GET PCI COMPLIANCE-READY WITH COLORTOKENS

Whether your organization is primarily a brick-and-mortar business or has an online presence with e-commerce, achieving PCI compliance can be challenging. Cardholder data is processed and stored in many different places, from systems in data centers and cloud platforms to point of sale (POS) systems, PCs, and in-store kiosks. To avoid PCI violations, IT teams need to understand exactly where cardholder data flows, minimize access by users and applications, and scan their environments for vulnerabilities and unprotected paths to confidential data. In order to protect PII (personal identifiable information) processing and storage servers against vulnerabilities and streamline PCI compliance, enterprises need to:

- Accurately assess the scope of systems that process and store cardholder data
- Get a granular picture of the communication in and out of credit card processing servers
- Document all the users and applications that access cardholder data
- Restrict access to cardholder data on a business “need to know” basis
- Apply PCI rules in dynamic cloud environments where enterprises have little control
- Minimize the blast radius of an attack

A Unified Approach to Data Protection and Compliance

Achieving and maintaining compliance with PCI standards can be challenging for any organization, regardless of size or industry. And even businesses that do manage to meet PCI requirements may find audits expensive, time-consuming, and stressful. ColorTokens helps enterprises address these challenges by simplifying ongoing PCI compliance, identifying changes in compliance scope, reducing the audit scope and time to audit, and accelerating any needed remediation. Additionally, ColorTokens supports PCI cloud compliance, which can enable merchants and retailers to prepare for their cloud transformation without additional security or hardware requirements.

ColorTokens’ Xshield micro-segmentation solution can see, stop, and predict security and PCI compliance violations across any workload, any deployment, and any user. It delivers a unified approach for organizations to simplify security and compliance across their hybrid infrastructures.

To meet PCI guidelines, accurately scope the PCI audit, and accelerate remediation of audit failures, organizations must perform the following steps to gain comprehensive visibility and control over their cardholder data:

- **Discover all systems that process and store cardholder data**
- **Micro-segment and isolate cardholder data from unauthorized users and applications**
- **Prevent unpatched POS systems from propagating malware**
- **Ease the burden of proving compliance to auditors with out-of-the box reports and real-time network maps**

Visibility into Vulnerabilities that Expose Cardholder Data

ColorTokens' Xshield delivers comprehensive visibility, identity-based micro-segmentation, and cloud workload protection for application workloads running on premises and on cloud platforms. Based on an AI/ML policy engine, Xshield automatically tags each workload with information such as the application it belongs to, the platform it runs on (such as VMware, AWS, Azure, or Google Cloud), and whether it is part of a card processing environment. Xshield further creates a comprehensive network map of all workloads, workload connections, and connections to domains across the web. With this comprehensive map, you can see how application workloads interact and visualize their dependencies.

Xshield also identifies paths for lateral movement that advanced attacks can use to reach cardholder data. The vulnerability scanner highlights the most exposed systems in card processing environments, so you can prioritize monitoring them for vulnerabilities and indicators of attack. Xshield further simplifies internal firewall traffic audits, uncovers misconfigured ports, and highlights unauthorized connections that violate PCI and other regulations.

Micro-Segmentation to Isolate Cardholder Data

Xshield allows users to quickly visualize and discover the PCI environment, including every communication going in and out and whether that communication is blocked or unauthorized. This reduces the time necessary to create a network diagram to start PCI compliance from weeks to days. The data can be downloaded and queried to understand every flow in the environment, whether authorized, unauthorized, or blocked, to create comprehensive audit reports and meet the requirements of qualified security assesors (QSAs).

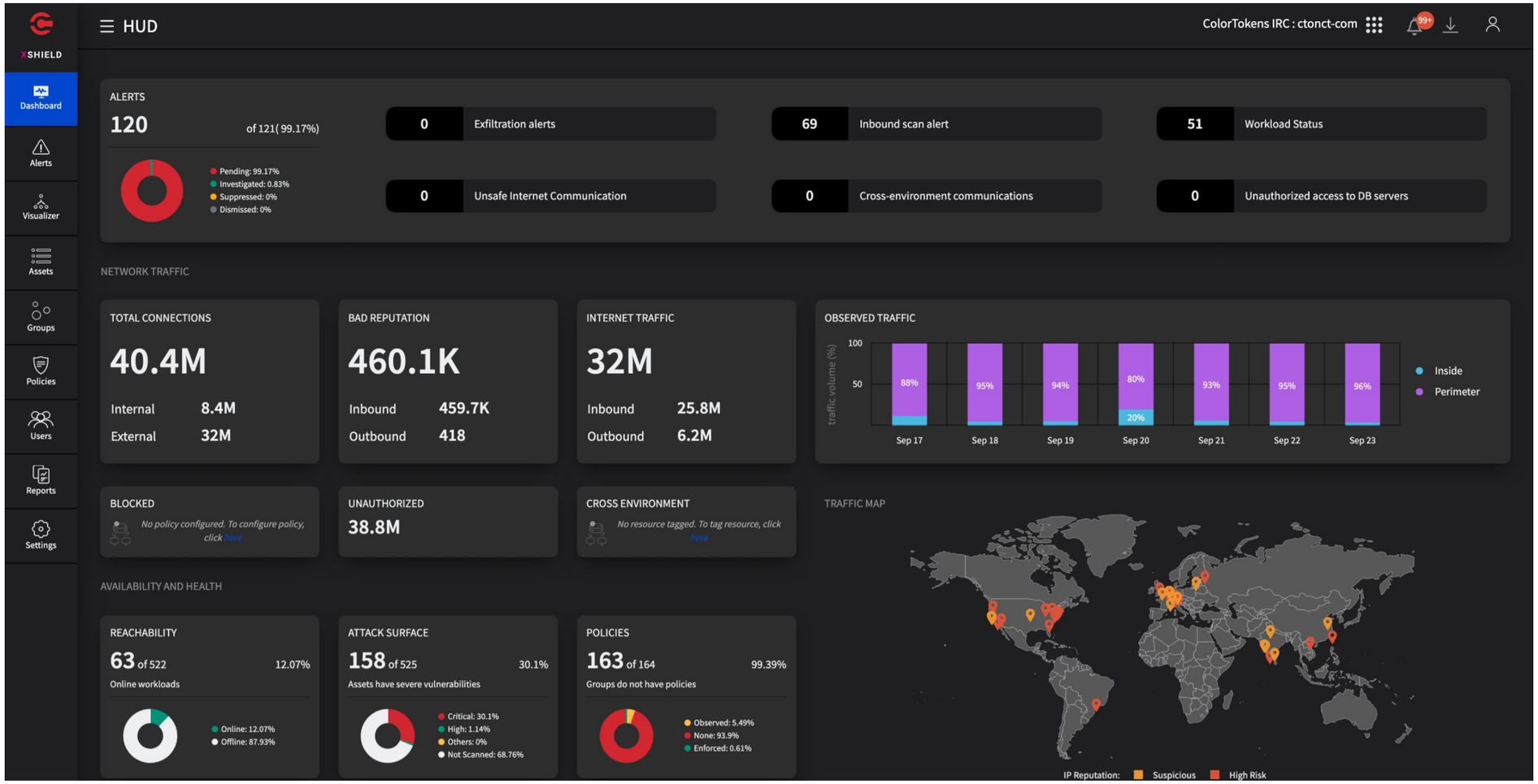

Figure 1. Unified display on the Xshield dashboard.

Xshield enables enterprises to isolate and protect cardholder data and processing systems by blocking traffic to and from unauthorized systems and users. It provides an automated and auditable process to create, monitor, and enforce policies that restrict access to each application workload to users and applications with a business “need to know” as defined by the PCI standards. The segmentation and isolation of the environment helps to minimize the scope of a PCI audit by half.

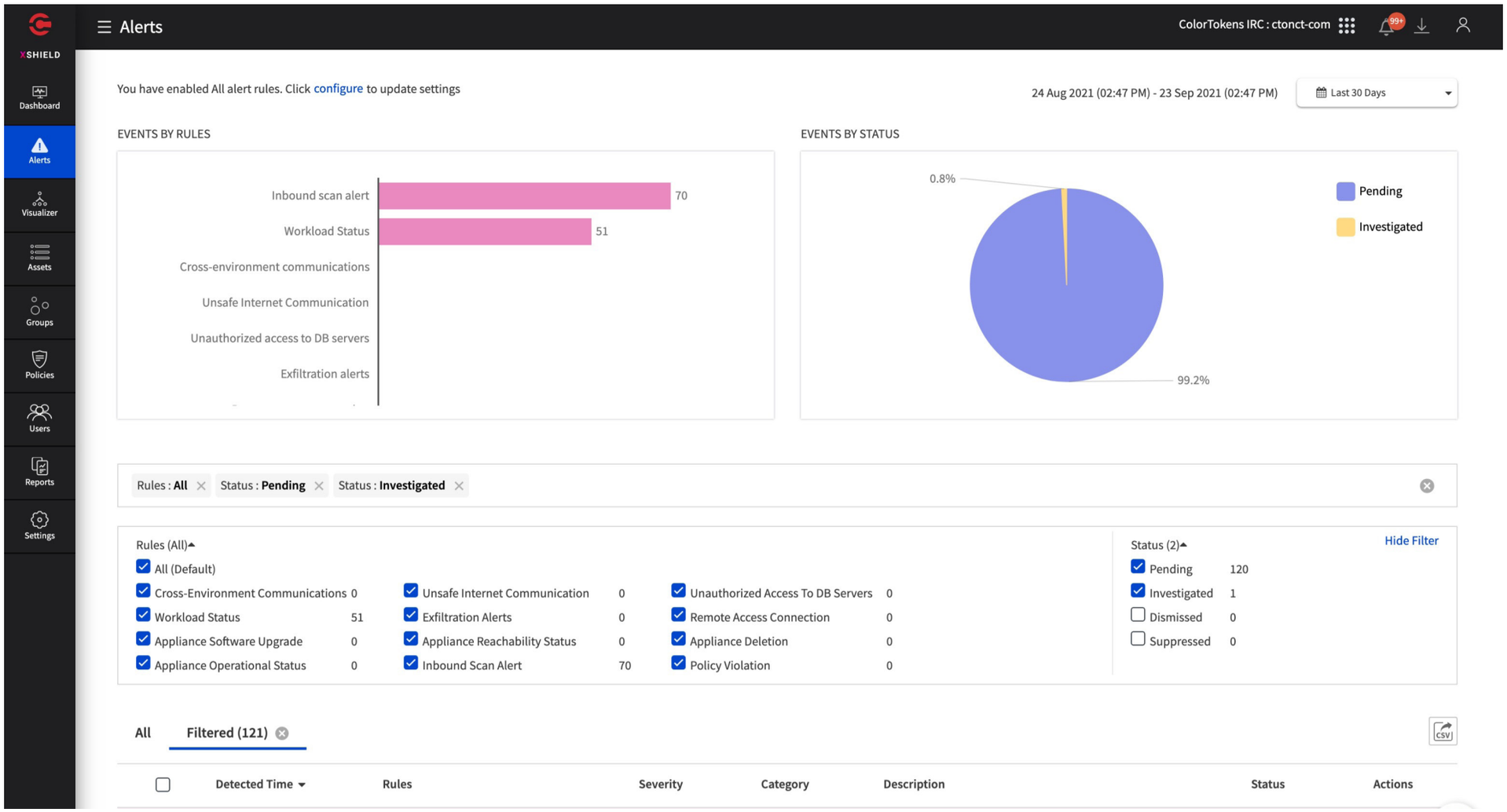

Figure 2. Network diagram on the Xshield dashboard.

Once policies are assigned to a workload, Xshield ensures that the policies follow the workload wherever it may reside, regardless of the underlying hardware or technology. When virtual environments move an instance of a workload, the security policies move with them. The effect of policies can be simulated and refined in a non-blocking “observe” mode, and deployed policies can be rolled back if necessary.

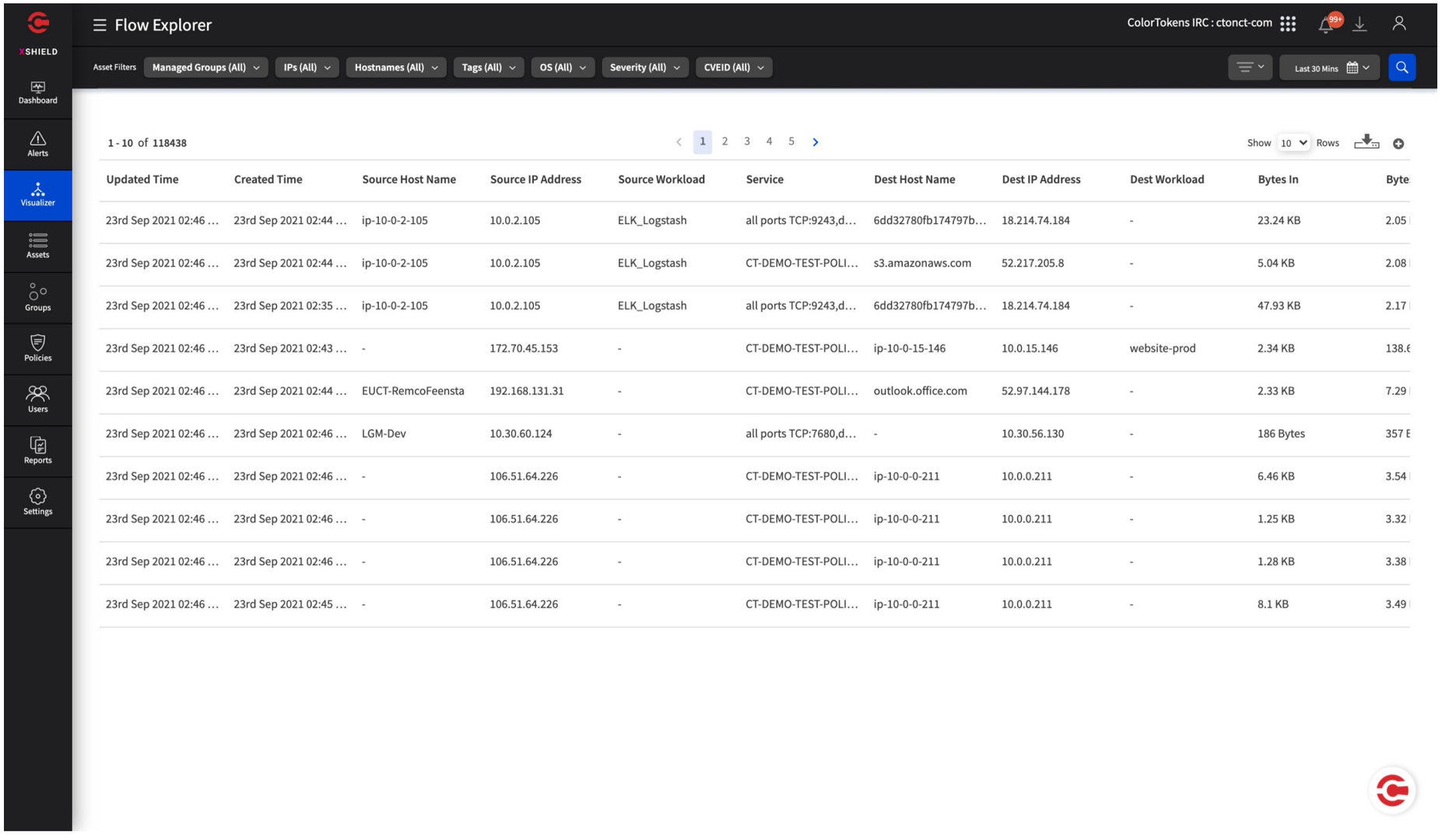

Figure 3. Traffic flow visualization on the Xshield dashboard.

When an audit is required, Xshield’s network traffic and policy violation logs give audit teams a comprehensive view from multiple firewalls in a single unified console, reducing the time to assess and compile the data for audit from weeks to hours.

Fast Track your PCI Compliance with ColorTokens

With ColorTokens Xshield, you can reap the benefits of enhanced security and a streamlined compliance audit. You'll be able to:

- Discover systems that process cardholder data in on-premises data centers and on cloud platforms
- Reduce risks by identifying paths for lateral movement into CDEs, exposed workloads, misconfigured ports, and unauthorized connections
- Implement micro-segmentation to isolate and protect cardholder data and processing environments
- Assign access policies to application workloads that enforce PCI requirements
- Reduce the burden of compliance by identifying PCI compliance scope changes and narrowing the scope of audits
- Create a faster picture of the PCI environment, shortening the time to create a network map from weeks to days

ColorTokens Inc. is a leading innovator in SaaS-based Zero Trust cybersecurity solutions providing global enterprises with a unique set of products and services for securing applications, data, and users across cloud and hybrid environments. Through its award-winning Xtended ZeroTrust™ Platform and context-aware machine learning-powered technologies, ColorTokens helps businesses accurately assess and improve their security posture dynamically.

As cloud adoption grows, traditional perimeters get redefined, and new attack vectors and threat actors materialize, corporations recognize their security posture needs to reflect their Zero Trust philosophy. ColorTokens' technology allows customers to achieve Zero Trust by utilizing rich, meaningful contextual information about the application, microservice, or protected resource, so customers can apply Zero Trust with as secure of a perimeter as they can. ColorTokens' cloud-based SaaS platform can automatically deploy next-generation security controls and increase security posture dynamically without any new hardware, downtime, reboots, or changes to a client's existing systems.

With a team of over 400 people, ColorTokens has global office locations in Santa Clara, California; New York; London; Copenhagen, Denmark; and Bengaluru, India. For more information, please visit **www.colortokens.com.**