

eBook

Diagnosing the Healthcare Attack Surface

The Power of a Continuous Offense

Get Started >



Introduction

Inside this eBook

Introduction

Common Attack Paths

The Consequences of an Exposed Attack Surface

The Power of a Continuous Approach for Shrinking an Attack Surface

How Chariot is Different

The digital landscape of the healthcare industry is under attack. Hackers are relentlessly targeting healthcare organizations, putting patient safety, sensitive data, and critical operations at increasing risk. Between 2010 and 2022, approximately 385 million patient records were exposed in cyber incidents, and in 2023, healthcare became the most targeted industry in the United States, accounting for over 20% of the nation's data breaches. Such incidents are an all-too-common headline and have the potential to cripple even the most well-resourced healthcare organizations.

At the heart of this cybersecurity crisis lies the healthcare industry's complex and expansive attack surface. The combination of legacy systems, IoT devices, virtual care platforms, mobile health applications, and an ecosystem of third-party vendors has expanded the boundaries of digital access and created a sprawling attack surface that is difficult for even the most seasoned IT and security teams to effectively manage.

In this ebook, we'll explore common attack paths found in healthcare organizations. More importantly, we will discuss how you can adopt a continuous threat exposure management approach (CTEM) to keep pace with your attack surface, shrink your risk exposure and meet critical regulatory compliance requirements, such as HIPAA, HiTRUST, and FDA regulations. By the end, you'll have a roadmap to proactively manage your attack surface, mitigate risks, and ensure the security of patient care.

1. Common Attack Paths

The healthcare industry is a prime target for cybercriminals due to the sheer value of the data it holds and the critical nature of the services it provides. From sensitive patient records to pharmaceutical intellectual property, healthcare systems are a goldmine for attackers. Some common attack paths exploited by attackers include:

Legacy Systems and Infrastructure

Healthcare providers often rely on well-tested and established systems to run all facets of their operation. Unfortunately, legacy and outdated software is far more susceptible to attacks due to the end-of-life nature and outdated security protocols. Compounded with an infrastructure often more than a decade old, these systems create an obvious entry point for cyber threats that can easily cripple an organization. Since 2009, 94% of healthcare organizations have experienced at least one cyberattack, many paralyzing operations. For example, in February 2024, a ransomware attack focused on patient billing swept the nation, compromising 85 million patient records and bringing hundreds of medical practices to the verge of bankruptcy. Ultimately, this attack affected over a fifth of the nation's economy.

Connected Medical Devices

An average hospital room houses 20 Internet of Medical Things (IoMT) devices. These devices range from simple pumps to complex lifesaving equipment, each offering a potential entry point for attackers. If successful, an attacker will cause critical malfunctions or seize the devices for ransom. As of 2024, 82% of healthcare organizations have experienced a cyberattack focused on IoT devices. Additionally, over 50% of medical devices in use have known critical vulnerabilities.

Virtual Care Platforms

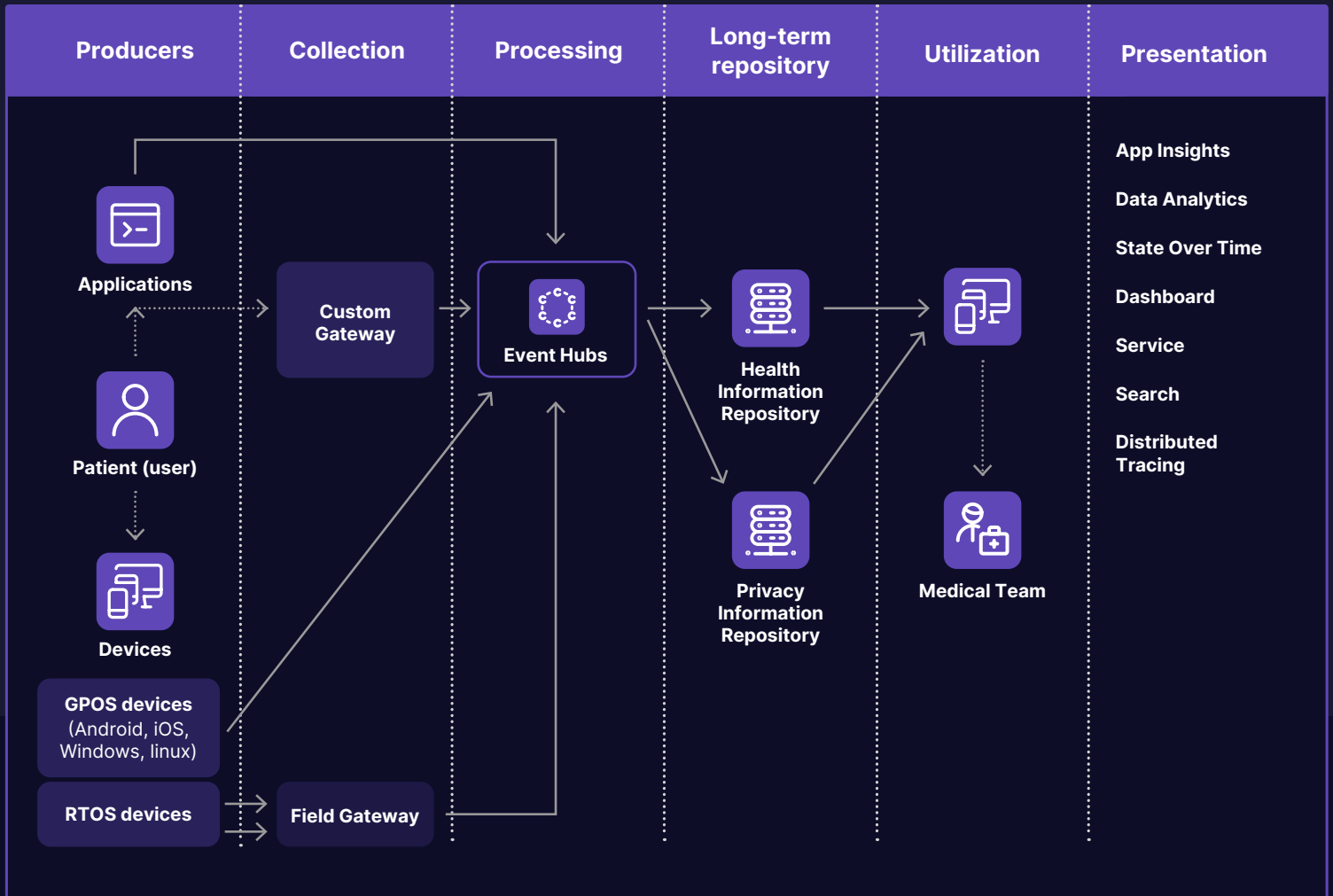
Virtual care surged in importance with the emergence of the COVID-19 pandemic, becoming a lifeline for patients. However, the rapid adoption of virtual care outpaced the implementation of security measures, leading to a 117% increase in malware incidents and offering adversaries countless new targets in video conferencing software, web portals, and the telehealth ecosystem.



94%

of healthcare
organizations have
experienced at least
one cyberattack

Telemedicine systems consist of two parts: the systems accessible to the patient and the backend system available only to the provider. The information flow between these systems broadens the attack surface, opening countless entry points for compromise, such as the patient’s (often poorly secured) home network. Below is a diagram which outlines the components and interaction flow of information.



Third and Fourth Party Vendor Ecosystem

Healthcare organizations are heavily reliant on third-party vendors for supply chain services and technologies. This collaboration makes the security posture of the organization dependent on the security posture of the vendor. Over the past two years, 98% of organizations worldwide integrated with a vendor who suffered a security breach. Furthermore, on average a healthcare organization has 200 fourth-party connections who have experienced a data breach.

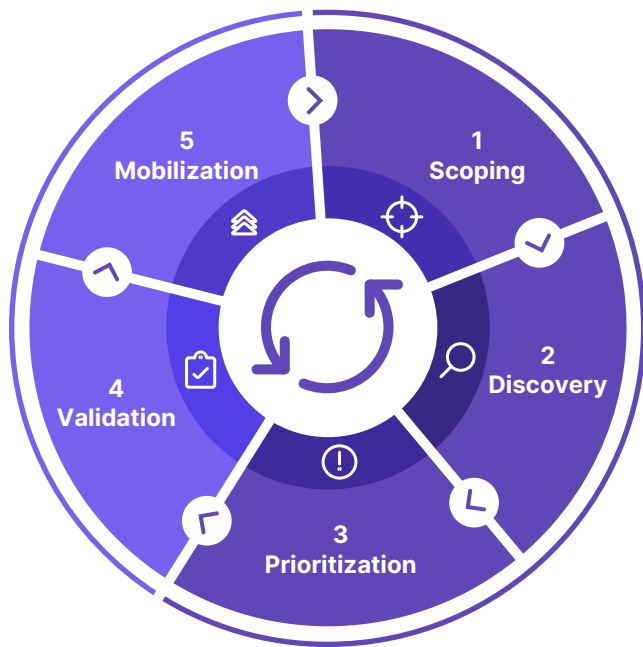
2. The Consequences of an Exposed Attack Surface

The consequences of an exposed healthcare attack surface can be severe, both in terms of financial impact and patient safety. In recent years we have witnessed countless real-world examples including ransomware attacks such as the May 2024 attack against Ascension Healthcare that crippled hospital operations, massive data breaches that compromised millions of records such as the Breach discovered by HCA Healthcare in July 2023, and insider threats that led to the theft of sensitive research.

These incidents illustrate the very real and severe consequences that arise from an inadequately secured healthcare attack surface. One in three Americans have been impacted by a health data breach in the past year, and the average cost of a breach to the healthcare organization is \$10.1 million.



One in three Americans have been impacted by a health data breach in the past year



3. The Power of a Continuous Approach for Shrinking an Attack Surface

To effectively manage their expansive and ever-changing attack surface, healthcare organizations are turning to continuous security programs, such as Continuous Threat Exposure Management (CTEM). Continuous programs overcome the challenges discussed above with a proactive, risk-based approach beyond traditional vulnerability scanning and penetration testing. Unlike point-in-time assessments, continuous testing enables an organization to fully understand the risk it faces from cyber threats at any given moment. To achieve this, CTEM programs use a five-step cycle: Scoping, Discovery, Prioritization, Validation, and Mobilization.

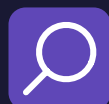


Scoping

The first step of a continuous security program is deciding what assets the program should test. There is a tradeoff between comprehensiveness and complexity: adding more asset categories increases both. We at Praetorian recommend starting with internet-facing assets in on-premises and cloud environments. As your program matures, you should add additional asset classes in the scope of testing. Some examples include:

- ✓ **Internal assets**
- ✓ **IoT devices**
- ✓ **BYOD devices**
- ✓ **Third-party SaaS platforms**
- ✓ **Source code repositories**
- ✓ **Vendor and partner assets**

Organizations should add assets to their program based on how important the assets are to the security posture of the organizations. Assets that provide direct access to an organization's crown jewels must be included from the start. Organizations can add remaining assets as their program matures. Threat modeling is a useful exercise to enumerate and prioritize all assets owned by an organization.



Discovery

After deciding what asset categories the program will include, the next step of CTEM turns those categories into an accurate mapping of the organization's attack surfaces. The discovery process is the beating heart of an effective CTEM program and deserve the most scrutiny. To achieve this, organizations need the ability to continuously discover and map their entire attack surface, including on-premises and web-based systems, cloud resources, connected medical devices, and third-party vendor connections. The map must change with the attack surface, making automated tools like Attack Surface Management or Vulnerability Scanners essential.

While a good detection tool is the core of an effective Discovery process, alone, it is not sufficient. Organizations must define and enforce processes around the tool to ensure it processes the correct inputs, returns high-quality outputs, and is easily fine-tuned. Without these processes, organizations will struggle with:

- ✓ **Lack of insight into dynamic attack surfaces, such as cloud environments**
- ✓ **Overwhelming numbers of false positives and alerts to triage**
- ✓ **Lag between the release of a novel vulnerability and an effective detection mechanism**

We address each of these sub-challenges in turn.



Dynamic Attack Surfaces

Dynamic Attack Surfaces are asset categories that change frequently, such as cloud environments, container orchestrators, and temporary subdomains. List-based approaches are infeasible to manage these surfaces. These surfaces move at the speed of automation. Therefore, the solution should respond in kind.

To manage Dynamic Attack Surfaces, organizations should build an automated integration for each surface, connecting that surface back to the discovery tool. For certain surfaces, this is a relatively simple process (e.g., teams can use a simple EventBridge rule in AWS environments to update the discovery tool every time a new machine comes on or offline). For others, this will require a custom, bespoke solution.

Integrations empower an organization to automatically keep pace with ever-changing attack surfaces.



Overwhelming False Positives

Because discovery tools rely primarily on automated techniques, developers must balance overreporting with missing vulnerabilities. Due to the critical nature of security, most vendors bias toward overreporting. While this approach reduces the risk of missing known vulnerabilities, it overwhelms the operators with an infeasible number of alerts to triage. Many security teams find their to-do lists growing longer each day as these alerts steal time away from other important tasks.

Managed Services can serve as a cost-effective means to augment your team and win back dozens of hours each week. Some ASM or Vulnerability Management vendors also offer their tool as a Managed Service, which allows you to “rent” engineers at the vendor company. These employees are highly trained in using their chosen tool, enabling them to triage efficiently and filter out all false positives.

Security teams may also look to Artificial Intelligence to screen out obvious false positive results. Whether added as a custom integration or embedded into the vendor’s platform, the AI feature will typically rely on an LLM to review each finding and silence false positives. LLMs have widely known limitations, such as hallucinations. As such, they are ideally situated to handle the lowest hanging fruit – stuff that is obviously wrong.



Discovery with Chariot

Praetorian's CTEM platform, Chariot, leverages all of the above techniques to uncover even the most obscure assets in your environment.



Prioritization

Not all threats are created equal. As your program begins to detect threats, your team must decide the order to process them. The prioritization criteria should be fully automatable, sortable, and filterable, making it possible to view your most pressing threats with one or two clicks.

As such, you may consider the following categories when prioritizing threats for triage:

- ✓ **Numerical risk rating (e.g., CVSS)**
- ✓ **Impacted assets**
- ✓ **Number of instances**
- ✓ **Exploitability (e.g., EPSS)**

Whatever metrics you choose, they should align with business objectives.



Validation

After you have a prioritized list of threats, your team needs a repeatable process to validate or triage each vulnerability. The validation process must:

1

Confirm if attackers can actually exploit the vulnerability

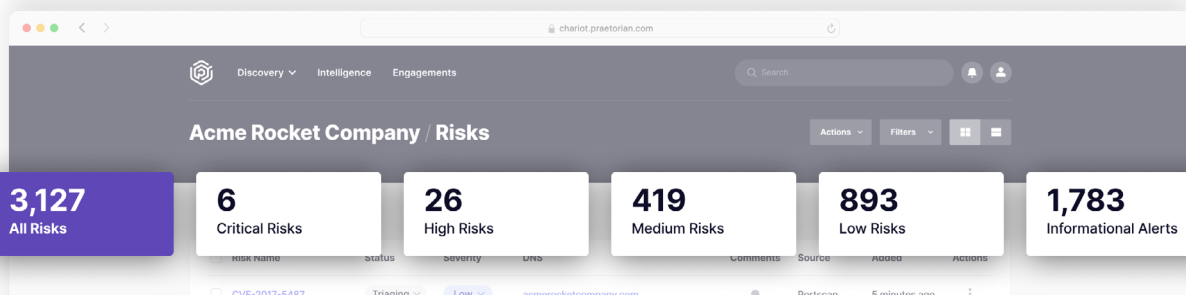
2

Determine what assets are at risk by exploiting the vulnerability

3

Investigate what compensating defensive controls exist and how they respond to a compromise

Based on the results from this investigation, the team will assign the triaged vulnerability a risk rating or mark it as a false positive. Organizations should create mappings for responses to the above tasks and various risk ratings.





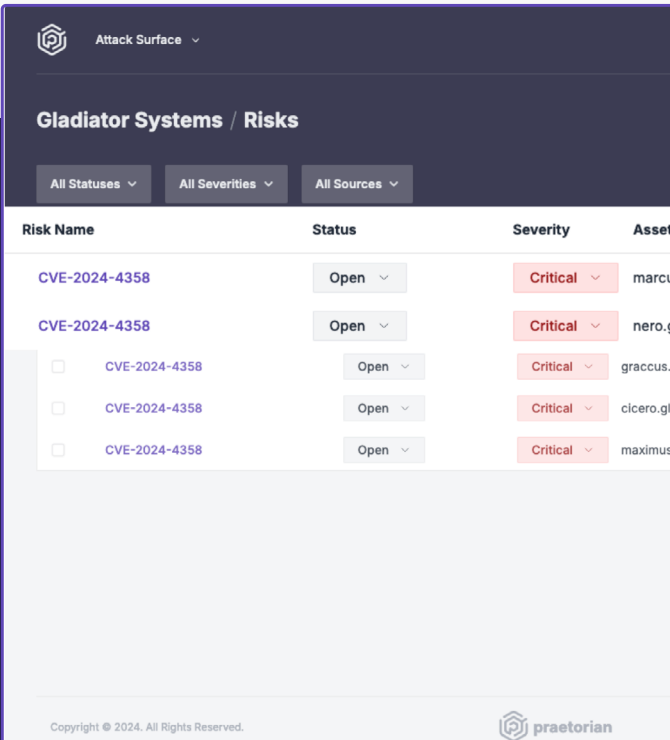
Mobilization

Mobilization is the process that occurs after you have identified a true positive that must be resolved. If you do not complete the mobilization step, everything completed up to this point is wasted effort. A good mobilization process details the steps necessary to remediate the vulnerability and ensure it remains remediated.

An organization's mobilization process should include procedures for:

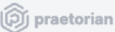
- ✓ **Identifying relevant stakeholders of affected assets.**
- ✓ **Agreeing on SLAs for remediation, based on risk rating.**
- ✓ **Determining follow-up process to ensure remediations are completed.**
- ✓ **Monitoring remediated assets to ensure regressions do not occur.**
- ✓ **Documenting all mobilization procedures in an easily accessible location.**

Where an organization can automate parts of its mobilization process, it should.



The screenshot shows the 'Attack Surface' interface for 'Gladiator Systems / Risks'. It features a table with columns for Risk Name, Status, Severity, and Asset. The table lists five entries for CVE-2024-4358, all with a status of 'Open' and a severity of 'Critical'. The assets listed are marcu, nero.g, graccus.ç, cicero.gla, and maximus.

Risk Name	Status	Severity	Asset
CVE-2024-4358	Open	Critical	marcu
CVE-2024-4358	Open	Critical	nero.g
<input type="checkbox"/> CVE-2024-4358	Open	Critical	graccus.ç
<input type="checkbox"/> CVE-2024-4358	Open	Critical	cicero.gla
<input type="checkbox"/> CVE-2024-4358	Open	Critical	maximus.

Copyright © 2024. All Rights Reserved. 

Proactive identification of Material Risk

Reducing your attack surface is an ongoing process, not a one-time event. To stay ahead of evolving threats, a managed offensive platform provides continuous monitoring to proactively identify and remediate vulnerabilities across your entire IT ecosystem. By adopting a continuously managed model, organizations strengthen their security posture by understanding severity of an exposure as well as the business context, allowing security teams to properly allocate resources, and meet continuous compliance requirements.

Take the next step to implementing a CTEM approach within your organization

Praetorian's Chariot platform is designed to embody the principles of CTEM, by combining people, process, and technology. Chariot incorporates attack surface management, vulnerability management, attack path mapping, breach and attack simulation, continuous penetration testing/red teaming, and exploit/threat intelligence into a single solution. These components, wrapped in a managed service, work in complete unison to provide unparalleled security coverage.

How Chariot is Different

1 We Consolidate and Save Money

We consolidate attack surface management, vulnerability management, continuous penetration testing, breach simulation, and exploit intelligence into a single cost-effective platform.

2 We Include Security Experts

Our team of offensive security experts provides continuous support, aligning your security strategy with best practices and emerging threats.

3 We Are All Signal and No Noise

We prioritize only critical and validated risks, ensuring you focus your time and resources on what truly matters.

4 We Give You The Ammo You Need

As an external third party, we help you obtain the buy-in from the business to fix the risks we uncover through demonstration of impact and hard evidence.

5 We Got Compliance Covered

Our tech-enabled service meets annual penetration test requirements, ensuring compliance and adding value to your security efforts.

6 We Verify Mitigation

We ensure identified risks are remediated and provide third-party validation, supporting your IT teams every step of the way.

Experience why the world's leading brands trust Praetorian

Contact Praetorian