual property and forward-looking business information. These systems may consist of servers, workstations, e-mail systems, applications and databases.

The main application domain of the OT organization is the factory floor, process automation and production systems. These systems may include equipment distributed over large geographical areas, such as water pumping stations or electrical transmission stations. The entire OT domain is shown on levels 0 to 3. OT teams are primarily concerned about the security and availability of their physical and cyber assets, as any disruption could cause human damage or production downtime.[1]



Purdue Model for Control Hierarchy logical framework. Source SANS Institute

A distinction between OT and IT is possible on the basis of the following criteria:

Operational Technology (OT) vs. Information Technology (IT)[2]

Rough environment	**Location of use**	**Work desks and offices**
Plant ISB workforce	**Installation**	**Qualified network personnel**
15-20 years	**Lifetime**	**3-5 years**
Plant-specific	**Topology**	**Star-shaped**
Network down times max. several ms	**Availability**	**Seconds to minutes range accepted**
Low, switches with few ports	**Device density**	**High, switches with a high port count**
Relatively small networks	**Expansion**	**Large networks**
Often part of plant monitoring	**Network monitoring**	**By trained specialist**
Rare	**Outsourcing**	**Widely used**
Rare	**Patch Management**	**Often, daily**

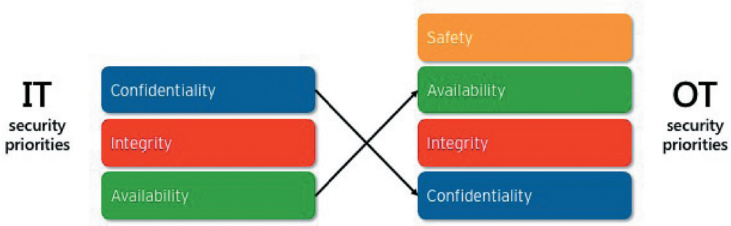
[1] Source: The Sans Institute (2020): Purdue logical framework or Control Hierarchy
[2] DriveLock: Cyber Summit 2020

Important insight:

- Personnel for the commissioning and maintenance of the systems are insufficiently trained in cybersecurity.
- The service lifetime of the assets is very long.
- The availability in the OT area is extremely important. Patching is a problematic factor (see 2.3.2).

2.2 Different protection priorities IT vs. OT

IT and OT have different definitions regarding security and priorities. While classic IT security is defined with confidentiality as the highest priority, followed by integrity and availability, OT has an additional security concern: operational safety. Operational security or occupational safety focuses on protecting people and the environment from physical damage - while information security primarily means protecting data from people (insider attack) and the external environment (e.g. cyber-attack). In OT, operational safety and availability are the top priority, followed by integrity and confidentiality.



An alternative presentation of these security dimensions can be found at Gartner.[3] The reason why an overall view of both worlds has become unavoidable is demonstrated by the much-cited incident at a chemical plant in Saudi Arabia. Malware was discovered in the plant that specifically attacked the security systems. It was specifically designed to disable the protective functionality. The malware known as Trisis was characterized by a very high degree of specialization that targeted the security system. It was coincidental that the attack was discovered and there were no further consequences.

Architecting Security for New OT Security Requirements

Source: Gartner (September 2018)

[3] Source: Gartner (2020): OT Security Best Practices

2.3 Why OT has become vulnerable

2.3.1 The change to an open OT

As mentioned above, production IT is no longer isolated from the internal or office IT and has become more vulnerable. There are reasons for this, which are related both to the history of existing production systems and to digitization:

- **External control: Currently, production facilities are increasingly controlled and monitored externally (e.g., when technicians access production facilities via remote maintenance access).**
- **Production reports: The company management requires reports from the production line in real time. This requires a connection from IT networks to OT.**
- **IIoT becomes IIot: The advent of the Internet of Things enable many control possibilities for production plants. Based on the Internet of Things (IoT), the intelligent "Smart Factory" is being developed under the keyword IIoT (Industrial Internet of things), which can be controlled via endpoint devices.**

This phenomena is only possible by coupling the production IT to networks and merging IT and OT to ensure permanent accessibility of OT facilities (manufacturing/production plants) from the outside. These networks can be attacked.

2.3.2 Weak points of ICS systems

Traditional ICS systems and their IT support facilitate cyber-attacks.

Durable production plants and obsolete systems

Classical production systems often have runtimes of 7 to 10 years and are not typically replaced after a few years - like a desktop or laptop computer, for example. In many cases their operating systems are obsolete and security updates (patches) are no longer available.

Problematic patching

Patching is a problematic factor in an industrial environment, as systems have to be shut down and production plant availability suffers as a result. Obsolete systems are a likely breeding ground for zero-day attacks, attacks through unclosed security holes in the software. Attackers will then have privileged network access.

Deficient IT security solutions

Old production plants are not equipped with IT security solutions by default since they were not designed with cyber security protections in the past. Antivirus scanners cannot be easily installed on production control systems because there is a risk of losing (manufacturer) certificates and warranties. Often the real-time scanner is also disabled here. It is not always possible to get updates for the scanner in a timely manner.

Too little IT security know-how

Production employees responsible for operating the systems are largely unfamiliar with possible attack vulnerabilities and IT risks. Overall, there are too few IT specialists with security know-how.

2.4 Why is the industrial sector particularly interesting for attacks?

The attractiveness of the industry sector for cyber-attacks is based on the high demand for availability and the concept of safety, which takes occupational safety into account. A manipulated plant or industrial robots can become a danger to humans. Additionally, in the industrial production process only downtimes (as shown above) in the millisecond range are tolerated. The stand still of production processes due to an attack causes inflated costs.

Cyber criminals use these conditions as a means of exerting leverage for their attacks (e.g., with blackmail software). Some well-known examples from the industry follow:

++++++++++++++++++++++++++++++++ HACKER ATTACK ++++++++++++++++++++++++++++++++

- The cyber-attack on the Norwegian aluminium producer Norsk Hydro paralyzed important IT systems. The blackmail software/Ransomware also attacked production systems via the office network and hindered production. As a result, the enterprise's share price fell, but the price of metal rose. The IT disaster was communicated very openly by Norsk Hydro.
- The Stuxnet computer worm - originally used against the Iranian nuclear program - attacked control systems for industrial plants and, in the course of its spread, also damaged other industrial companies.
- The Trojan Industroyer shut down the Ukrainian power grid. The malicious code was capable of corrupting multiple communication protocols used by SCADA (Supervisory Control and Data Acquisition) systems.

3. NIST AND CMMC Compliance Is Key

The United States Department of Commerce, in collaboration with the National Institute of Standards and Technology, has enacted strict controls with respect to manufacturers who must comply with cyber security standards which must be abided by tier 1, 2, 3, 4 and 5 level suppliers for those who contract with the U.S. Federal government. In addition, primary suppliers that subcontract to CMMC levels 2 and 3 are ultimately responsible for the cyber security of those contractors. Hence, this has led to the commercial version of NIST in the way of CMMC.

CMMC compliance standards are key for ensuring contract security when handling Controlled Unclassifi ed Information (CUI). This is important due to the levels of controls that need to be implemented. Each contract has five different levels that are specified below. These controls are mandated, and if not enforced correctly, can result in the loss of a US Federal contract. Albeit, the Cybersecurity Maturity Model Certification is continuing to evolve, greater than 85 % of these controls can be satisfied by DriveLock endpoint security software. The CMMC model includes the following 5 levels:

Level 1 – Federal contractors wanting to pass an audit at this level must adhere to 17 controls of NIST 800-171 rev1.

Level 2 – At this level U.S. Federal suppliers must be able to handle 48 controls of NIST 800-171 rev1 and another 7, as mentioned in the NIST publication.

Level 3 – In order to reach level 3 certification, the final 45 controls of NIST 800-171 Rev1 plus another 13 controls are to be met or exceeded.

Level 4 – On top of levels 1 through 3, 11 more controls in the NIST 800-171 Rev2 document must be met as well as 15 new controls for an ongoing security effort.

Level 5 – To reach the zenith of this spectrum of controls, Federal contractors MUST implement the final four controls in NIST 800-171 Rev2 and 11 new ones as well.

In attempting to minimize risks for industrial production and control systems result from threats which, due to existing weaknesses, cyber threats can cause damage to the ICS and a fi rm. Some of these damage points may include a company's proprietary data, technical and/or financial information, loss to a company's reputation and eventually fiancial losses attributed to these leaks. Below are some examples of how data can be vulnerable when these controls are not met in a manufacturing environment.

The critical and most frequently occurring TOP threats to ICS are published annually by manufacturing trade organizations or government agencies that support cybersecurity in information technology. The following table demonstrates some of most important ones.

Top 3 threats	Trend since 2016
Infiltrating malware via removable drive and external hardware	↑
Infection with malware via Internet and Intranet	↑
Human Error and Bad Actors	↑

In other places there are, among others, a compromise of the extranet and cloud components, social engineering and phishing, (D)DoS attacks.

TOP 1: Infiltrating malware via removable drive and external hardware (e. g., Bad USB)
Example: Stuxnet attack via a removable drive (USB drop attack).

For this purpose, commercial removable drives and hardware that exploit plug & play are also used, e.g.:

- USB Rubberducky
- Bash Bunny
- USB Ninja Cable

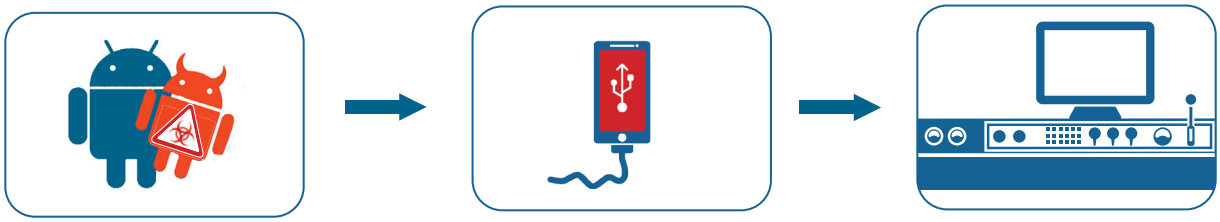
Infiltration through removable media can be controlled at the user and level and all files transferred can be audited and controlled. For further maturity of this control, encryption of these USB devices needs to be enforced to prevent infiltration of malware via removable media. Additionally, preventing solely against malware can leave insider threat security flaws. In these events users can still steal sensitive information. This information should be able to be catalogued to each user and all forensics of this kind of threat should be traceable to a figurative patient zero. To prevent exfiltration and malware from being executed, controls can be implemented such as scanning USB devices and other removable media for malware before allowing them to connect and the drive to mount. This will enforce better controls against these kinds of attack vectors.

DriveLock as a product can be implemented to cover the majority of CMMC and NIST controls as was mentioned earlier. Additionally, DriveLock can be configured to run side by side other solutions that a client may have. There is no need to rip-and-replace an entire solution. Rather, DriveLock can be added through a tiered and modular way that fills the gaps in this process, all the while helping to manage Microsoft's AV Defender©, MS Bitlocker© and MS Firewall© products. This helps consolidate current tools already used by many firms, and can be managed under a single pane of glass.

This allows the configuration to be customized to harden the security posture of any client, as well as becoming compliant with the ever so strict NIST and CMMC controls. These controls can effectively eliminate many risks, making compliance and continued security the mainstay of a firm's competitive advantage.

Attack scenario:

A leading industrial company operates over 15 year old systems, whose controller system is based on Windows XP. In order to install updates, the industrial systems are equipped with a USB port that represents an unprotected interface to the SCADA system.



These USB interfaces are not only used by the employees for the installation of updates but to also, for example, to listen to music, or charge mobile phones.

The mobile phone of an employee infected with malware was therefore capable of transmitting the virus onto the SCADA system, and completely halt the normal operations of the factory.

Consequences:

- **The tool was destroyed.**
- **The maschine was damaged.**
- **The construction data was sublimely modified.**
- **Hackers drive the working arm of the production robot to the end positions, thus endangering the life and limb of the workers.**

Source: DriveLock

TOP 2: Infection with malware via the Internet and intranet

According to Comparitech the author identified 268,362 "never-before-seen" malware variants in 2020.[4] This was an increase of 74 % from 2019 when SonicWall recorded a total of 153,909 "never-before-seen" malware variants. At peak times there were up to 420,000 new variants per day. In total, the number of malware variants increased by 117.4 million in the period under review - with an upward trend compared to the same period last year.

TOP 3: Human error and Bad Actors

These include attacks with phishing emails that exploit the inexperience or carelessness of employees. As mentioned above, production facilities are not monitored and maintained by trained IT personnel. Moreover, insider attacks should not be underestimated. This also includes the aforementioned perpe-tuated attack of malware from office to production systems.

4. Protection measures for ICS systems

Four widely cited effective precautions to protect against cyber attacks:

1. **Restricted use of removable media and mobile devices**
   Rules for the use of removable drives and endpoint devices should be established and widely distributed. The use of removable drives and mobile endpoint devices in ICS environments should fundamentally be limited.

   Fully encrypting data mediums is recommended (including maintaining notebooks).[5]

2. **Protection against malicious software**
   A concept for protection against malware and its implementation is required. The threatened IT systems may cause infection such to external interfaces and removable media which must be considered.

3. **Awareness raising and workforce training**
   Operating personnel must be regularly informed and educated on the relevant security threats in the OT area.

4. **Auditing, logging and detection of events on endpoints and systems**
   Operational and safety-relevant events must be identified promptly.

[4] https://www.comparitech.com/antivirus/malware-statistics-facts/
[5] German Federal Office for Information Security (2019): Recommendation: IT in the production, Industrial Control System Security, https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005E.pdf?__blob=publicationFile&v=1

5. Industrial Security control with DriveLock

In this chapter, we will describe how the DriveLock Zero Trust Platform helps to eff ectively and securely implement these measures in the industrial sector. DriveLock cloud-based endpoint security solutions help "harden" your production systems.

5.1 The Zero Trust security approach as a benchmark

Zero Trust is a security concept whose goal is to protect companies from threats and the effects of data theft. The model is based on the principle **"never trust, always verify"**. Compared to conventional concepts, the Zero Trust model represents a paradigm shift in that it treats all devices, services and users equally and fundamentally distrusts them. Traditional security concepts combat the attacker from outside the network, but do not consider them an intruder after they have entered the network.

Zero Trust fundamentally means:

- Access to all resources and assets is secured and are location independent. This includes applications, network drives and USB devices.
- Access control is based on the principle: Does a user really need this application for their daily work and which rights (e.g., read, write, full access) do they get? This principle is strictly observed.
- All data traffic is checked and logged.
- The infrastructure is designed to scan everything and trust nothing, including employees.

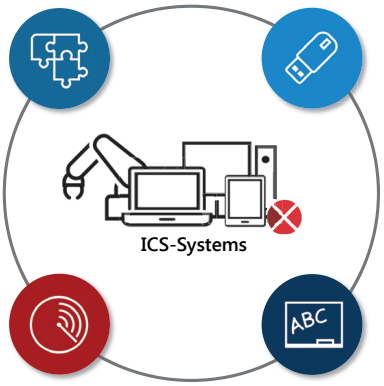
The Zero Trust concept has no influence on the speed or performance of the endpoints or devices, since the so-called "Agent" is not always running.

With its Zero Trust platform, DriveLock offers a range of effective IT security solutions that live up to this principle.

1. Device Control
2. Application Control
3. Security Awareness
4. Endpoint Detection & Response

DriveLock Zero Trust Platform

Application Control
Flexible application control with a granular set of rules. Different learning modes and integration of software distribution systems.



Device Control
Controlled and logged access to external drives and devices with the appropriate user acceptance.

Endpoint Detection & Response
Continuous real-time monitoring of endpoints. Over 600 different events are detected, correlated and evaluated.

Sercurity Awareness
Multimedia Security Awareness library with regular updates or the own content. Notification based on triggers (events, recurring, etc.).

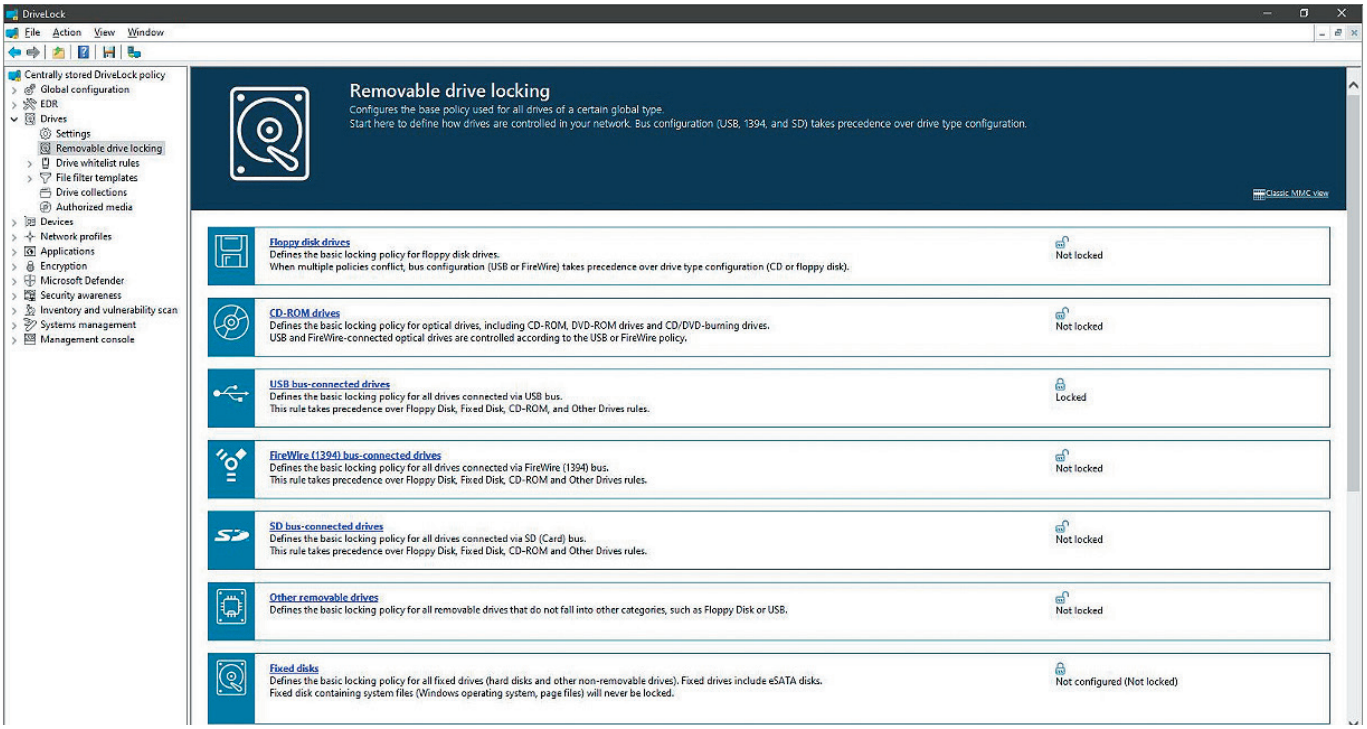
Source: DriveLock

5.1.1 Restricted use of removable drives and external devices by Device Control

Careful handling of (mobile) data carriers and the exchange of data carriers is recommended. With smart device control, a large number of granular setting options are relevant for flexibility and smooth production flow. A general ban of data carriers such as memory sticks is not plausible in many production environments.

However, mobile data mediums can also be lost, so you should always encrypt data on these devices to prevent unauthorized access. In addition, the careless handling of data mediums from unknown sources can allow malware to enter the ICS systems. This must also be prevented.

Device Control from DriveLock:



With **DriveLock Device Control** an organization can prevent sensitive data from getting onto external storage media and prevent external data mediums from easily being attached and read. This gives you control over external data mediums and data flow. DriveLock checks each attached device and locks it if necessary. This ensures that only approved devices or external drives can be used.

If an employee connects a device to the USB port, the computer recognizes whether it is an external hard disk, a USB stick or like device. DriveLock can be used to control which USB media are allowed. Another rule could be to allow the connection of USB devices, but the user is not allowed to write any files to the device (enforcing a read-only solution). With DriveLock, you can create shadow copies to secure production sites that comply with the GDPR or similar requirements in US states. In addition, DriveLock provides features for the enforced encryption of data written to external drives.

When using external devices, the issue of security awareness is of great importance. Today, users take advantage of the ever-present USB ports in many different ways. The "simple" charging of a smartphone through a USB port of an ICS can lead to extensive security problems. Besides the management of black and whitelists for devices, the use of so-called usage guidelines is very important. Here the device is only released after an acknowledgment by the user or only after requiring entry of their username and password.

5.1.2 Application Control protects against malware

Application control based on a positive list is one of the most effective preventive measures.

DriveLock Application Control prevents malware execution, the exploitation of tools (such as Powershell) by malicious scripts and protects against zero-day exploits. This is based on a procedure that checks each program to be executed against a whitelist (positive list) of approved programs. This list is dynamically extended. Unknown software, which might have slipped through a virus scanner that is not current, is not executed.

This intelligent and learning whitelist management allows a large number of very heterogeneous ICS to be securely managed with minimal staffing. The solution thus relieves the workload for security teams and ensures company-wide that only known and secure applications are able to run.

In comparison: The problem with antivirus (AV) software is that only known malware is detected. But malware disguises itself or is not known to the AV scanner at the time of an attack. In general, these scanners are faced with a task that cannot be accomplished. With over a quarter million new variants that came about in 2020, AV software cannot maintain real time updates on the threats. Hence, black and whitelisting are key options to enhance AV efforts in a network.

You may now be wondering if Microsoft Windows application control provides protection similar to DriveLock. Windows 10 includes AppLocker, a greatly improved successor to the prior Software Restriction Policies. However, if you compare DriveLock Application Control to AppLocker, you will find that AppLocker only offers limited protection:

This service is not sufficient and only fully functional Application Control from DriveLock can provide the necessary security in this instance. The capabilities of DriveLock reach far beyond this. For example, DriveLock supports older operating system versions (prior to Windows 7). Policies can be implemented in a more granular way (e. g. technicians are granted higher rights than business users). DriveLock also requires much less administration to provide the same level of security as AppLocker.

Finally, here are some examples of scenarios that DriveLock makes possible, but which are impossible or very difficult to configure with Windows 10 alone:

- Automatic whitelisting of all applications installed by specific administrator or service accounts.
- Blacklist or whitelist rules based on an enterprise-wide application database.

5.1.3 Use case: Maintenance/emergency access to a production system

The effective interaction of application control and removable drive control will be explained using a maintenance example.

Special requirement:

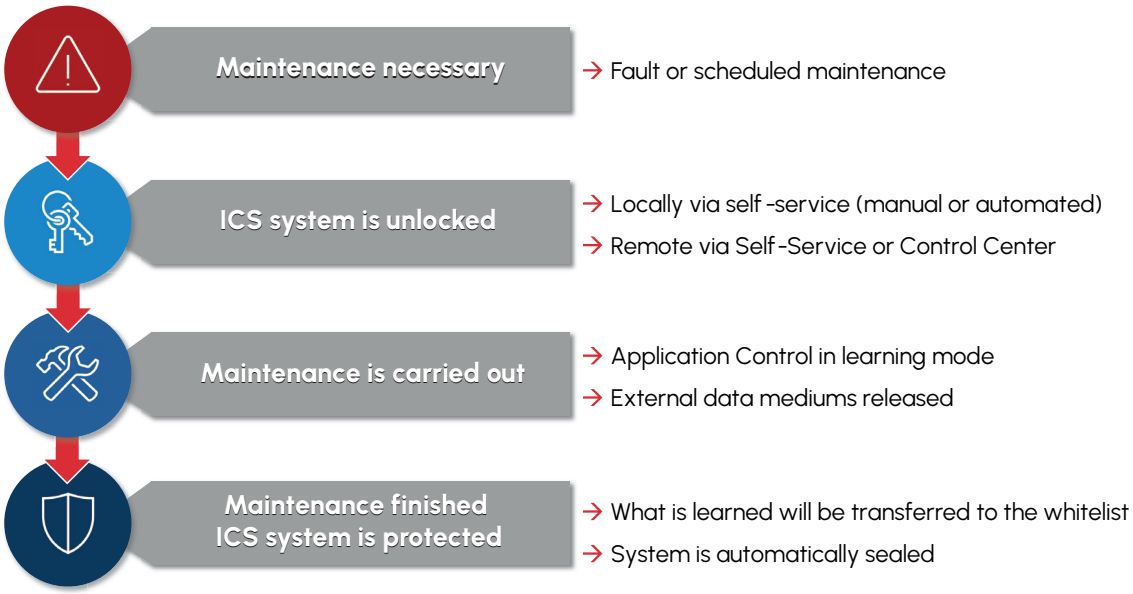
In the industrial environment, maintenance work on IT systems is often carried out ad hoc or is tied to very narrow time slots. It is thereby important that no dependencies to a central service desk can arise, and that a secure operation is guaranteed at all times. This also structures the central management of corresponding security solutions for production facilities in a very labor-intensive manner. A combination of different approaches is necessary to counteract this effectively. On the one hand, it is crucial that maintenance work be carried out in a decentralized manner without a need to observe the corresponding group IT lead times - even during the ICS offline operation. On the other hand, the solutions must be able to log or document safety-relevant changes of the machine controls. Finally, when using Application Control, it must be possible to automatically make changes to the black and whitelists when updates and patches are made. Self-learning whitelists are able to detect software updates individually per the ICS and allow them access based on an applicable set of rules.

Regarding the actual procedure:

In case of scheduled or ad hoc maintenance (or malfunction), technicians first unlock the system. This can be done manually, or in the case of production lines, remotely (e.g., from the control station). In this scenario, the "Security" is opened for a short time. An essential aspect of this is that full logging takes place during the time slot with "relaxed" security.

Technicians are then able to perform software maintenance while DriveLock's application control in the learning mode "registers" the software update. DriveLock ensures that software updates and clean installations are whitelisted after the maintenance mode has ended. It guarantees that the new applications can be executed without permanently bypassing the defined security profile.

Use case maintenance/emergency access

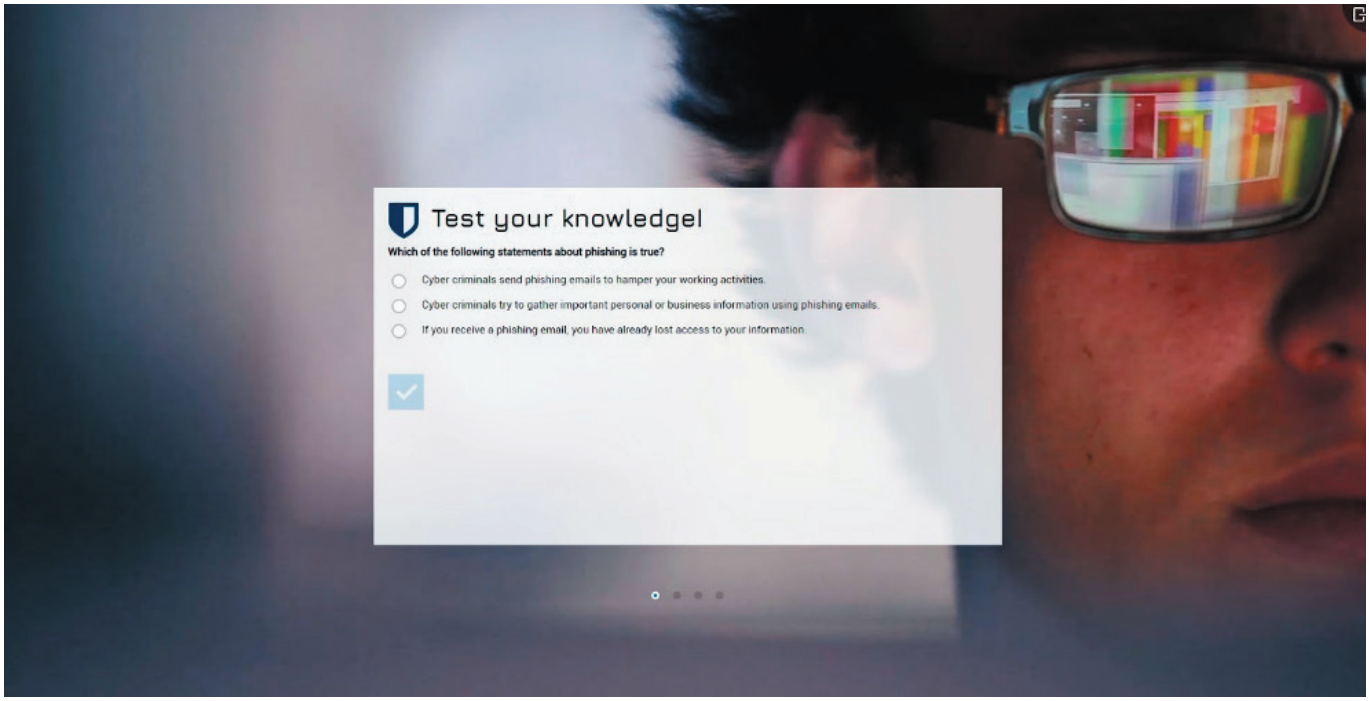


5.1.4 Avoiding human error and educating employees through Security Awareness

The employee remains the weakest link in a holistic security strategy. Research amongt security officers have repeatedly shown that human error is one of the greatest risks. Such negligent actions are not necessarily malicious. We all make mistakes and hackers are becoming more sophisticated. It is therefore important to educate the workforce and explain to them how important they are within the chain of protective measures. Security Awareness Training will help sharpen a sustainable security awareness.

Security Awareness from DriveLock:

DriveLock Security Education Programs such as anti-phishing training will help teach employees to react properly to phishing and social engineering attacks and create a sustainable security awareness among users. Occasional security awareness can be applied at the time of work - on the job: When a new application is launched, DriveLock checks whether it is a secure application and, if in doubt, outputs a short security campaign on the topic of "Dealing with New Applications". Users receive context-related safety instructions.

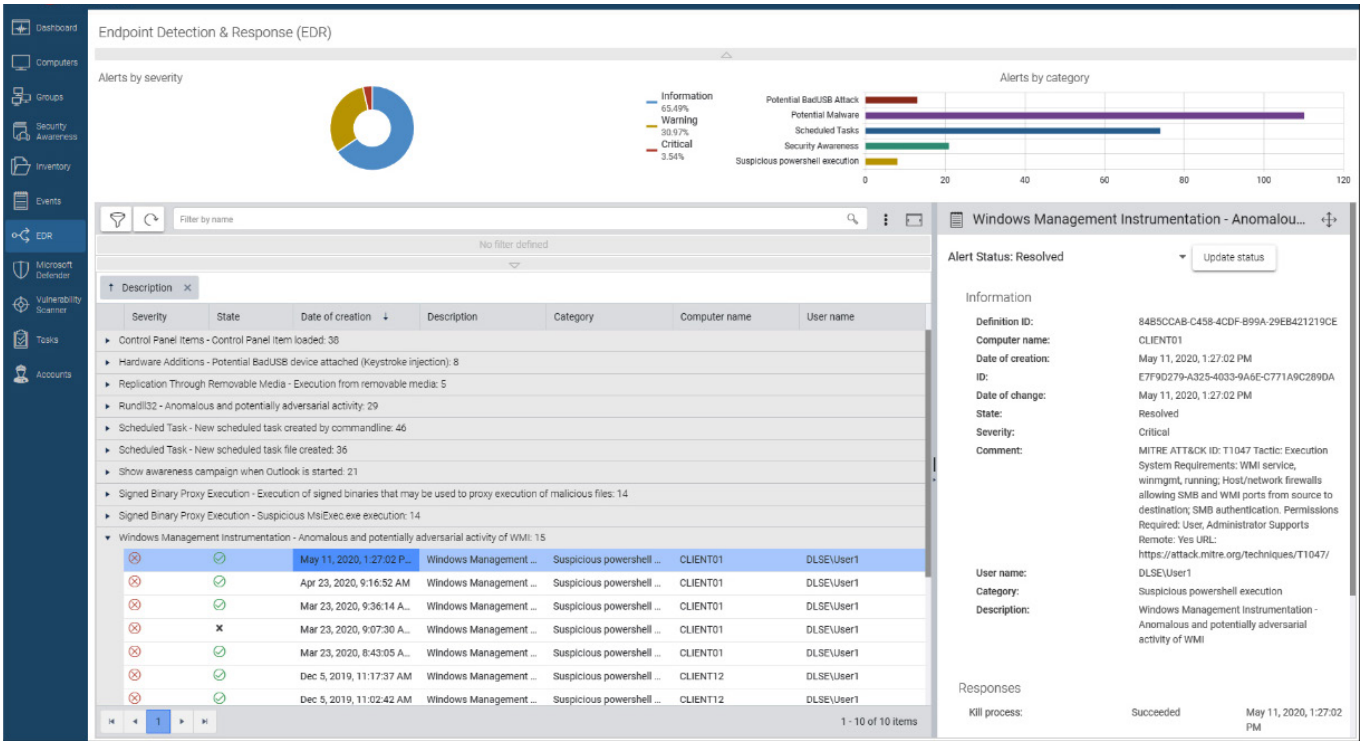


5.1.5 Endpoint Detection and Response

The aforementioned prevention measures make life significantly more difficult for attackers. Although, they do not give a 100 % guarantee of complete safety. There are cases where these preventive measures do not go far enough. If malware has already penetrated the systems, then tools are important to detect the intruder and to recognize the attack tactics and patterns.

Endpoint Detection & Response (EDR) from DriveLock

Endpoint Detection & Response solutions, or EDR for short, provide real-time visibility and control over endpoint devices. They enable behavioral and forensic analyses by recording and monitoring security-relevant events. You can react to critical incidents and the receipt of alerts, for example, a warning, either automatically or manually.



5.1.6 Full encryption of data mediums and maintenance notebooks

To protect sensitive data, it is recommended that an organization encrypt external data mediums. In this context, the encryption of maintenance notebooks is also mentioned as a measure against the introduction of malware.

Encryption modules from DriveLock:

DriveLock Encryption Solutions enable the encryption of hard disks, directories, folders, files and USB sticks:

- **Transparent and fast, hard disk encryption**
- **Reliable file and directory encryption**
- **Encryption of removable media such as USB sticks, CD/DVD or mobile hard drives**
- **Extension of the handling of Microsoft BitLocker encryption with additional functions essential for companies (DriveLock BitLocker Management)**

Advantages of DriveLock BitLocker Management over Microsoft-only functionality

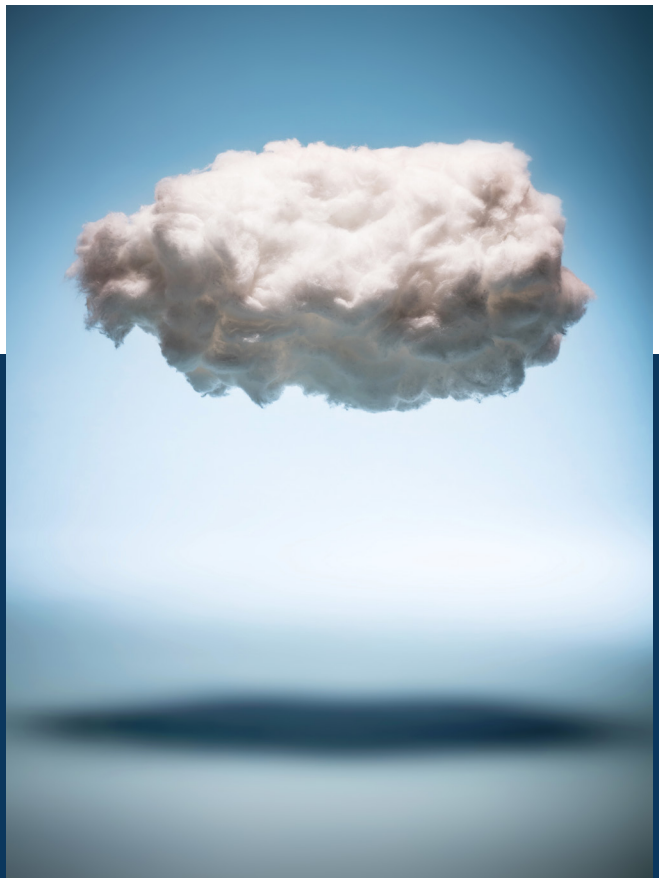
BitLocker is the Full Disk Encryption included in Windows 10. But with increasing regulatory requirements, BitLocker encryption alone is often insufficient. DriveLock BitLocker Management manages the existing BitLocker installation and adds essential features to it.

5.2 Effective protection for industrial plants with security from the cloud

As we have shown in the first chapters, not only are the potential intrusion points for malicious programs increasing, but the number of malicious programs is growing exponentially, and the attacks are becoming more and more complex. In order to be able to implement the recommended measures with your own personnel (i.e. to introduce and support the solutions) you will need to invest in employees, training and systems. The lack of skilled workers is only one of several obstacles in this respect. These general conditions can lead to security solutions being set up and configured initially, but there are no further customizations during operation. As a result, the level of security deteriorates over time.

An alternative is to have the proposed IT solutions managed by a service provider.

DriveLock offers its Endpoint Protection solutions as **Managed Security from the Cloud**. We can provide a comprehensive, fully configured security profile based on the respective solution modules. This allows the production company to start protecting its endpoint devices immediately. In addition, these security profiles are constantly being further developed by us and adapted, as well as optimized to meet the current requirements.

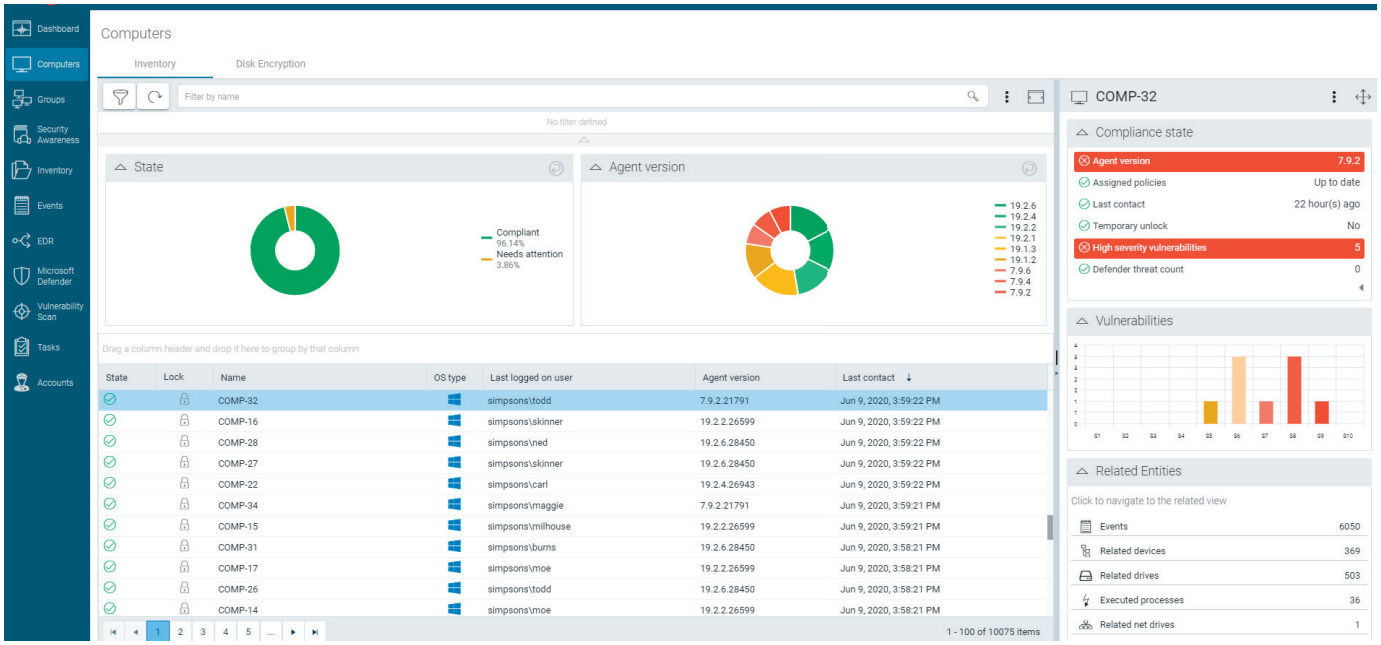


You will benefit from:

- Total Cost of Ownership advantages
- Integrations with Microsoft and Linux based systems
- Rapid deployment & automatic updates
- No Rip and Replace implementation methods
- Predefined security policies
- No additional investments in hardware
- Continuing advancement to protect data with the latest security methods

5.3 DriveLock also offers

- A unified interface for configuring all protection functions/modules/protective measures - the DriveLock Management Console (DMC)



- A modern and customizable web-based interface with extensive evaluation and analysis options - the DriveLock Operations Center (DOC)
- A flexible, policy-based management for online and offline systems
- Integration possibilities with, for example, software distribution or Security Information and Event Management (SIEM) systems
- Extensive logging options with an integrated anonymization of personal data

Conclusion

The manufacturing industry and OT are undergoing changes with the advent of digitization, yet security solutions are still lagging behind. Attackers are profiting from the insufficient security knowledge of employees, from long-running systems with limited security solutions and an OT networked with the office IT, which is not prepared for cyber threats.

Companies must have a comprehensive and cost-effective security solution without compromising production performance, so that they may take full advantage of integrated manufacturing systems while minimizing risks at the same time. DriveLock offers a tried and trusted Zero Trust software platform with a comprehensive security solution that is second to none. So it doesn't matter if you are a SME or Fortune 100 firm DriveLock can help you find your security.

Contact us!

DriveLock SE
+49 (89) 546 36 49-0
info@drivelock.com

www.drivelock.com