DriveLock
securing your digital tomorrow

DriveLock Vulnerability Management

Whitepaper

DriveLock
securing your digital tomorrow

Contents

DriveLock
securing your digital tomorrow

Executive Summary

In times of digital transformation, your success depends on how you can reliably protect people, businesses and services from cyber-attacks and the loss of sensitive data. With the omnipresence of information technology and its dependencies, organisations face an increase in the number and severity of threats. This has a negative impact on operations, assets, and people. Given the potential damage that can result from human error and targeted cyber-attacks and other threats, an organisation must place greater emphasis on managing the vulnerabilities and risks associated with its systems.

Attackers exploit vulnerabilities or weaknesses in software to gain control of computer systems, steal sensitive information, and cause disruption to operations. Vulnerabilities can be found in operating system components or software applications. IT managers must identify and control the risks associated with these vulnerabilities. Managing the myriad configurations within system components has become an impossible task using manual methods. Whenever possible, organisations look for automated solutions that can reduce costs, increase efficiency, and improve the reliability of cybersecurity efforts over the long term. It is important to identify vulnerabilities that require immediate attention. Automated, risk-based vulnerability management helps to manage a large number of vulnerabilities and maintain focus for fast and effective action. The DriveLock Vulnerability Management solution identifies vulnerabilities on endpoints, makes them visible and thus prevents potential malware attacks. IT administrators can identify and control the risks associated with vulnerabilities.

Ever-changing IT landscapes and evolving cyber threats mean that regular scans and compliance checks are necessary to protect businesses from cyber-attacks. To keep your corporate environment secure, you need a vulnerability management solution that gives you complete visibility into your attack surface so you can manage and measure your cyber risk. DriveLock Vulnerability Management is part of the DriveLock Zero Trust Platform and provides you with a comprehensive view of your infrastructure.

Threat landscape

Cyberattacks and data breaches can be caused by a variety of things. For example, in the case of Equifax [ZDNet], not fixing a known vulnerability that can affect the software or libraries used - within a reasonable amount of time - has serious consequences. The Equifax data breach is a typical example of a significant cyberattack which exposed the personal information of almost 150 million customers [ZDNet].

In other cases, unsecured data that remains exposed to the Internet can be a problem. Zero-day vulnerabilities can be exploited at will before fixes are available, or in some of the worst cases, an organisation or individual can be targeted by state-funded Advanced Persistent Threat (APT) groups that have considerable resources and tools at their disposal.

In fact, sometimes a single vulnerable endpoint, network, server, or application is enough to affect millions of people. Shellshock, Heartbleed, Poodle and EternalBlue are just a few of the notorious vulnerabilities that open the door to malware data theft and other attacks. There are countless others - in 2017 there were 1,522 publicly reported vulnerabilities. The Zero Day Initiative discovered that 929 of these were labelled "critical" or "high" [ZDI].

Costs for companies

In addition to the threat landscape, there is the question of the cost for companies that are subject to an attack or data breach. Cybercrime is a profitable business, with relatively low risks compared to other forms of crime. The Ponemon Institute has prepared a management report. In 2019, the average time it took to detect and contain a breach was 279 days. The faster a data security breach can be detected and contained after a cyber-attack, the lower the costs. The average total cost of a "data breach" worldwide amounts to US$3.9 million, in Australia AU$2.62 million.

279 Days Time to identify and contain a breach (MTTD 206, MTTR 73)	**$3.9 M ($4.8M Germany)** Average total cost of data breaches	**+27 % ($4.45M vs. $3.5M)** Breaches caused by a malicious attack were more costly than breaches caused by human error	**51 %** Malicious attacks were the most common and most expensive root cause of breaches

The challenge

Attackers exploit vulnerabilities or other weaknesses in software to gain control of computer systems, steal sensitive information and cause service interruptions. Vulnerabilities can be found in operating system components or software applications. IT administrators must identify and manage the risks associated with these vulnerabilities. Organisations that do not scan for vulnerabilities and do not proactively address discovered flaws are highly likely to have their computer systems compromised.

Vulnerability Management

The Australian Cyber Security Centre (ACSC) urges organisations to conduct vulnerability management activities in order to be better equipped in identifying, prioritising and responding to enterprise security vulnerabilities. Because the nature of cyber threats evolves over time, conducting regular assessments are also important to meet the challenges of today's threat landscape (ACSC p3). However, vulnerability management products can be very complex to use, use a lot of network bandwidth and consume system resources. As a result, organisations are reluctant to perform daily vulnerability scans. Instead, scans are performed weekly, monthly or quarterly. And even after a scan is complete, IT departments are faced with the question of how to easily fix vulnerabilities. Vulnerability Management continuously assesses risks, and automation makes it a daily routine.

Effective risk-based vulnerability management requires a clearly defined process.

A Vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Note: The term weakness is synonymous for deficiency. Weakness may result in security and/or privacy risks. [NIST].

The **NATIONAL VULNERABILITY DATABASE (NVD) [NIST NVD]** is the US government repository for standards-based vulnerability management data represented by the Security Content Automation Protocol (SCAP). This data enables the automation of vulnerability management, security measurement and compliance.

Use Tools for Automation

Where possible, organisations try to normalise the data describing the system so that the various monitoring results can be combined, correlated, analysed, and reported in a consistent manner. Managing the myriad configurations within the system components has become an impossible task using manual methods. Whenever possible, organisations look for automated solutions that can reduce costs, increase efficiency, and improve the reliability of cybersecurity efforts in the long run. Standardised tools for automation is recommended by authorities [NIST P21]. For organisations with a large number of components, the only practical and effective solution is to use automated solutions that use standardised reporting methods such as SCAP.

Standardisations with SCAP

When purchasing solutions, organisations are well-advised to shortlist SCAP-validated solutions. **SCAP** means **Security Content Automation Protocol**. SCAP provides a **common language for describing vulnerabilities, misconfigurations and products**. For organisations who want a reliable way of conveying the security standing of the enterprise architecture within the organisation, this is a useful starting point [NIST-SCAP]. SCAP comprises a set of specifications that standardise the format and classification used to transmit information on software errors and secure configurations.

For example, the Common Vulnerability Scoring System **(CVSS)** is a specification within SCAP that provides an open framework for communicating the characteristics of software vulnerabilities and for calculating their relative severity. The CVSS provides a way to capture the key characteristics of a vulnerability and produce a numerical score that reflects the severity of the vulnerability. The numerical assessment can then be adapted into a qualitative ranking (for example, low, medium, high, and critical). This is to help illustrate and aid in the accurate assessment and prioritisation of vulnerability management processes [FIRST]. CVSS is a published standard that is used by organisations worldwide. CVSS assessments can be used to improve your security posture.

OVAL® is a trademark of the US Department of Homeland Security (DHS). Open Vulnerability and Assessment Language (OVAL) is a language for representing system configuration information, assessing machine state, and reporting assessment results. International in scope and free for public use, **OVAL®** is an information security community effort to standardise how to assess and report upon the machine state of computer systems. OVAL includes a language to encode system details and an assortment of content repositories held throughout the community.

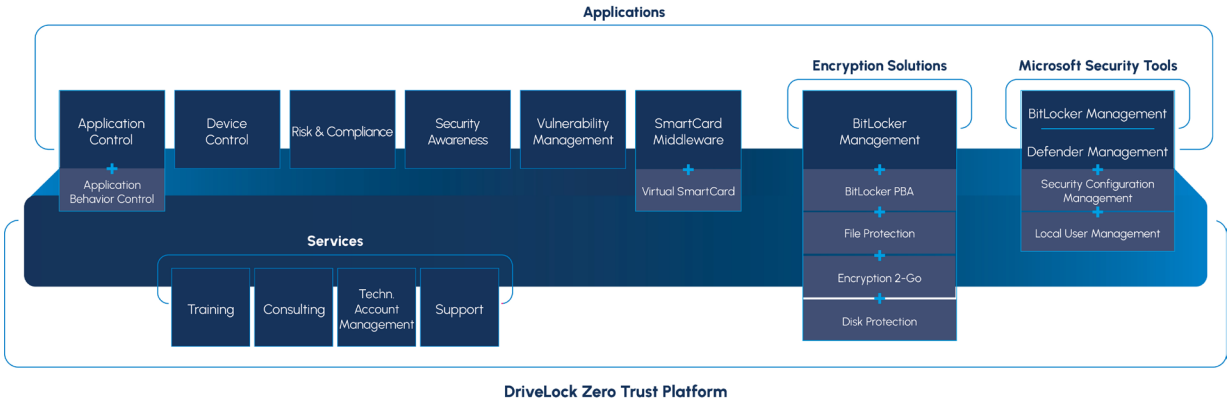
Sponsored by the US Department of Homeland Security and a registered trademark of The MITRE Corporation, **CVE** is a SCAP specification that provides unique common names for publicly known vulnerabilities in information systems [Mitre]. Following the NIST's recommendation, security software must include support for Common Vulnerabilities and Exposures (CVE).

The DriveLock Vulnerability Scanner

Ever-changing IT landscapes and evolving cyber threats mean that regular scans and compliance checks are necessary to protect businesses from cyber-attacks. To keep your corporate environment secure, you need a vulnerability management solution that gives you complete visibility into your attack surface so you can manage and measure your cyber risk. DriveLock Vulnerability Management is part of the DriveLock Zero Trust Platform and provides you with a comprehensive view of your infrastructure.

You receive a continuous assessment of your security and compliance posture so that you can discover unknown assets and vulnerabilities and prioritise vulnerabilities to minimise your cyber risk and prevent breaches.

DriveLock Vulnerability Management (VM) is available both on-premise and as a cloud-based service that performs an automated daily vulnerability scan. Organisations can quickly identify their threat and vulnerability risk. DriveLock VM provides continuous visibility into IT systems. It builds on a proven SCAP feed database with comprehensive vulnerability coverage. And utilising an OVAL scanner it includes a language to encode system details. The DriveLock vulnerability scanner automatically scans for vulnerabilities on a computer system. It does this on a scheduled, ad-hoc or - if desired - regular basis. DriveLock is using a vulnerability database that is updated several times a day.



Key Benefits

- Continuous assessment of vulnerabilities and your current security posture
- Always knows changes to your attack surface
- A comprehensive overview of your IT infrastructure
- Focus on what is important by quickly identifying which vulnerabilities need to be prioritised for the best risk reduction
- Ensures security and demonstrates compliance using specific metrics that clearly communicate status
- Standardisation through SCAP-validated solution
- Scalable solution for small, medium, and large enterprises
- Customised implementation and hosting models for your company

Focus on helping customers understand the vulnerability risk their business faces.

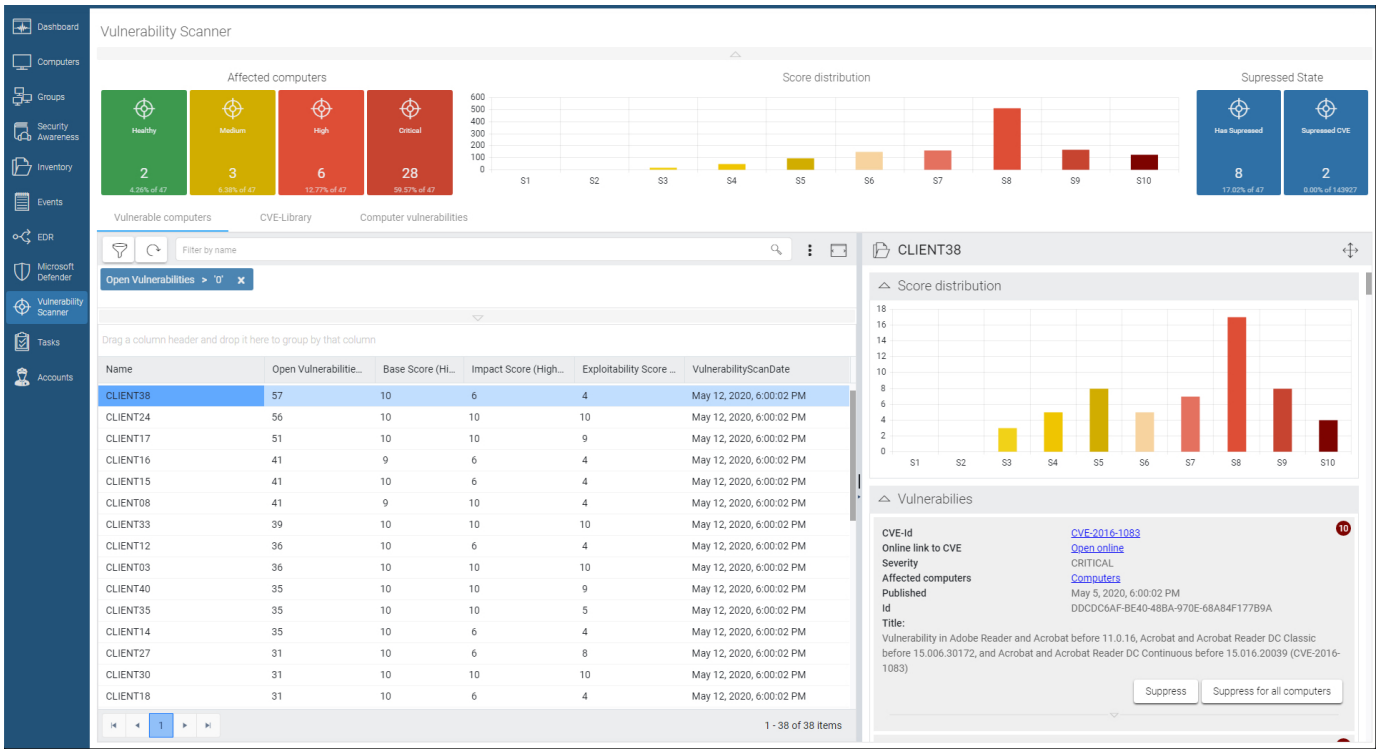
DriveLock
securing your digital tomorrow

Features

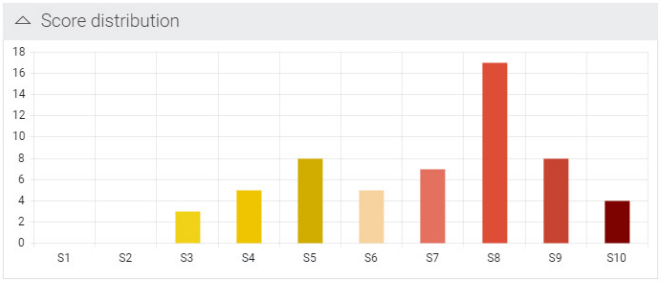
- Comprehensive vulnerability database with 115000 definitions for a total of approx. 140,000 CVEs
- Provides insights by continuous monitoring
- Determine if a vulnerability is exploitable
- Provides an overview of all vulnerabilities with different scores on the endpoints
- Triggers scans automatically, scheduled, or manually
- Suppresses vulnerabilities that are not of interest
- Newly created Dashboard, widgets, and specific view in the DriveLock Operations Center
- Hourly update of the internal threat database
- Follows NIST's standard by utilising SCAP and detected CVEs with CVSS scores
- Runs under Windows 10, 8, 7 and Windows server
- Multi-tenancy, multi-user and role-based access

Monitoring & Reports

Thanks to the DriveLock vulnerability database, the agent detects vulnerabilities on the endpoints and prevents malware attacks on the endpoints. IT administrators can identify and control the risks associated with vulnerabilities. The results found are displayed in a separate view in the DriveLock Operations Center. The vulnerability scanner finds missing patches, outdated software programs, or libraries with known vulnerabilities. The used database and individual vulnerabilities are managed and updated by the National Institute of Standards and Technology (NIST) and US-CERT. It assesses according to severity, probability of occurrence and impact. The DriveLock Operations Center displays all information and provides filters, groupings, and even reports. This allows a much more detailed and, above all, more accurate assessment of the security posture in your company.



Vulnerabilities that are not relevant to your company or found to be acceptable can be suppressed. This is an important function so that analysts can focus on the relevant threats. Views show the total number of found vulnerabilities on all devices in your environment and classifies the severity of the vulnerabilities as low, medium, high, and critical in the Vulnerability Statistics pane. By clicking on a pane, it drills down to the appropriate endpoints and lists more details.



- **Identify weaknesses in your environment**
- **Assess how critically the weaknesses are**
- **Quick high-level look at possible vulnerabilities**

You gain insight into the security posture of your company in almost real time and provide detailed information about weaknesses. With DriveLock, vulnerability management is a simple daily routine. Vulnerability dashboards provide details categorised by severity or type, age, and affected endpoints. They provide the possible severity levels and ratings as well as a description of the current vulnerabilities and their remediation.

These are the individual reports we can provide:

Environment vulnerability state

- Distribution of vulnerability scores
- Detailed information about a single computer
- Detected vulnerabilities, Scan date and state...
- Detected vulnerability and vulnerability Information
- Scan coverage

Detected CVEs with CVSS scores

- Base/Exploitability/Impact metrics

Reporting configuration

- Suppress CVEs that cannot be patched
- Suppress CVEs on single computers

Compliance reports

- Vulnerability Management Overview
- State changes over time
- Vulnerability trending and threat level over time

Vulnerability statistics - Total Number of Vulnerabilities

Shows the total number of vulnerabilities on all devices in the network and classifies the severity of the vulnerabilities as low, medium, high, and critical in the Vulnerability Statistics pane.

Vulnerabilities Based on CVSS

Prioritisation of remediation can be done only if there is visibility into the category of the vulnerability. DriveLock uses the Common Vulnerability Scoring System (CVSS), which determines the severity of the vulnerability based on principal characteristics that are translated into a numerical score.

Recently Discovered Vulnerabilities

This shows vulnerabilities that have been recently discovered. Show all vulnerabilities or CVEs that have recently become known but have not yet been discovered on any endpoint.

Vulnerability Aging

This shows vulnerabilities grouped by the number of days since they were detected and that have not been fixed.

Top Vulnerabilities

This shows top vulnerable assets by their CVE ID, and the number of devices at risk.

Vulnerable Assets

Determine top vulnerable devices and software assets. This displays the software assets installed on systems in the organisation and the risk associated according to their level of vulnerability. Click an asset name to see the details of the affected endpoint.

Vulnerable Endpoints

Shows the total number of vulnerabilities that a host has, and the severity rating by which they are grouped.

Vulnerability trending and Threat level over time

Shows the timeline of vulnerabilities on endpoints and their severity. Administrators can see if they are moving in the right direction.

Written by Andreas Fuchs, Director Product Management 2020-07

Contact us!

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

www.drivelock.com