BlackstoneOne.
peace of mind

Vulnerability scans and AI-powered Vulnerability Management

The Product Sheet includes
The importance of Vulnerability scans
BlackstoneOne's vulnerability solution through Vulnerability Management

Contact Phone: +45 70 209 209
Email: sales@blackstoneone.net

Valid from
December 2023

BlackstoneOne.
peace of mind

The importance of Cyber Security

Have you implemented an IT infrastructure in your company or organization? If so, you should focus on quickly determining whether you are at risk of data leakage or exploitation due to known vulnerabilities.

At BlackstoneOne, we offer vulnerability scannings which identify any existing security vulnerabilities in your network or system. It is a proactive measure used to detect any weaknesses that an attacker may exploit to gain unauthorised access to a system or network.
BlackstoneOne vulnerability scannings are automated and includes scans for known vulnerabilities, analysing the configuration of your system and network, and using an automated tool to detect any possible vulnerabilities.

Are you the next victim of a cyber crime?

Organizations of all sizes depend upon a more diverse set of technologies than ever before. With the advancement of technology, the global cyber security landscape has seen increased threats in recent years. In 2020, malware attacks increased 358% compared to 2019.
From here, cyber attacks globally increased by 125% through 2021, and increasing volumes of cyber attacks continued to threaten businesses in 2022. This is a significant record, causing major issues for businesses worldwide. The growing number of cyber attacks has also led to a series of extensive regulations regarding cyber security, imposing greater requirements on the businesses and organizations.

The increased cyber risks aswell as the regulations in the area have the protection and documentation of your digital infrastructure more important than ever. Therefore, it is necessary to take action to protect valuable and sensitive data in your organization.

Our costumers range from small and highly specialized businesses to large private and public organizations. We offer a platform that proactively, consistently, and continuously scans your system and network, notifying you when new vulnerabilities emerge. The platform provides you with a quick and comprehensive overview of your vulnerabilities and directs you to the necessary measures and solutions, allowing you to minimize risks within or around your IT systems.

Our expertise in navigating the complexity of implementing hybrid environments and employing the latest technologies for securing digital networks means, that you don't have to build deep skills in IT security in your organization. We ensure that your digital infrastructure is built on a strong and secure foundation, reducing the complexity of the identified vulnerabilities.

50%

of the municipalities in Denmark use BlackstoneOne

The engine room of your business must be ensured in order for it to function

At BlackstoneOne, we scan the engine rooms that form the foundation of your business. Through automated Vulnerability Management we ensure an efficient process around your identified vulnerabilities. Vulnerability Management is relevant due the increased cyber risks but is also relevant as it is required in various regulatory contexts, including:

NIS2 & DORA

The NIS2 Directive is an updated version of the existing NIS Directive, aiming to ensure that legislation for cyber and IT security in Europe follow the digital developments. The sectors affected by the NIS2 requirements appear here. Vulnerability scans can be a way for organizations and businesses to meet and document the minimum requirements of NIS2. The DORA Directive is a sector-specific regulation that applies to entities within the financial sector. DORA encompasses "tools necessary to duly and effectively protect all relevant physical components and infrastructure, including computer hardware, servers, as well as all relevant premises, data centers, and sensitive designated areas [...]" (Article 5(2)). The DORA Directive indirectly mandates vulnerability scans according to Articles 21 and 22. The requirements in NIS2 and DORA aim to ensure a high, common level of cyber and information security across all EU member states. Vulnerability Management is a crucial part of both directives as it helps organizations identify and address threats to their systems and data.

NB.
NIS2, DORA and GDPR only apply to companies in EU. However, many non-EU countries are making changes in its existing cyber security laws, such as adding managed service providers to the scope of the NIS regulations.

GDPR

GDPR is the General Data Protection Regulation. A law that applies to all businesses and organizations in the EU concerning the protection of personal data. GDPR requires that data controllers in organizations ensure compliance with the law, and therefore, data controllers must incorporate data protection into everything conducted within the organization or company.
Vulnerability Management is a crucial part of complying with GDPR, as it assists organizations in identifying and protecting personal data from threats and vulnerabilities in systems that process such data.

NSIS

NSIS (National Standard for Assurance Levels of Identities) is The Danish implementation of the common European Identity standard eIDAS (electronic IDentification, Authentication, and trust Services). The purpose of the standard is to establish a common framework for trust in digital identities and digital identity services through a set of technical and organizational requirements. Vulnerability Management is a crucial part of NSIS, as it assists organizations involved in a trust chain in protecting their IT systems and data from cyber threats. Therefore, NSIS plays a part in identity solutions such as MitID and NemLog-in, as well as various decentralized solutions like organizations with a Local IdP.

Know what's exposed.
Fix what matters.

The Danish Data Protection Agency recommends conducting vulnerability scans regularly in order to prevent cyber attacks. Therefore, it is not sufficient to do vulnerability scans only 2-4 times a year. BlackstoneOne keeps track of your attack surface, showing where and how your company may be vulnerable, prioritizing issues and filtering noise so you can fix the problems that matter most. Your digital infrastructure is automatically scanned monthly, and we offer 'Automatic Frequency Prioritization,' increasing the scan frequency automatically on vulnerable IP's and landing pages (URL) in your infrastructure.
Automated scans imply:

HIGH-RISK

Devices with high-risk vulnerabilities will be scanned at least daily.

MEDIUM-RISK

Devices with medium-risk vulnerabilities will be scanned at least every four day.

LOW-RISK

Devices with low-risk vulnerabilities will be scanned at least weekly.

Secure your attack surface without the complexity

To maintain a strong security level, it is crucial that you regularly scan all your active devices. Therefore, we automatically perform a monthly host discovery in your digital infrastructure, ensuring that all active devices are included in the ongoing scanning analyses, both newly identified and previously registered devices. Hence, we provide a continuously updated and accurate overview of the current vulnerabilities found on the scanned devices in your infrastructure. Our results are generated based on multiple scanning processes and technologies, providing a comprehensive and focused overview.

> BlackstoneOne caught things, where I do not dare to think about how bad it could have gone.
>
> /Project Manager at Nyborg Forsyning & Service, Kaj Andersen

Why choose BlackstoneOne?

Reduces cyberthreats
An overview strengthens your IT-security and thereby reduces risks related to vulnerabilities in your IT infrastructure.

Timesaving
You save both time and resources, which can be spent on other value-creating tasks.

Supports compliance
Supports compliance with requirements, including GDPR and NIS2, with regular vulnerability scans in the organization.

Developed by us
We own, develop and maintain the platform ourselfs, why we offer easy and quick access to our support to ensure security.

Regular scans
BlackstoneOne vulnerability scans are conducted regularly as new vulnerabilities emerge on an ongoing basis.

Economically beneficial
In addition to saving resources and time, the platform is undemanding. The simplicity of the platform means that you do not have to recruit, train and retain employees with deep IT technical security skills.

Attention to the essentials
BlackstoneOne scans automatically screen IP's if they are detected on a URL scan. Therefore, the same vulnerable device does not appear several times.

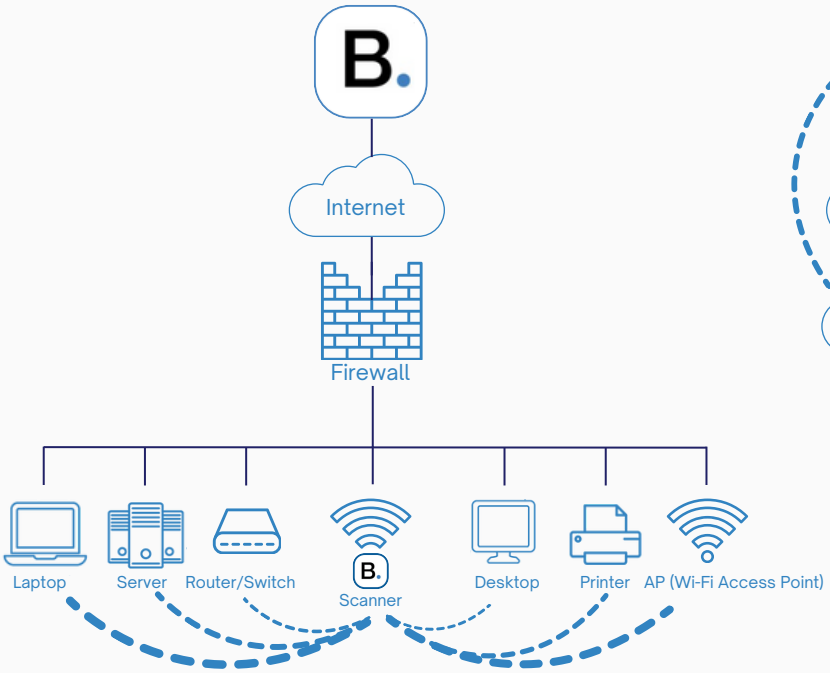
AI-enhanced communication: From lack of competence to skills development

We have developed a tangible and user-friendly AI assistant in our platform, helping you understand and manage the complex vulnerabilities found in an accessible way.
The AI assistant work as a co-pilot, scanning numerous sources for information and providing optimal descriptions and guidance to address vulnerabilities tailored to the specific IT-environment where the vulnerability is found. This enables a more precise and efficient resolution process.
With the AI assistant it is moreover possible to translate, making it easy to convey vulnerability descriptions and solutions to relevant system owners in the organization.
A relevant feature that the AI assistant implies is that you can search for information about specific vulnerabilities found in your network without revealing which company you are searching on behalf of. When using our AI assistant, you do not draw attention to the vulnerabilities in your infrastructure. Thus, the AI assistant works as a proxy to obtain specific information about your vulnerabilities.

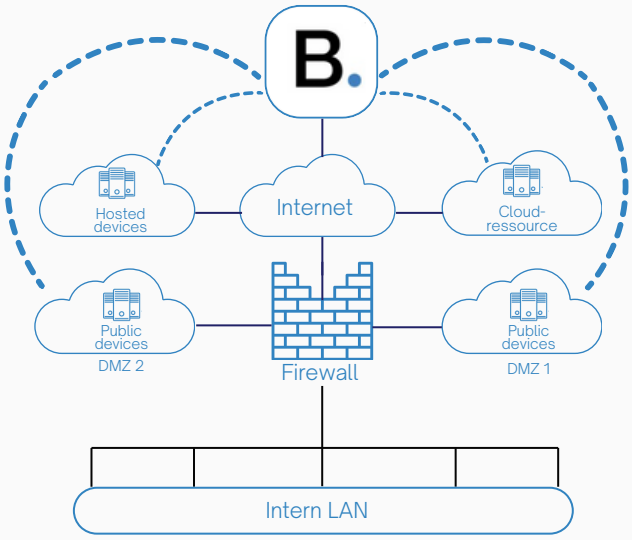
We help you understanding your vulnerabulities

Vulnerability scans by BlackstoneOne uncover known vulnerabilities and misconfigurations on internal and external networks, including servers, network devices, printers, web servers, and applications.

Internal vulnerability scan



External vulnerability scan



An internal vulnerability scan is conducted through one or more scanners placed in your infrastructure. The scans uncover vulnerabilities exposed on your internal network, including internal servers, clients, printers, IP's, network devices, and web applications.

An external vulnerability scan focuses on the organization's external infrastructure, such as web servers and customer portals, including internet-facing IP'S, websites and landing pages. External vulnerability scanning is typically performed with knowledge of the organization's IP's, URL's and any whitelisting that may prevent blocking.

NB.
Some servers can be accessed both internally and externally, why it is important to scan both internally and externally.

The identified vulnerabilities are accessed through the BlackstoneOne portal, where detailed descriptions of the vulnerabilities is avaliable. This can be issues related to the lack of patching on the operating system, installed third-party software, or recommended configuration adjustments.

Our mission and core values

An up-to-date overview

With BlackstoneOne, you get an updated overview of your vulnerabilities.

User-friendly

BlackstoneOne is a time-saving and intuitive solution, that focus on user-friendliness and does not require technical expertise.

User-managed

With BlackstoneOne, you ensure that each user receives the right information.

User-influenced

We highly value user input and continually evolve based on our customers' needs and preferences.

Book a demo and learn more at: www.blackstoneone.net

BlackstoneOne.
peace of mind