SOLUTION BRIEF

Trellix Helix for remote workers

Keeping an eye on VPN usage

Marco Van der Aar
Consulting Sales Engineer,
EMEA—Northern Europe

Introduction

Table of contents

Remote work has been necessary over the last couple years, and it looks like it's here to stay at many organizations. Virtual private network (VPN) technology can support organizations that are fully remote or adopting a hybrid model. For some, this means increasing capacity on their current solution, but for others this calls for deploying a completely new VPN solution. Given the urgency and the prime focus on availability, it's a challenge to guarantee all best practices are followed: strict access control, use of multifactor authentication (MFA), and a strict watch on VPN solution usage.

Obtaining legitimate VPN access is a tactic often used by adversaries for their initial access and for establishing a more permanent foothold in the target environment. Currently, espionage actors from China, North Korea, and Russia, as well as cybercriminals, are exploiting this attack vector in spear-phishing campaigns.

Trellix Helix detects and alerts your organization to any misuse of VPN, other suspicious traffic, or behavior from users connected to critical servers. With nearly 3,000 detection and correlation rules built in, combined with several advanced analytic engines to detect compromised VPN accounts, Helix is a turnkey cybersecurity solution designed to mitigate any risk involved with increased VPN usage.

Mitigating risk with Helix

Helix is a cloud-hosted security operations platform that allows your organization to take control of any incident from alert to fix. Available with any Trellix subscription solution, Helix integrates your security tools and augments them with advanced SIEM, orchestration, and threat intelligence capabilities to capture the untapped potential of security investments.

With Helix, you can:

- **Detect advanced threats** by correlating data from multiple tools and overlaying advanced behavioral analytics and intelligence
- **Minimize the impact of an incident** by accelerating response time with orchestration and automation
- **Expand visibility** by centralizing security data and infrastructure, whether on-premises or in the cloud

For monitoring VPN abuse specifically, a limited set of log data needs to be sent to the Helix platform. For each use case, the various steps to integrate solutions and absorb the relevant logs in Helix are described below.

As a start, a suitable Helix instance is needed. Obtain a Helix license for enough events per second (EPS) to cope with the expected number of events being sent to Helix. Trellix can assist by helping you choose which log sources are needed or advised and how many EPS they would typically use.

Integrate on-premises log sources

1. Go to the Trellix Market and select Helix in the filters section. This will show two versions of the Helix Communications Broker (Comm Broker), one for CentOS and one for Ubuntu. Each option also comes with a downloadable installation and configuration guide.
2. Following the manual instructions, install and connect Comm Broker to the Helix instance and verify connectivity from the Helix console. Configure Comm Broker to listen on the relevant port(s) for syslog and/or JSON-based logs.
3. From the VPN concentrator, enable sending logs to Comm Broker. Do the same for other critical assets where needed, like your MFA solution. For critical Microsoft Windows servers, you can send logs to Comm Broker using tools like NXLog.

Helix configuration

After your logs are configured, sign in to Helix and navigate to the operational dashboard. Verify there are EPS flowing in and monitor them over time to validate the actual EPS rate is within the purchased rate. While Helix does allow for short spikes, a sustained oversubscribed environment will start queueing logs, and at some point might cause logs to be dropped altogether.

To function properly, some rules and analytic engines need to be aware of the internal network being used. To set this up, navigate to the Configure – Lists section and find the Home Net list, where you can enter the local network ranges using CIDR format.

Rules and dashboards

Included with Helix are close to 3,000 out-of-the-box detection rules, combined into 50+ rule packs covering various risk areas. More than 150 dashboards are also provided, including 13 dashboards specific to Helix analytic engines. Using these dashboards, it's easy to track potential anomalies like incoming SSH or RDP connections, geo-infeasibility for remote user account usage, and many more.

Helix provides the option to easily create your own custom dashboard—either by building it yourself from the ground up or basing it on an existing dashboard—to provide what you think is relevant in a single view.

Integration in existing SIEM

If your organization already uses a SIEM, you can integrate alert data from Helix and send it to the SIEM solution. The Helix manual describes the process.

Appendix 1—What Helix does

We understand that every organization is unique and there will always be third-party components in the security infrastructure. So you can get the most out of your investments, Helix is equipped to integrate with many existing and often cumbersome security processes. In addition, Helix delivers a new, unified user experience across the Trellix product portfolio.

Detect what others miss. Helix combines Trellix Network Security, Endpoint Security, and Email Security – Server with the industry-leading Threat Intelligence Exchange.

Make other security products better. Helix applies threat intelligence rules and analytics to existing security and IT products. With broad support for hundreds of devices, any log source becomes more valuable.

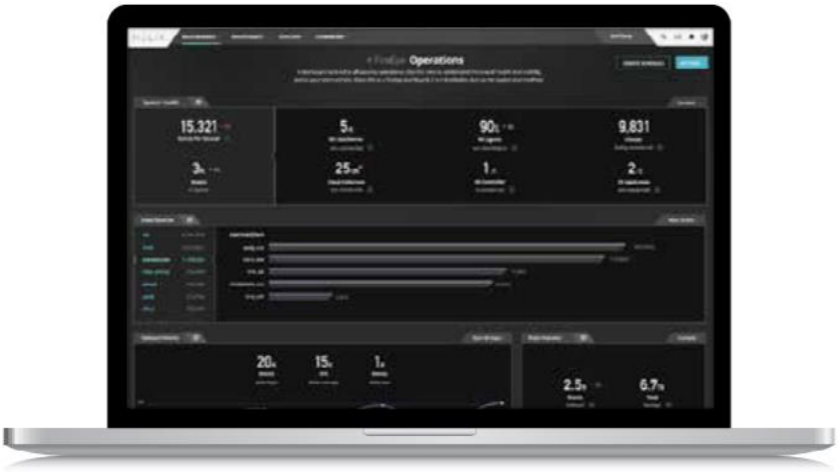

Figure 1. Operational interface for immediate situational awareness

Work faster from a unified console. Helix features a single console (see Figure 1) for each of the major SOC use cases such as alert management, search, analysis, rules, analytics, investigations,t and reporting. By offering a single console, Helix eliminates friction, providing minimal activity impact or zero impact for the security analysts.

Enhance your analytical capabilities. Helix powers the SOC with tools that emphasize response speed, including sub-second search across all events, context on alerts, simple pivot and analysis tools, and malware analysis reports on any hash.

Automate response. Helix orchestration lets SOC teams take advantage of predeveloped Trellix playbooks with best-practice response processes that you can run automatically based on a combination of events and alerts.

Improve your broad situational awareness. Helix reports and dashboards allow your organization to customize views and gain quick insights into any part of your environment.

Manage cases. Organize,collaborate, and assign action steps through the investigative process with automated and manual workflows.

Achieve compliance. Helix reports show auditors the data needed for compliance.

Appendix 2—Other features and benefits

Feature	What it does	Benefits
Investigative workbench	Facilitates all SOC functions from a single interface, including alert management, search, analysis, investigations, and reporting	Provides greater visibility into threat actors and their TTPs
Contextual intelligence	Infuses frontline intelligence and rules into existing alert and event data	Provides greater visibility into threat actors and their TTPs
Orchestration	Automates response with prebuilt and customizable playbooks created by frontline practitioners	Provides efficient security operation with fewer human errors
Security analytics	Provides context into who is targeting your organization and why	Detects and analyzes advanced threats through a combination of methods, including rules and applied threat intelligence
Guided investigations	Leads users through prepopulated investigative methods and a series of "next step" searches that provide useful context to the investigation for the responder to pursue	Upskills analysts and increases the effectiveness of incident responders
User and behavior analytics (UBA)	Detects non-malware-based attacks by analyzing various behavioral patterns	Consolidates alert volume and analyzes it to detect behavior anomalies, lateral movement, and compromised accounts
Compliance management	Allows you to retain and organize data for compliance reporting using prebuilt and customized dashboards	Simplifies your organization's reporting for compliance audits and prevents the risk of audit for non-compliance

To learn more about Trellix, visit: www.trellix.com.

Trellix
6220 American Center Drive
San Jose, CA 95002
www.trellix.com

About Trellix
Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers.