HADRIAN

How exposure management reduces risks on the edge

A modern solution for protecting organizations' most important assets.

The edge isn't defined anymore

More assets exist on the perimeter than ever before

In today's fast-paced world, businesses are compelled to adopt digital transformation to stay competitive. The benefits of digital transformation are significant and far-reaching:

- **Improved customer experience** – By leveraging technologies such as mobile apps, social media, and chatbots, businesses can create personalized interactions with their customers.
- **Increased efficiency and productivity** – Digital tools have automated manual processes, reducing errors and improving accuracy. This frees up employees to focus on more value-added tasks such as innovation and business development.
- **Greater agility and flexibility** – On-demand cloud applications have helped organizations quickly scale their operations up or down. And, remote working tools enable employees to work more effectively.

By embracing digital transformation, organizations have been able to stay ahead of the curve, adapt to changing market conditions and take advantage of emerging opportunities. However, digital transformation activities have blurred organizations' security perimeter. With more employees, customers and 3rd party applications accessing enterprise infrastructure risk management have become increasingly challenging.

40%

of firms will take a cloud-native-first strategy in 2023 as they look to increase agility and efficiency while reducing costs according to Forrester's 2022 Infrastructure Cloud Survey.(1)

24%

more workers chose to work remotely in 2022 compared to 2021.(2)

87%

of senior executives, as reported by Gartner in 2021, identified digital transformation as a top priority for their organization.(3)

Threat actors are exploiting the new edge

Attacks are increasingly targeting exposed assets

Digital transformation also brings new risks and challenges, particularly in terms of cybersecurity. Cybercriminals and threat actors are quick to exploit vulnerabilities in digital infrastructure, resulting in data breaches, financial losses, and reputational damage for organizations.

In the rush to adopt new technologies and stay ahead of the competition, security considerations are often overlooked. Cloud computing, IoT devices, and mobile applications among other have led to an expanded attack surface for threat actors to exploit.

> There is the perception that organizations focus their security efforts around their traditional “known” environments. This creates an incentive for threat actors as they are more likely to find an exposed asset on the internet that they can exploit.
>
> **Olivier Beg - Head of Hacking at Hadrian**

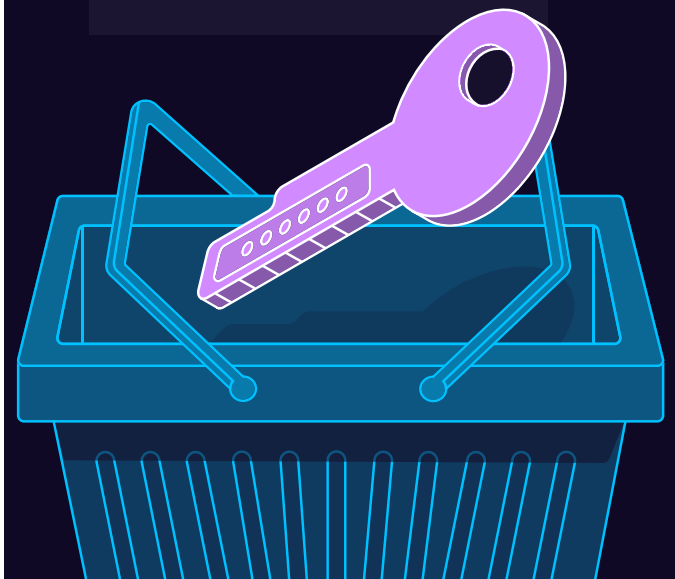
Organizations should focus on the benefits of digital transformation and address the risks and threats that come with it. Threat actors exploit this lack of security considerations by targeting vulnerabilities in new technologies and exploiting them to gain access to sensitive data.

69%

of organizations have experienced an attack targeting an unknown, unmanaged, or poorly managed external-facing asset.(4)

10/55

zero-day vulnerabilities exploited in 2022 involved internet-facing edge devices.(5)



How the threat landscape is being reshaped

Initial Access Brokers have very different incentives than traditional threat actors

Initial Access Brokers (IAB) are part of a growing trend of collaboration in the criminal underworld. Historically, ransomware gangs and other threat actors conducted all aspects of an attack themselves, from gaining access to a network to encrypting data and negotiating ransoms. However, this has changed with the rise of IABs. These attackers focus on gaining access to networks and then selling that access to other criminals.

IAB often have limited skill sets and are not able to develop malware or run sophisticated ransomware programs. They often make a profit by selling access to numerous organizations to other cybercriminals to use in attacks.

The arrangement is also beneficial to ransomware gangs and other advanced persistent threat groups which have often been bottlenecked by the number of systems they can hack into.

Instead of targeting specific industries or organizations, attacks by IAB are comparatively indiscriminate. They often utilize known vulnerabilities and search for any vulnerable asset on an organization's edge that they can exploit. As IABs become established it is expected that ransomware gangs will be able to attack increasing numbers of organizations.

25,059

CVE records were published in 2022, an increase of approximately 25% in 2021.(6)

15 minutes

after a CVE announcement, threat actors begin scanning the internet, according to research.(7)

Existing processes can't keep up

Traditional vulnerability management programs are no longer fit for purpose

The principle of vulnerability management is simple: organizations prioritize vulnerabilities based on their severity and the level of risk they pose. However, as shown, the number of breaches that utilize vulnerabilities still occurs at high rates. Vulnerability management programs generally struggle for three reasons:

- **Poor visibility** – In order for vulnerability management programs to work organizations need to know what their attack surface is. However, according to Forrester, on average organizations have an attack surface 30% larger than they knew they had.
- **Ineffective discovery** – Identifying vulnerabilities is in the attack surface has two challenges; the first is identifying as many of them as possible, as any that are missed could result in a breach. The second is minimizing the number of false positives, which slow teams down and prevent them from remediating the real risks.
- **Inaccurate prioritization** – Many organizations fail to prioritize vulnerabilities and instead focus on remediating vulnerabilities based on their age or contextless scoring such as CVSS. This approach can result in critical risks being left unaddressed, which can lead to security breaches.

56%

of large companies handle 1,000+ security alerts each day.(8)

66%

of security teams say that it is difficult to protect complex and dynamically changing attack surfaces.(9)

68%

of all cyberattacks exploit vulnerabilities that have had a patch available for over a year.(10)

A modern approach to a modern problem

Introducing Continuous Threat Exposure Management

Continuous Threat Exposure Management (CTEM) is the ongoing monitoring and identifying threats, vulnerabilities, and risks in real-time. It enables organizations to identify and respond to threats quickly, reducing the risk of a successful attack.

> By 2026, organizations prioritizing their security investments based on a continuous exposure management programme will be three times less likely to suffer from a breach.
>
> **Gartner**

How you reduce risk is unique to your organization, however CTEM provides the architecture to address the challenges you face:

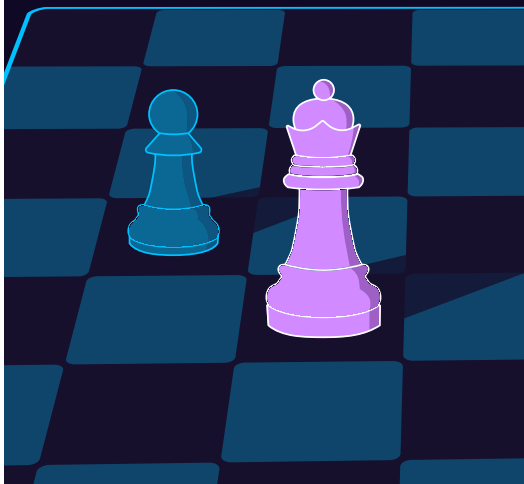
- Minimizing the number of security incidents that organizations currently face.
- Creating safe environments in constantly changing environments.
- Identifying the weak points in your security posture that an attack could utilize.
- Reducing the risk created by the technology that supports remote workers.
- Moving critical business functions to 3rd party services or platforms.

87%

percent of senior executives prioritize digital transformation as an organizational priority, according to Gartner's report.(3)

85%

percent of senior executives prioritize digital transformation as an organizational priority, according to Gartner's report.(3)



Understanding Exposure Management

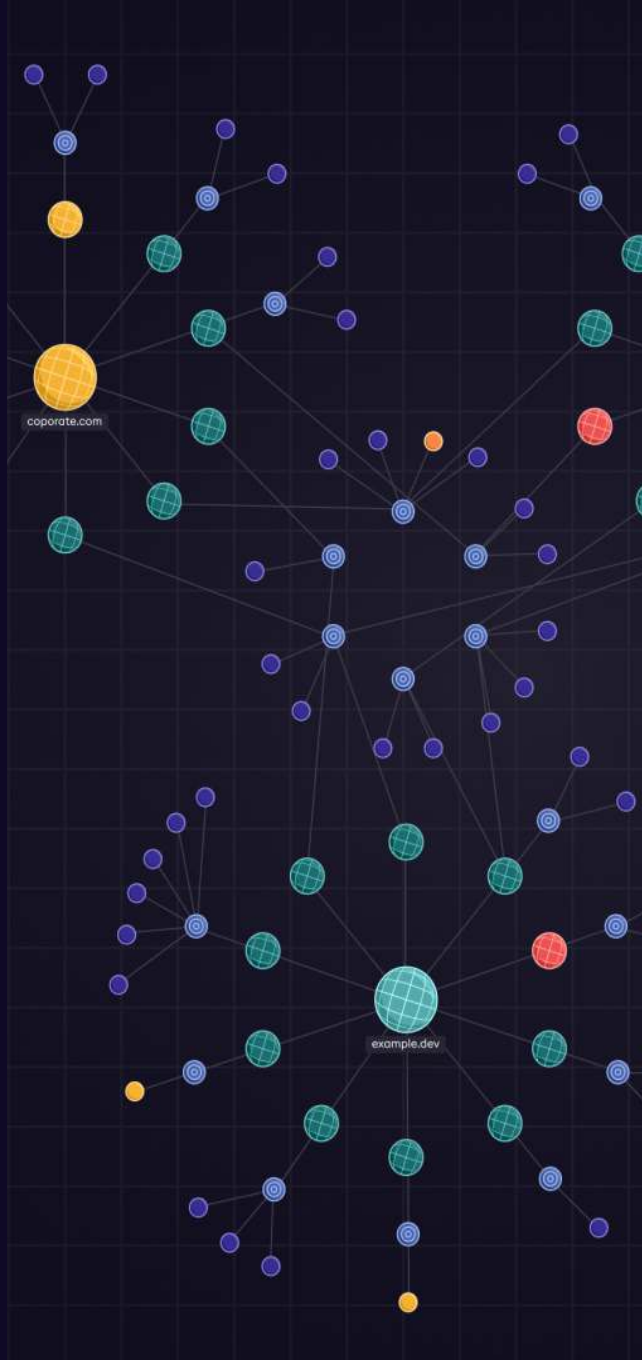
Delivering what vulnerability management can't

Exposurement management programs goes beyond vulnerability management in a number of ways:

- **Assessing security posture** by including the entirety of your organization's attack surface, not just known and manually cataloged assets.
- **Determining the likelihood and impact of exploitation** based the organization's entire environment, not just looking at risk in siloed cases.
- **Recommending remediation activities** for the wider organization to implement, not just the teams responsible for vulnerability patching.

In order to successfully implement an exposurement management program several capabilities are needed:

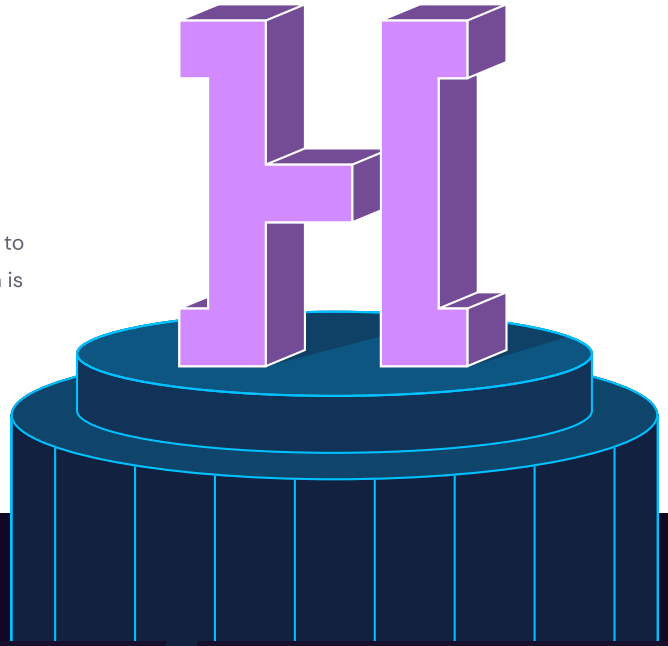
- Continuous external-facing asset discovery.
- Autonomous detection of exploitable risks.
- Accurate prioritization of the risks.
- Validation that the risks have been resolved.



The Orchestrator of Hadrian

Preventing breaches with exposure management

Hadrian's provides continuous coverage of the external exposure management lifecycle, to reduce risks, improve efficiency, and streamline compliance. At the heart of our platform is the Orchestrator, which conducts 24x7x365 analysis like a real-world adversary by dynamically chaining 200+ "hacker" modules together.



1

Assets

The Orchestrator discovers unknown assets by processing 1.1Tb of data daily to discover every asset belonging to your organization. To prevent unwanted surprises Orchestrator continuously scans for signs of new and changing assets.

2

Context

Hadrian's platform contextualizes your assets to understand how an adversary would conduct an attack. Hadrian fingerprints OS information, modules, libraries, input fields, authentication methods and much more during this stage.

3

Risks

The Orchestrator uses its knowledge of your environment to probe for weaknesses, learning as it goes and refining the techniques that it uses. Hadrian reliably identifies previously undiscovered risks to your organization with fewer false positives.

HADRIAN

Hadrian is a leading provider of External Attack Surface Management (EASM), Continuous Automated Red Teaming (CART), and Continuous Threat Exposure Management (CTEM) solutions. Our platform catalogs known and unknown assets wherever they are, investigates vulnerabilities by executing exploits like a threat actor, and prioritizes risks for fast remediation based on your unique environment.

Get a demo | Learn more

(1) Forrester, Infrastructure Cloud Survey (2022)
(2) Owl Labs, State of Remote Work (2022)
(3) Gartner, Speed Up Your Digital Business Transformation (2019)
(4) ESG, Security Hygiene and Posture Management (2022)
(5) Madiant, Move, Patch, Get Out the Way: 2022 Zero-Day Exploitation Continues at an Elevated Pace (2023)
(6) CVE, Metrics webage (accessed April 2023)
(7) Palo Alto, Incident Response Report (2022)
(8) Sumo Logic, State of SecOps and Automation (2020)
(9) Ponemon, The Cybersecurity Illusion: The Emperor Has No Clothes (2019)
(10) Abdalslam, Patch Management Statistics, Trends And Facts (2023)
(11) Cloud Native Computing Foundation, Cloud Native Security Microsurvey (2021)

Trusted by market leaders

BIOLANDES | CTC GLOBAL | beyond. | KCK

KINGSWAY CAPITAL | bank prov. | LEROY MERLIN | London Business School