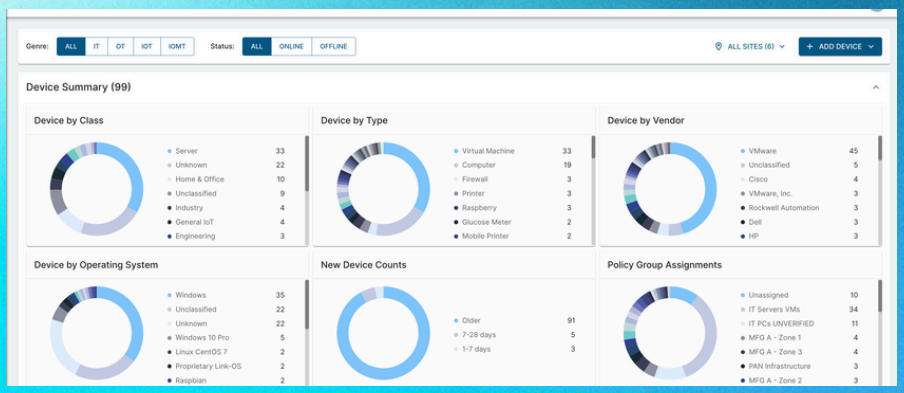
CROWDSTRIKE | ELISITY

ELISITY



Elisity and CrowdStrike Integration

Elisity offers a powerful integration with CrowdStrike's endpoint protection solution, CrowdStrike Falcon. With this integration, Elisity combines its expertise in network segmentation and identity-based access controls with CrowdStrike's in-depth endpoint security insights. This integration aims to refine cybersecurity measures, focusing on key areas such as asset verification, data enrichment within Elisity's IdentityGraph™, and the strategic use of CrowdStrike's Zero Trust Score to bolster access control.

The integration offers significant improvements in an organization's capability to manage and secure its network infrastructure. This creates a platform where informed decisions are made easier, thanks to the availability of comprehensive and actionable data from CrowdStrike. Let's explore the distinct advantages this integration brings, particularly how CrowdStrike intelligence can be seamlessly woven into Elisity's security framework to provide enhanced protection and smarter cybersecurity management.

Elisity-CrowdStrike Integration: Enhancing Cybersecurity Operations

At the core of this integration is the ingestion of CrowdStrike's rich endpoint data into IdentityGraph™. CrowdStrike gathers extensive data about device behavior, threat incidents, and overall endpoint health. When this data is brought into the Elisity platform, it serves two primary purposes: enhancing the capabilities of Elisity's Microsegmentation and enriching the data within the IdentityGraph™.

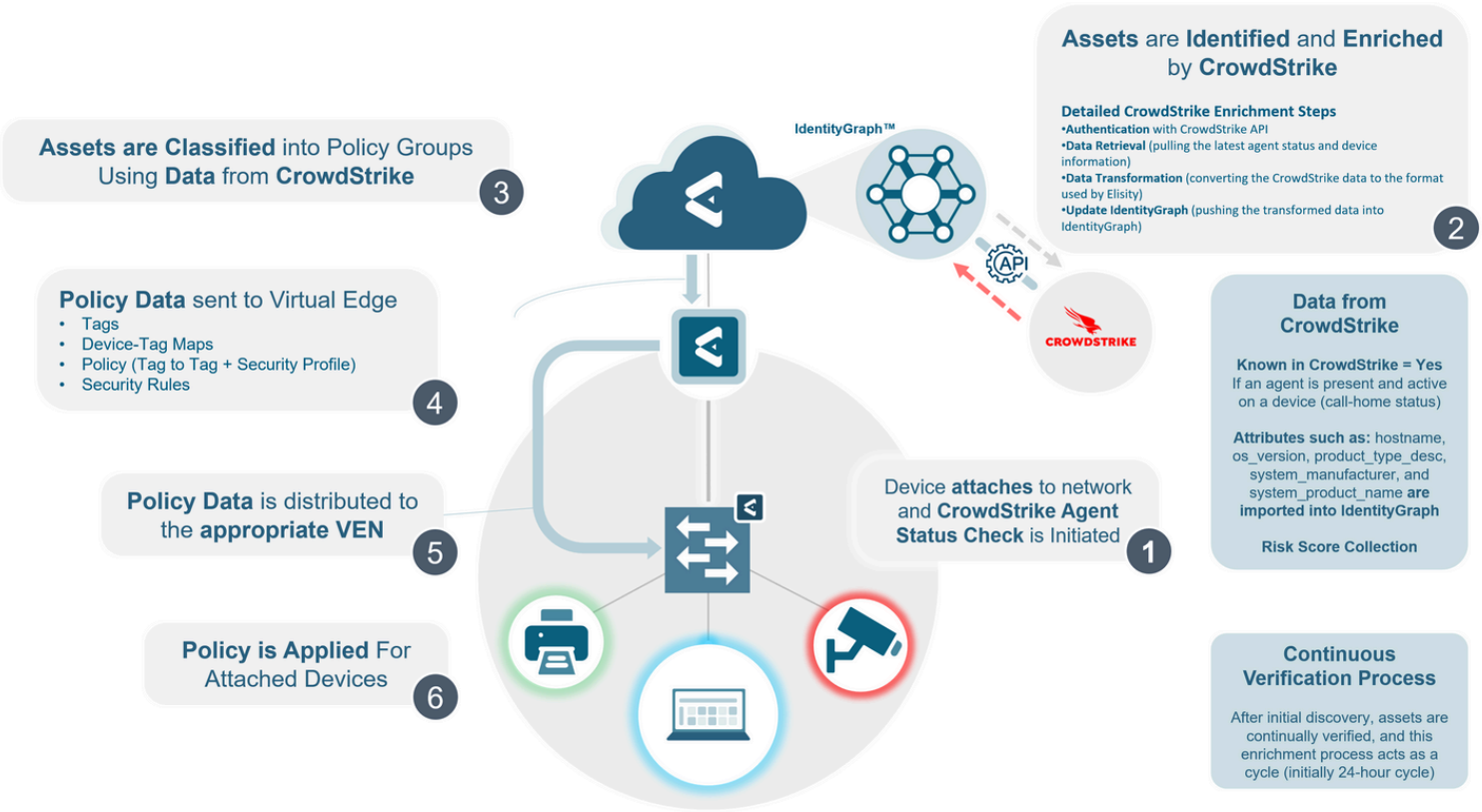
What does this mean practically? When a device attaches to your Elisity-secured network, we pull data from every available identity source into IdentityGraph™ where it can then be used as Policy Group match criteria. Policy Groups are then used as the endpoints for access policies in the Elisity framework. IdentityGraph™ automates this data aggregation for every asset on your network, enabling faster policy decision making and ultimately stronger policies. The more data you have about devices, the more confidently you can deploy least privilege access policies to those endpoints.

Microsegmentation Enhancement:

Elisity's Microsegmentation is designed to control access to network resources based on the identity of devices and users. By integrating CrowdStrike's data, Elisity can make more informed decisions about access control. This data provides additional context, allowing for more dynamic segmentation policies.

Enriching IdentityGraph™:

Elisity's IdentityGraph™ is a powerful tool for mapping the relationships and interactions between users, devices, and applications across a network. This enriched data helps in creating a more comprehensive picture of the network, leading to more accurate and effective policy decisions.

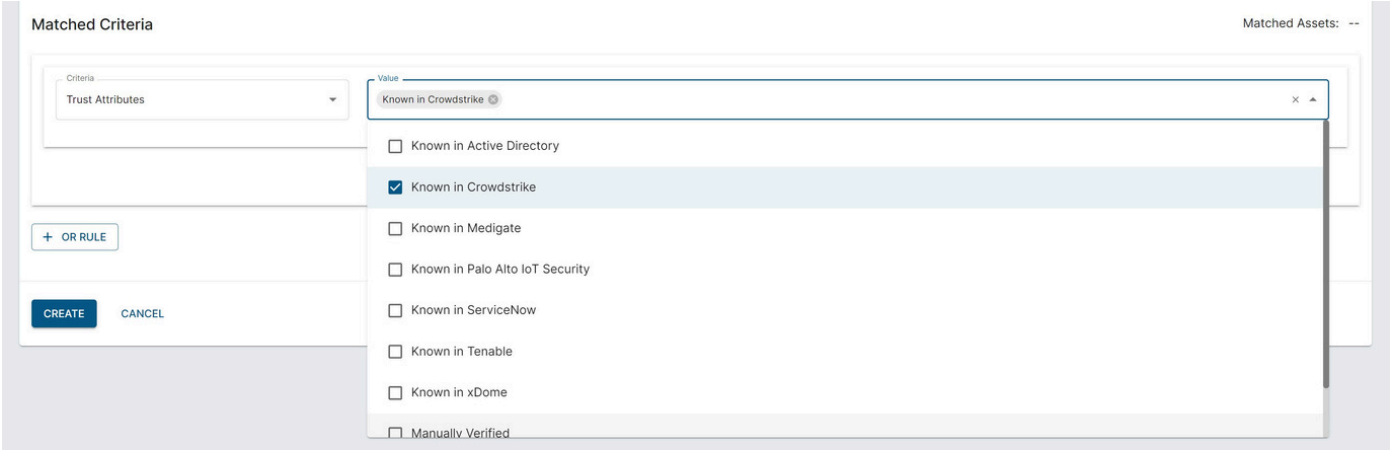


Key Use Cases of the Integration

The integration of CrowdStrike data into Elisity's Cloud Control Center brings several key use cases that significantly enhance cybersecurity operations. Let's explore these use cases and understand how they contribute to a more secure and intelligent network environment.

1. Asset Verification:

A critical aspect of network security is ensuring that only authorized and recognized assets have access. With CrowdStrike data integration, Elisity can now verify assets that are known within CrowdStrike directly in its environment. This verification process is vital because it allows Elisity to cross-reference the security status and history of an asset as reported by CrowdStrike, ensuring that only devices with a verified security posture can access network resources. This not only strengthens security by preventing unauthorized access but also ensures that network policies are applied to the right assets, reducing the risk of security breaches.

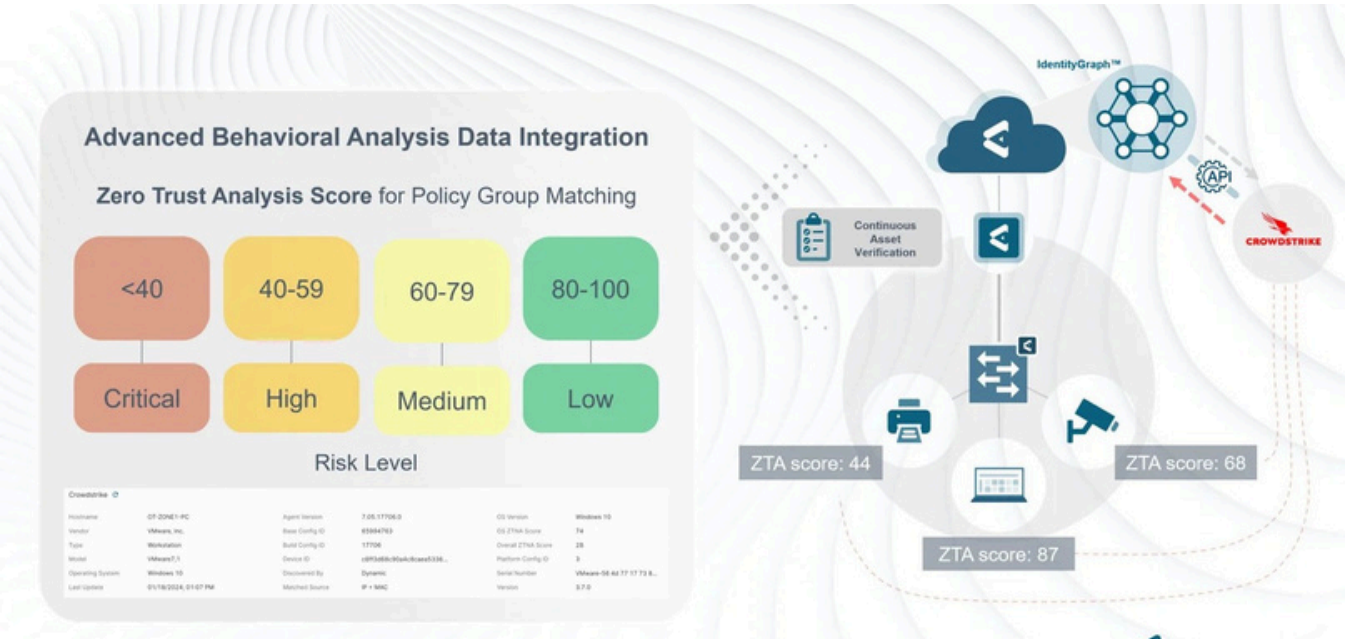


2.Data Enrichment for Discovered Devices:

Elisity's IdentityGraph™ is a dynamic tool that maps network interactions and relationships. By integrating CrowdStrike's data, the IdentityGraph™ is enriched with additional context about each device. This includes identity information about the device and the device's security status. Such enrichment provides a deeper understanding of the devices on the network, leading to more informed decisions regarding policy enforcement and access control. This enriched data helps Elisity tailor its security measures to the specific characteristics and risk profiles of each device, enhancing the overall effectiveness of the network's security posture.

3.Leveraging Zero Trust Score as a Trust Metric:

CrowdStrike's Zero Trust Score becomes an instrumental metric within Elisity's access control framework. This score, indicative of an asset's trustworthiness, can be used by Elisity in Phase 2 of our CrowdStrike integration to make real-time decisions about network access and policy enforcement. By utilizing this score, Elisity can dynamically adjust policies based on the evolving trustworthiness of a device, ensuring that network access is continuously aligned with the current risk level. This approach is crucial in a Zero Trust model, where trust levels are never static and need to be constantly reevaluated.



The integration of CrowdStrike data into Elisity's Cloud Control Center unlocks powerful capabilities for asset verification, data enrichment, trust assessment, and proactive threat management. These use cases collectively strengthen the security framework, ensuring a more secure, responsive, and intelligent approach to network security management.

Operational Benefits of CrowdStrike Integration

The integration of CrowdStrike data with Elisity's Cloud Control Center brings several operational benefits that directly impact the effectiveness and efficiency of cybersecurity operations. Let's discuss these benefits and their significance in a broader cybersecurity strategy.

Improved Accuracy in Threat Detection:

One of the most significant benefits is the enhanced accuracy in threat detection. By leveraging CrowdStrike's extensive threat intelligence and endpoint data, Elisity can identify and respond to potential threats with greater precision. This integration allows for more nuanced detection capabilities, moving beyond traditional signatures to behavior-based analytics. The result is a more proactive and preemptive approach to threat management, crucial in today's dynamic threat landscape.

Streamlined Security Operations:

Security operations become more streamlined and efficient with this integration. The process of correlating data and responding to incidents is significantly accelerated, as CrowdStrike's insights are directly available within Elisity's interface. This seamless flow of information reduces the need for manual data analysis and cross-referencing, allowing security teams to focus on strategic decision-making rather than routine data management tasks.

The Integration in a Broader Cybersecurity Strategy:

Incorporating CrowdStrike data into Elisity's Cloud Control Center is more than just an operational enhancement; it represents a strategic alignment in cybersecurity efforts. This integration ensures that endpoint intelligence and network segmentation work hand in hand, creating a more resilient defense against a wide range of cyber threats. It's an approach that acknowledges the complexity of modern networks and the sophistication of current cyber threats, offering a comprehensive solution to meet these challenges.

Conclusion:

The integration of CrowdStrike data into Elisity's Cloud Control Center offers a range of advantages that collectively enhance an organization's cybersecurity posture. From improving the accuracy of threat detection to streamlining security operations and ensuring dynamic policy compliance, this integration is a significant step forward in cybersecurity management. Organizations looking to maximize the value of their CrowdStrike investment and strengthen their overall security infrastructure will find this integration particularly beneficial.

Additional Resources:

For those interested in implementing this integration or seeking further information, a range of resources are available at elisity.com/knowledge. Detailed documentation on the setup and configuration can be found on Elisity's support portal, and further insights into optimizing the use of CrowdStrike data within the Elisity environment at https://support.elisity.com/hc/en-us