DATA SHEET

Terrain-based Proactive Cyber Defense

Intelligence-based Cyber Awareness for Contested Digital Environments

Understanding Your Environment is the First Step in Cyber Defense

Holistic visibility across your entire threat landscape is vital, particularly against modern adversaries. An adversary's ability to get in, lurk undetected, and study your environment directly impacts how well they can exploit your business.

That same visibility is equally — if not more — important when defending your environment. You can't protect what you can't see. To better safeguard your data and assets, you need to understand what you have, identify points of exposure or vulnerability, and proactively analyze critical areas to prioritize any security weakness.

Understanding is the first step in both offense (adversary) and defense (you).

What is cyber terrain and why should I worry about it?

Cyber terrain is the cumulative topography of an organization's IT infrastructure. It is comprised of all operational IT and data assets, network connections, and security controls.

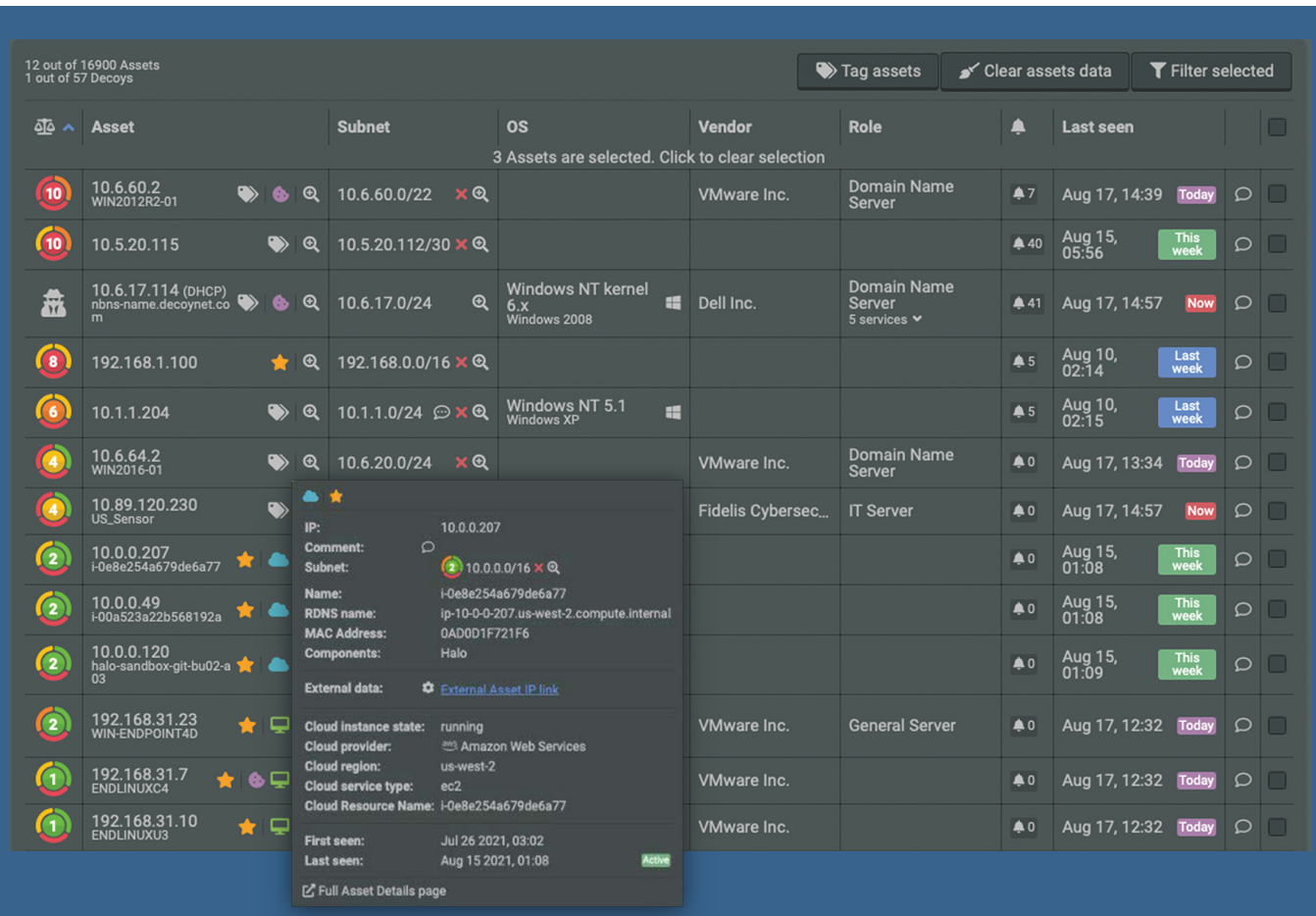
Cyber terrain mapping is essential in its influence of cyber decisions about operations, investments, and architecture to improve defensibility, resiliency, and security. It helps better identify your assets and assign value to each. But why is it important to know one's own terrain?

To reduce cyber security risk, the NIST Cybersecurity Framework recommends a number of actions. One of those requirements is "to identify, prioritize, and focus resources on the organization's high value assets (HVA) that require increased levels of protection—taking measures commensurate with the risk to such assets."

Cyber terrain mapping gives you insight into all of your IT assets, so you can identify those most critical to your operation.

Benefits of Fidelis Security Terrain-based Cyber Defense

- Discover on-premises assets using passive network monitoring. Extend visibility and terrain mapping across clouds with Fidelis Halo® discovery and inventory.
- Identify assets by role, operating system, connectivity, and more.
- Identify unmanaged assets on your networks (e.g., BYOD and IoT devices) to fortify and defend assets without endpoint protection and/or where it's not always possible or feasible to install EPP/EDR agents.
- Identify shadow IT that likely isn't properly secured by analyzing all traffic and cloud provisioning activities.
- Create a deception network based on a terrain map that enables decoys to be automatically installed, moved, and adapted as the terrain changes.
- Define and prioritize your most important assets to improve fortification and protection of the most critical assets.



Dynamic cyber terrain table based on automatic profile and classification of asset and services enables holistic visibility and

Fidelis Elevate – Terrain-based Proactive Cyber Defense

The Cyber Terrain Problem

When an adversary targets your enterprise, one of their first objectives is to map your environment. They will discover your assets, learn the asset's role in the organization, operating system, communication paths, installed software, vulnerabilities, users, and more.

Often, enterprise security teams don't fully understand the terrain that they're trying to defend. This is especially true in modern, dynamic, and distributed hybrid and multi-cloud environments. Instead, they rely on static network drawings and periodic asset inventories. That is a problem.

Particularly since the security perimiter is now dynamic — changing constantly as new cloud services are added and removed. Typically, cloud assets are controlled by product and project teams throughout the enterprise (otherwise referred to as Shadow IT since they were deployed outside of IT and security controls may not have been consistently applied). The result is a disparate view of cyber terrain that can't keep up with the rate of change throughout the enterprise. XaaS, shadow IT, BYOD, and IoT complicate the role of security professionals while introducing a wealth of attack surface opportunities for adversaries.

Cyber terrain describes the security battleground. Mapping cyber terrain in real-time enables security teams to better understand and protect the environment, to discover security weaknesses, and to fortify them before an adversary can exploit any vulnerability or misconfiguration.

The Cyber Terrain Solution

Fidelis Elevate is an active XDR platform. It provides deep, contextual data that enables advanced cyber terrain mapping across your entire environment. This also includes visibility across servers, endpoints, and cloud assets. This mapping provides a complete and continuous inventory and assessment of attacker movements and methods to more effectively thwart nefarious activities. It applies a risk analysis algorithm to help prioritize alerts and highlight potential weaknesses, and it presents assets within a communication map displaying open protocols and ports between computers, networks, and subnets. In doing so, Fidelis Elevate shifts security analysts to a more proactive approach that enables SOC teams to anticipate, detect and respond to threats faster.

Learn More about Fidelis Elevate

Cyber Terrain Mapping Using Fidelis Elevate

- Monitor all network traffic over all ports and all protocols to help identify and assign roles to endpoints based on observed communications.
- Discover all of your assets in the cloud and on-prem and identify the risk in a single source.
- Detect the operating system and role of the asset (e.g., Workstation, Web Server, File Server, Mail Server, Doman Name Server, IOT devices, and more)
- Monitor and manage assets detected within the environment. Active Directory integration provides knowledge of assets and users. EDR integrations provide additional details about assets where EDR is present.
- Review communication paths between your assets, including which ports and protocols are used, and subnet definitions.
- Understand the existence of an endpoint agent, vulnerabilities of installed software, and the vendor of the asset.
- Inventory and assess cloud assets discovered from Fidelis CloudPassage Halo.
- Update vulnerabilities when new software is detected and via daily updates to the Common Vulnerabilities and Exposures (CVE) database.
- Assign vulnerability information from supported common vulnerability scanners.
- Create uncertainty for attackers by automatically creating and modifying a decoy network to modify the terrain. Constantly changing environments make it difficult to distinguish real assets from decoys, allowing the defender to detect and investigate active attacks early in their life cycle.
- Take a multi-dimensional risk analysis approach to assets based on importance, available security coverage and threat score computed based on known vulnerabilities and alerts. Risk is computed for all assets, including those detected

Refer to the Fidelis Elevate Asset Risk Calculation datasheet for more information on mitigating risk with Active XDR via the Fidelis Elevate platform.

About Fidelis Security®

Fidelis Security® is the industry innovator in proactive cyber defense, safeguarding modern IT for global enterprises with proactive XDR and CNAPP platforms. Fidelis Security consolidates IT security operations to shrink attack surfaces, automate threat detection, and accelerate analysis, forensics, and response so that organizations remain resilient through cyber-attacks and emerge stronger and more secure. Fidelis Security is trusted by top commercial, enterprise, and government agencies worldwide.

Contact us to learn more

www.fidelissecurity.com/contact
or scan the QR Code