HHS 405(d) HICP Segmentation with Elisity: Elevating Healthcare Network Security

Securing Healthcare's Digital Frontier: A Comprehensive Guide to Implementing 405(d) HICP Guidelines with Elisity

Introduction

Overview of Cybersecurity Challenges in Healthcare

The healthcare industry is a nexus of innovation and vulnerability. On one hand, advancements in medical technology have ushered in unprecedented capabilities for patient care. On the other hand, these very advancements make healthcare organizations attractive targets for cyber-attacks. From sensitive patient data to life-supporting medical devices, the stakes couldn't be higher. Cybersecurity isn't merely an IT concern; it's a patient safety issue.

Importance of 405(d) HICP Guidelines

Recognizing the urgency of this situation, the U.S. Department of Health and Human Services (HHS) introduced the Health Industry Cybersecurity Practices (HICP) under section 405(d) of the Cybersecurity Act. These guidelines serve as a blueprint for healthcare organizations, offering a structured approach to identify vulnerabilities and implement robust cybersecurity measures. More than a set of recommendations, the 405(d) HICP guidelines are a strategic framework designed to bolster the industry's cybersecurity posture. They emphasize the need for microsegmentation, policy

Related Content

HHS 405(d) HICP White Paper
Elisity Healthcare Demo Video
Securing Patient Care with Elisity

enforcement, and risk assessment—key components that translate into actionable steps for healthcare providers.

By aligning with the 405(d) HICP guidelines, healthcare organizations not only fortify their cybersecurity defenses but also demonstrate a commitment to regulatory compliance and, most importantly, patient safety.

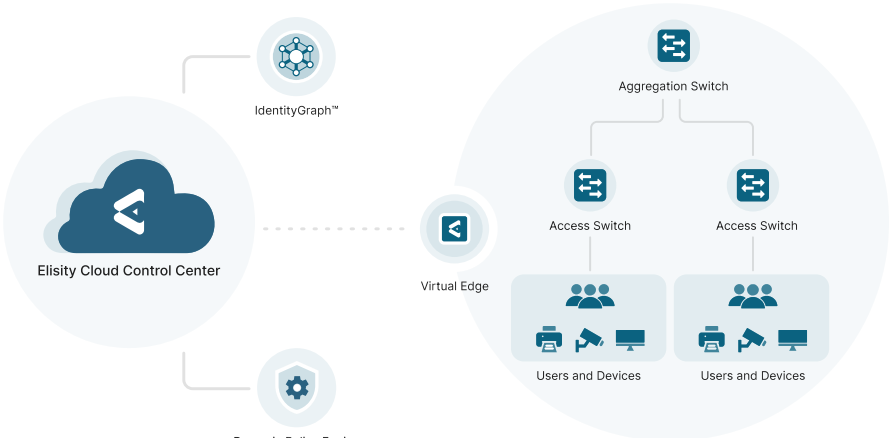
Related Content

HHS 405(d) HICP White Paper
Elisity Healthcare Demo Video
Securing Patient Care with Elisity

Elisity Platform Overview

Identity-Based Policy Enforcement

In an environment as dynamic and sensitive as healthcare, one-size-fits-all security solutions fall short. Enter Elisity: a platform engineered to bring identity-based policy enforcement to the forefront. By recognizing each user's unique identity and device interacting with the network, Elisity provides a nuanced, context-sensitive security layer known as the IdentityGraph™. This allows for granular control over who has access to what and under what conditions, elevating the organization's security measures to a new paradigm.



Integration with Existing Identity Providers

Understanding that healthcare organizations often operate within an intricate web of existing systems, Elisity is designed to integrate seamlessly with prevalent identity providers such as Active Directory. This interoperability ensures that user roles, already defined in these systems, can be directly mapped to policies within Elisity's platform. The result is a streamlined process that eliminates redundancy and minimizes the scope for error.

Through its intelligent design and integration capabilities, Elisity simplifies the complex task of securing a healthcare network. It acts as a bridge, linking existing infrastructures to cutting-edge security measures while adhering to the highest standards of compliance and operational efficiency.

Elisity: A Modern Solution for 405(d) Segmentation

User and Device Role Mapping

In healthcare settings, the roles of users and devices are fluid, often changing based on specific needs and tasks. Elisity's platform excels in recognizing this dynamic environment. It allows for real-time user and device role mapping, empowering organizations to enforce security policies that are as agile as their operations. Whether it's a nurse accessing patient records or a contractor calibrating medical equipment, the system ensures that each interaction is regulated according to its context.

Real-Time Policy Adjustments

Security is not a set-and-forget affair, especially in healthcare where situations can change rapidly. Elisity's platform is built to adapt in real-time. The moment a user's role changes or a new device is introduced to the network, policies adjust automatically to reflect this new state. This dynamic responsiveness is crucial in maintaining an uncompromised security posture without hindering operational efficiency.

Context-Sensitive Access Control

Understanding the 'why' and 'how' behind each network interaction is pivotal in implementing effective security measures. Elisity's platform offers context-sensitive access control, taking into account not just the 'who' but also the 'what' and 'where.' For instance, it can restrict a radiologist's access to specific imaging equipment or confine a maintenance contractor to a designated network segment. This level of granularity significantly reduces the attack surface, adding an extra layer of security.

Related Content

HHS 405(d) HICP White Paper
Elisity Healthcare Demo Video
Securing Patient Care with Elisity

By offering these advanced capabilities, Elisity transcends traditional security measures, bringing a level of sophistication and customization that is especially beneficial in healthcare settings. It equips organizations with the tools they need to not only defend against threats but also to adapt and evolve in a landscape that is constantly changing.

Related Content

HHS 405(d) HICP White Paper
Elisity Healthcare Demo Video
Securing Patient Care with Elisity

Alignment with 405(d) Guidelines

Microsegmentation

One of the cornerstone recommendations of the 405(d) HICP guidelines is the implementation of microsegmentation to isolate network components and restrict unauthorized access. Elisity's platform aligns perfectly with this directive. Its identity-based policy enforcement enables effective microsegmentation by assigning users and devices to specific network segments based on their roles. This not only restricts access to authorized personnel but also minimizes the potential impact of a security breach.

Policy Enforcement

The 405(d) guidelines stress the importance of robust policy enforcement mechanisms to mitigate risks. Elisity's real-time policy adjustments and context-sensitive access controls serve as practical solutions for enforcing these guidelines. The platform's ability to automatically adapt policies based on changing user roles and device interactions ensures that healthcare organizations are always in compliance with 405(d) recommendations.

Risk Assessment

Risk assessment is another key aspect of the 405(d) guidelines, advocating for continuous evaluation of vulnerabilities. Elisity's platform contributes to this by offering insights into user behavior and network interactions, thereby enabling healthcare organizations to assess risks proactively. This data-driven approach not only helps in identifying vulnerabilities but also aids in formulating targeted security measures.

By aligning its capabilities with the core tenets of the 405(d) HICP guidelines, Elisity offers a practical pathway for healthcare organizations to achieve both cybersecurity resilience and regulatory compliance. Its features map directly onto the guidelines, providing a cohesive and comprehensive approach to healthcare cybersecurity.

Related Content

HHS 405(d) HICP White Paper
Elisity Healthcare Demo Video
Securing Patient Care with Elisity

Case Study: Bupa Cromwell Hospital's Implementation of Elisity and Medigate

Healthcare institutions like Bupa's Cromwell Hospital are often at the forefront of cybersecurity, with a plethora of connected devices, highly sensitive patient data, and essential services. Medical devices like MRI and CT scanners often operate on legacy systems, making them challenging to protect with traditional IT security measures.

Bupa Cromwell Hospital, a state-of-the-art facility in London specializing in complex procedures and advanced care, was keen to improve its security posture against a new wave of threats, without disrupting operations. Bupa Group CISO Paul Haywood emphasized the company's dedication to patient data protection and its journey towards a cloud-dominant environment, which required effective management of policy and access.

Challenge

One of the significant challenges Bupa Cromwell Hospital faced was dealing with unmanaged devices, those without a software agent or additional IT control capabilities. These devices typically use old operating systems and cannot be patched or managed with traditional network security systems, making them preferred attack vectors for ransomware and other directed attacks.

Despite investing in a variety of solutions, the hospital struggled to gain deep visibility into the devices on its network and understand potential risks. They needed an all-encompassing view to quickly identify unmanaged devices and deploy policy without a substantial hardware refresh.

Solution

To address these challenges, Bupa Cromwell Hospital partnered with Elisity and Medigate to develop an advanced security solution for their infrastructure management. Elisity provided identity-based microsegmentation for the existing access layer switching infrastructure, requiring no additional hardware or network downtime. The Identity Graph by Elisity created context for effective security policy management by understanding users, devices, apps, and their relationships on the network.

Medigate, on the other hand, offered award-winning device discovery and risk assessment capabilities. By integrating these two platforms, the team identified policy gaps and developed microsegmentation and least privilege access policies mapped to device classes and user groups. This integration streamlined device identification, asset management, and ongoing policy maintenance while reducing the risk of security breaches for medical and IoT devices.

Outcomes

The Elisity and Medigate joint solution significantly benefited Bupa Cromwell Hospital. It delivered real-time visibility into medical devices, assessed vulnerabilities, and provided policy recommendations for efficient enforcement by Elisity. This streamlined policy management ensured a reliable approach to infrastructure management and protected patient information.

Cromwell Hospital CISO Alma Kucera reported that the implementation allowed them to manage traffic going into their medical devices and introduced layers of mitigation in defense and depth around the key risks identified.

According to Paul Haywood, Bupa's CISO, "In my 30 years of working in technology and security, I've never delivered a product into an environment and got instant benefit like we did with Elisity and Medigate."

This case study is an excellent example of how combining identity-based microsegmentation with device discovery and risk assessment capabilities can significantly improve healthcare organizations' cybersecurity posture, even in complex environments with a variety of connected and unmanaged devices.

Related Content

HHS 405(d) HICP White Paper
Elisity Healthcare Demo Video
Securing Patient Care with Elisity

Conclusion

In an era where cybersecurity threats are not just evolving but proliferating, healthcare organizations find themselves on the frontline of this digital battlefield. It's not just about protecting data; it's about safeguarding lives. Given this high-stakes scenario, the U.S. Department of Health and Human Services introduced the 405(d) HICP guidelines as a strategic framework for healthcare cybersecurity.

Elisity's platform emerges as a natural ally in this endeavor. With its focus on identity-based policy enforcement, real-time adaptability, and granular access controls, Elisity offers a comprehensive solution that addresses the unique challenges of healthcare cybersecurity. More importantly, its capabilities align perfectly with the 405(d) guidelines, providing a cohesive and practical approach to not just meeting but exceeding regulatory requirements.

But the ultimate measure of success is not just compliance; it's the enhancement of patient safety and trust. In this regard, Elisity doesn't just offer a platform; it offers peace of mind. By implementing Elisity, healthcare organizations are not just adopting a solution; they are making a commitment—a commitment to the highest standards of cybersecurity, operational efficiency, and patient care.

Related Content

HHS 405(d) HICP White Paper
Elisity Healthcare Demo Video
Securing Patient Care with Elisity