COLORTOKENS

USE CASE BRIEF

RANSOMWARE - PREVENT LATERAL MOVEMENT

Ransomware is malware designed to encrypt data files and hold them unusable to demand ransom. These attacks can take seconds to damage your valuable infrastructure systems and data. If not contained, ransomware causes irreparable economic and brand damage to organizations regardless of size or industry. Ransomware targets business processes essential for delivering critical manufacturing, healthcare, utility, retail, and financial services.

Ransomware has become highly profitable for cybercriminals extracting money from victims. The average ransom increased 40-fold in the last five years from $5,000 in 2018 to $200,000 in 2020. The demands from ransomware exceeded $5M recently, and organizations spent $1.85M in one day recovery costs. They pressure victims to pay, threatening the release of confidential business information, executive decisions, or IP.

Ransomware variants have evolved for compatibility from desktop to mobile devices. Attackers have developed their business model of extortion. Ransomware-as-a-service providers allow affiliates of attackers to offer the use of tools in exchange for compromised data on the dark web. Each successful ransom payment helps tool creators work on profit-sharing models and work with hackers. Ransoms collected in cryptocurrency like Bitcoin make it difficult for government agencies to track cybercriminals and bring them to justice. The outlook of ransomware variants is not getting better; there are four times more new variants of Ransomware since WannaCry.

Organizations have started to realize that perimeter security solutions are ineffective against preventing ransomware. The blurring of the perimeter has resulted in opening new entry points for cybercriminals to exploit. Once inside, ransomware spreads laterally to other endpoints and assets in the network if left undetected. Attackers focus on spreading the malware through lateral movement, making the perimeter security ineffective. Cybercriminals frequently exploit organizations using remote access tools for their employees and outsourced staff by gaining a more accessible path through a remote connection and crippling the system through lateral movement.

Key Steps to Mitigate a Ransomware Attack

Secure your networks and workloads

- Restrict internet access
- Least-privilege access and Zero Trust segmentation
- Verify and monitor third-party access

Respond to compromise

- Immediate quarantine
- Identify compromised data

Phases in Ransomware attack

- **Campaign:** Attackers use phishing emails or weaponize websites to trick users into downloading a beacon (malicious code), thereby infecting the assets or workloads.

- **Infection:** The beacon downloads and execution begin, though the data files do not get encrypted. The malicious code dwells in the machine for an extended period to find the scope of data encryption. At this stage, detection controls have failed. The perimeter firewall, proxy, AV, EDR, and IPS/IDS have allowed the traffic to go through

- **Staging:** The beacon executed connects to command and control, which the attacker controls. The attacker uses the command-and-control server to execute commands remotely to the compromised machine. The malicious code runs even in a reboot connecting with the command-and-control server. The attacker “owns” the system.

- **Scanning:** Malicious code scans the local machine to find the files to encrypt and then scans the data stored in a cloud-synced from local data, network file share, and USB drive. At this stage, the attacker understands the permission levels of the compromised user, such as read, write, or delete, and can build the data inventory.

- **Encryption:** Usually, encryption starts with local files, then the cloud or network file shares data. The data in the cloud or network file share encrypts for download, replacing the original data file.

- **Ransom:** Once the encryption is complete, the attacker demands the ransom.

Customer Checklist for Preventing Ransomware

- ☑ Organizations can prevent ransomware threats with a robust plan. A critical step is to gain complete visibility of their assets and network. IT and security teams require comprehensive visibility into the network with vulnerability scanning to limit the blast radius and, identify and address gaps before the malware spreads laterally.

- ☑ Organizations should disable ports not used for business processes such as Remote Desktop (RDP) -Transmission Control Protocol (TCP) Port 3389 used for remote connections to other computers and prevent port 3389 exploits. A single pane display of network connections helps gain critical insights into traffic flow and dependencies.

- ☑ Organizations need Zero Trust policies to create least-privilege access to all systems and services to restrict malware propagation. Host-based micro-segmentation is essential for creating micro-perimeters and preventing access to critical Enforcing. The least-privileged access ensures role-based user access for assets and workloads.

- ☑ Segmentation-based security posture should evolve from network-based to host-based. The applications and workloads should be auto-tagged as they move from on-premises to cloud environments without reconfiguring security policies. Host-based micro-segmentation minimizes the threat exposure and controls unsolicited traffic in a distributed environment.

- ☑ Organizations often find correlating logs from multiple sources confusing. They need a centralized log management system with seamless integration to security information and event management (SIEM) tools to triage individual events and understand the implications and severity of the attack to the application and the organization.

- ☑ Visibility into network activity enables organizations to identify patterns that help differentiate legitimate and abnormal traffic flows over time. Logging of movement creates a robust analytical tool to either update or implement new security policies.

ColorTokens Xshield gives you visibility and prevents the lateral spread of ransomware

ColorTokens Xshield delivers real-time protection against ransomware in core data center and cloud workloads by segmenting and preventing lateral movement. Xshield helps prevent large-scale, costly corporate attacks with a software-defined micro-segmentation solution based on a Zero Trust architecture. The Zero Trust architecture works on the principles of least-privilege access to segment the network. The Zero Trust security model helps secure networks and workloads by restricting internet access, reducing the attack surface, preventing lateral infection, and stopping a ransomware attack efficiently.

Organizations can visualize, intervene, and block unauthorized and malicious behavior during the ransomware attack phases by verifying and checking third-party access. Automated policy assignment and auto-tagging ensure uniform and consistent security posture when assets move from on-premises to a cloud environment, helping to keep distributed assets secure. Xshield helps quarantine any affected workloads or data at once, thereby isolating any infected systems to prevent ransomware spread.

Xshield Solution Overview for Ransomware Prevention

Unified Intuitive Dashboard

The heads-up display dashboard provides a unified view of an organization's critical security. The dashboard features network alerts, workload status, traffic insights, workload vulnerability, policy coverage status, policy tampered status, notifications, and insight into top users by connection. The traffic insights are available for seven days over 24 hours, giving users visibility into every part of their infrastructure.

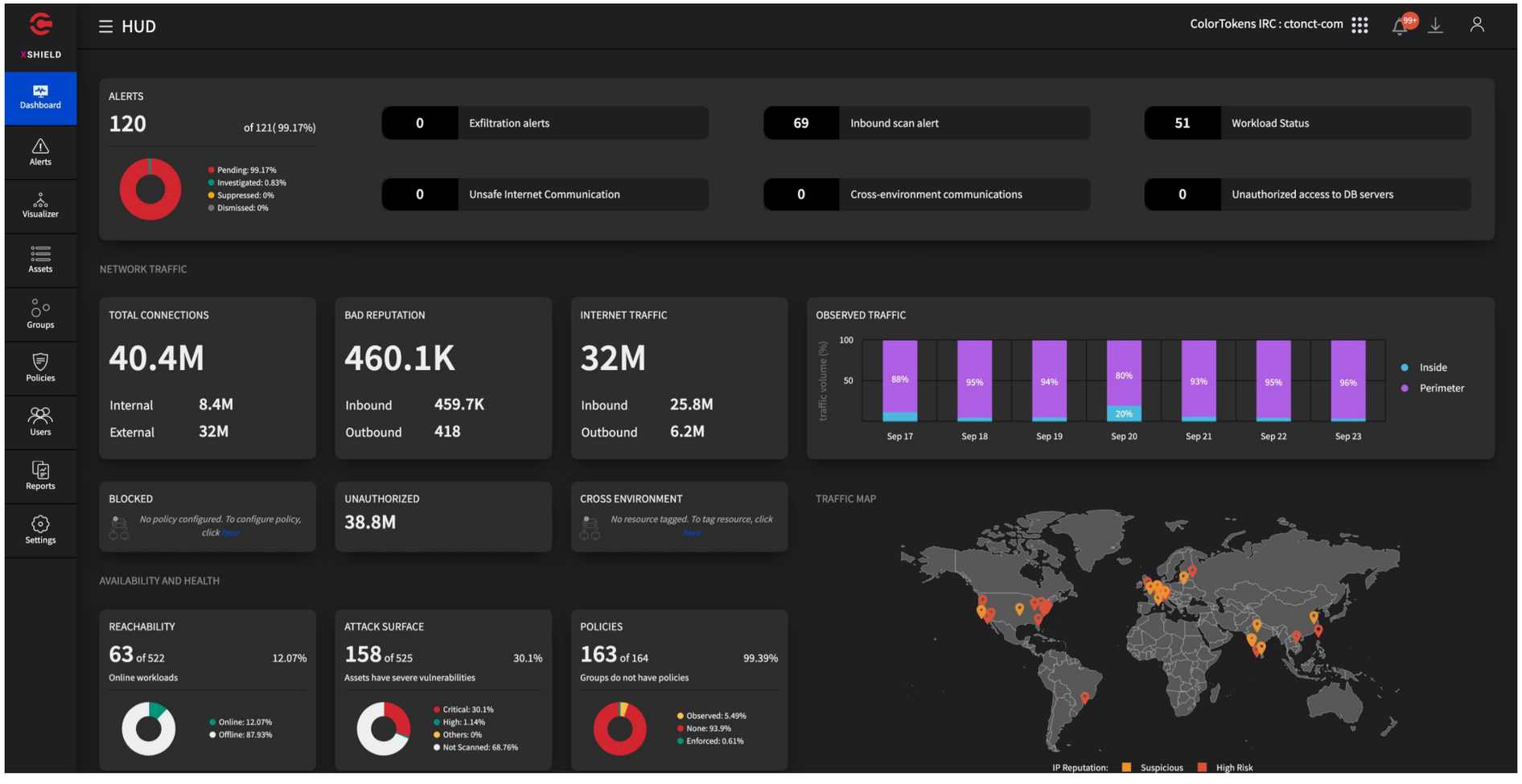


Figure 1: The Unified Inuitive Dashboard

Deep Traffic Insights

The traffic widget displays the perimeter (North-South) and inside (East-West) traffic from the workload. This widget is is essential to planning a micro-segmentation approach that stops ransomware from spreading.

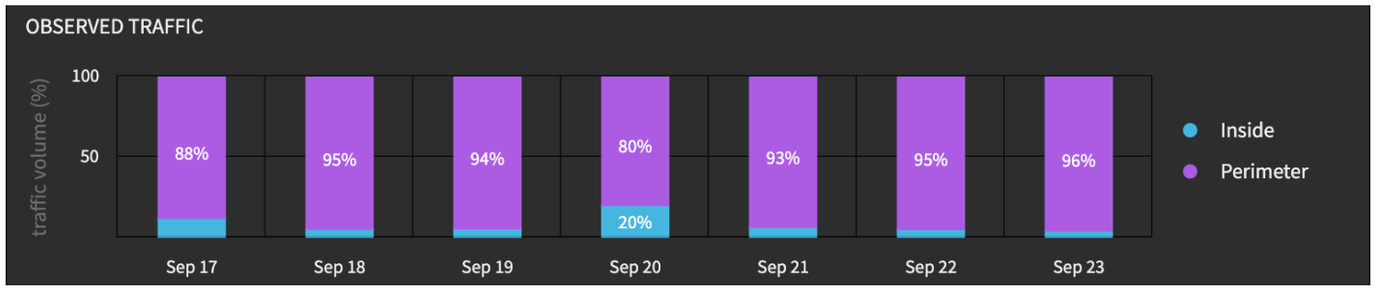
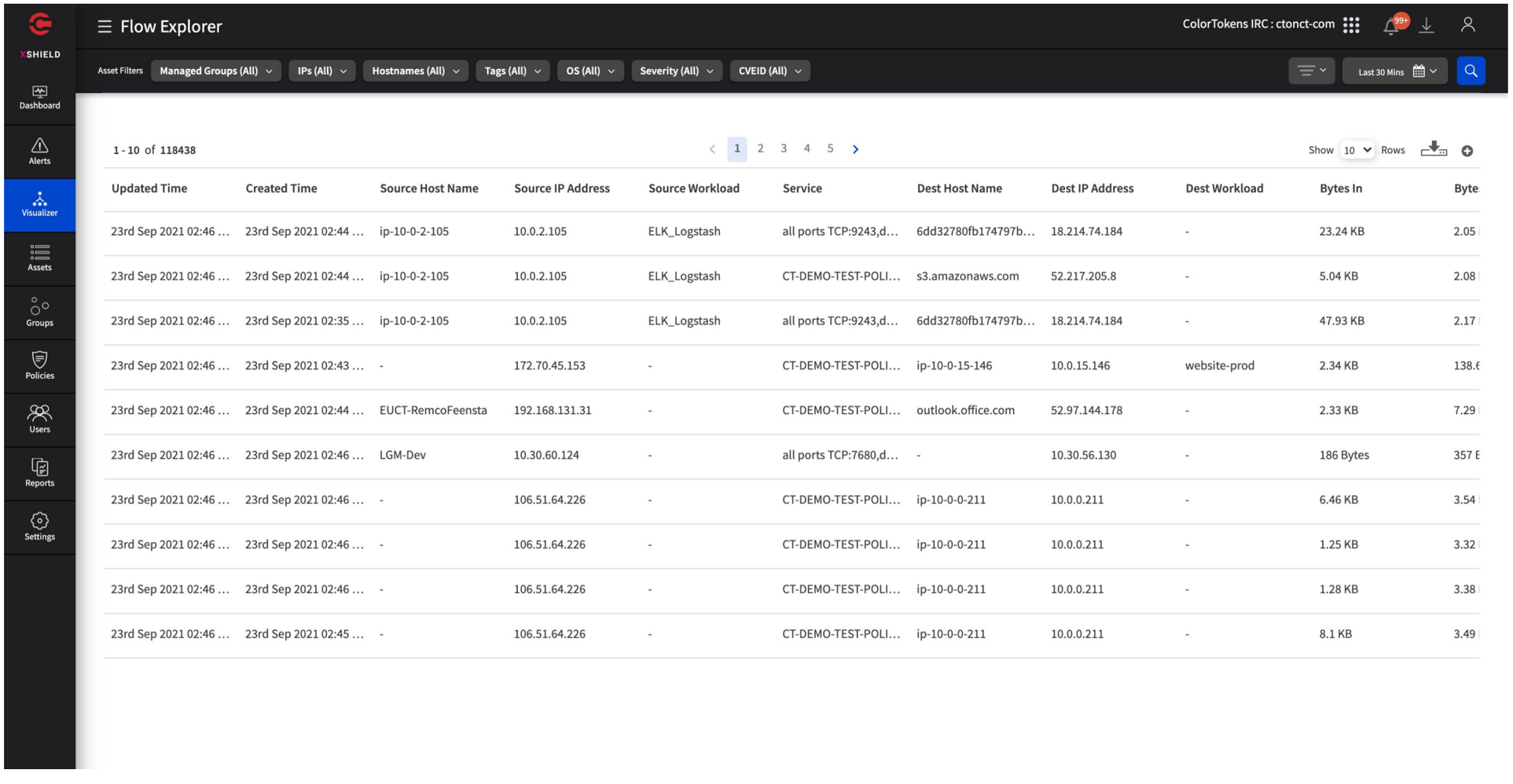


Figure 2: Traffic Insights on the unified dashbaord

Flow Explorer

The Flow Explorer enables the view of specific traffic flows to analyze traffic logs for data transferred between managed assets, discovered assets, workload groups, domain groups, endpoint groups, IP addresses, and hostnames. The data can be downloaded for analysis offline.



Updated Time	Created Time	Source Host Name	Source IP Address	Source Workload	Service	Dest Host Name	Dest IP Address	Dest Workload	Bytes In	Byte
23rd Sep 2021 02:46 …	23rd Sep 2021 02:44 …	ip-10-0-2-105	10.0.2.105	ELK_Logstash	all ports TCP:9243,d…	6dd32780fb174797b…	18.214.74.184	-	23.24 KB	2.05
23rd Sep 2021 02:46 …	23rd Sep 2021 02:44 …	ip-10-0-2-105	10.0.2.105	ELK_Logstash	CT-DEMO-TEST-POLI…	s3.amazonaws.com	52.217.205.8	-	5.04 KB	2.08
23rd Sep 2021 02:46 …	23rd Sep 2021 02:35 …	ip-10-0-2-105	10.0.2.105	ELK_Logstash	all ports TCP:9243,d…	6dd32780fb174797b…	18.214.74.184	-	47.93 KB	2.17
23rd Sep 2021 02:46 …	23rd Sep 2021 02:43 …	-	172.70.45.153	-	CT-DEMO-TEST-POLI…	ip-10-0-15-146	10.0.15.146	website-prod	2.34 KB	138.6
23rd Sep 2021 02:46 …	23rd Sep 2021 02:44 …	EUCT-RemcoFeensta	192.168.131.31	-	CT-DEMO-TEST-POLI…	outlook.office.com	52.97.144.178	-	2.33 KB	7.29
23rd Sep 2021 02:46 …	23rd Sep 2021 02:46 …	LGM-Dev	10.30.60.124	-	all ports TCP:7680,d…	-	10.30.56.130	-	186 Bytes	357 B
23rd Sep 2021 02:46 …	23rd Sep 2021 02:46 …	-	106.51.64.226	-	CT-DEMO-TEST-POLI…	ip-10-0-0-211	10.0.0.211	-	6.46 KB	3.54
23rd Sep 2021 02:46 …	23rd Sep 2021 02:46 …	-	106.51.64.226	-	CT-DEMO-TEST-POLI…	ip-10-0-0-211	10.0.0.211	-	1.25 KB	3.32
23rd Sep 2021 02:46 …	23rd Sep 2021 02:46 …	-	106.51.64.226	-	CT-DEMO-TEST-POLI…	ip-10-0-0-211	10.0.0.211	-	1.28 KB	3.38
23rd Sep 2021 02:46 …	23rd Sep 2021 02:45 …	-	106.51.64.226	-	CT-DEMO-TEST-POLI…	ip-10-0-0-211	10.0.0.211	-	8.1 KB	3.49

Figure 3: Comprehensive Flow Explorer

Real-Time Network Alerts

The dashboard displays events by rules including:

- Unsafe internet communication
- Zero Trust violations with TCP
- Zero Trust violations with non-TCP
- Cross-environment communications
- Unauthorized access to database servers.

> ***"Certain attacks — such as ransomware attacks — can cause serious damage if allowed to spread laterally. Identity-based segmentation seeks to limit the propagation of such attacks."***
>
> – *(Source:* Gartner®, Hype Cycle™ *for Network Security, Published 14 July 2021)*

The events displayed by status and a detailed view indicate what actions we can explore and whether to suppress or dismiss the alert.

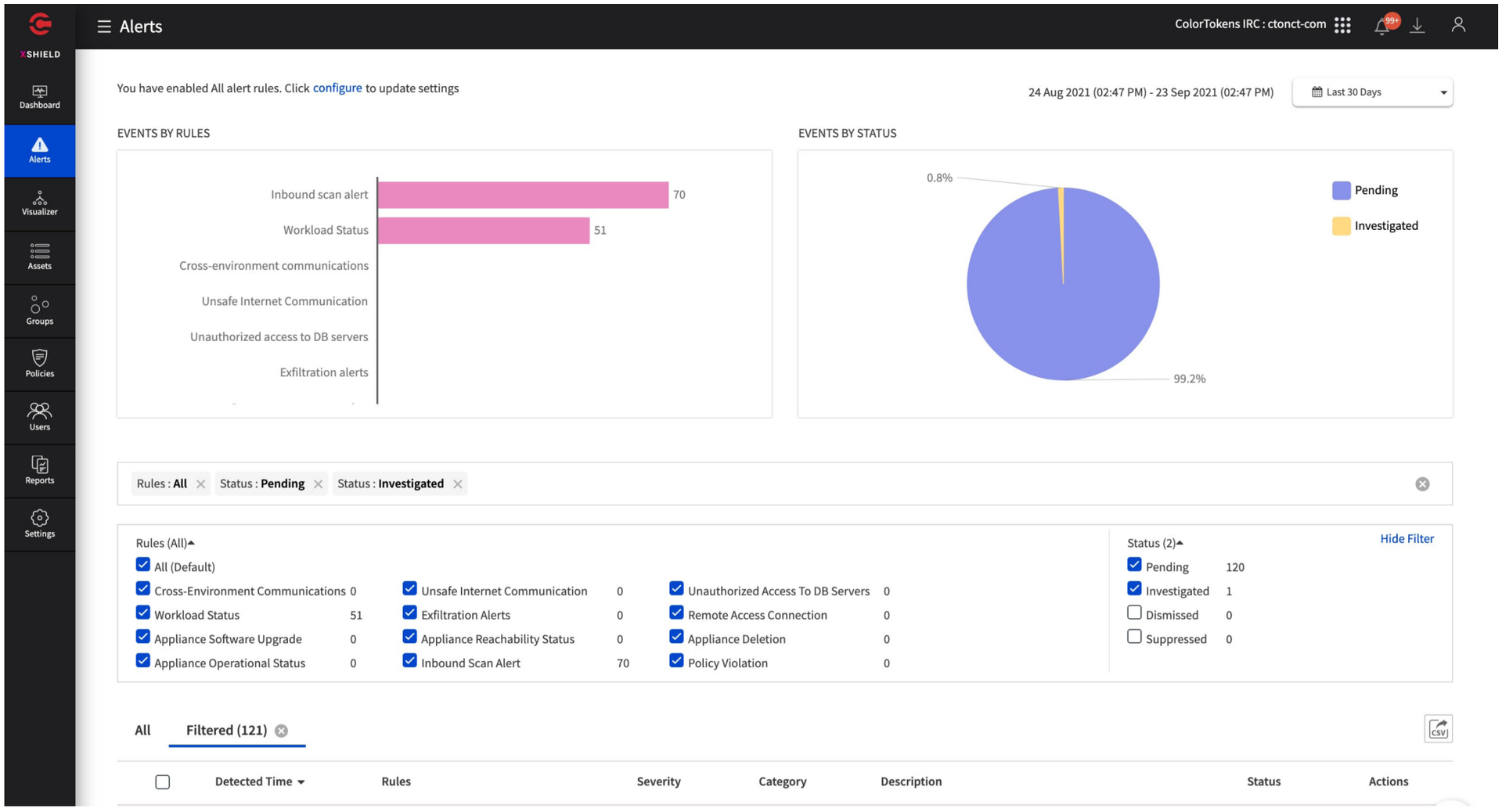


Figure 4: Display of Network Alerts

Rich Visual Explorer

The Visual Explorer is a rich and insightful representation of interactive communication collected between managed workloads, endpoints, networks, and other managed and discovered resources. The access policies govern these connections and dynamically create an intuitive, easy-to-explore visual representation. Visualization provides details of unauthorized command and control communication and the link to command and control.

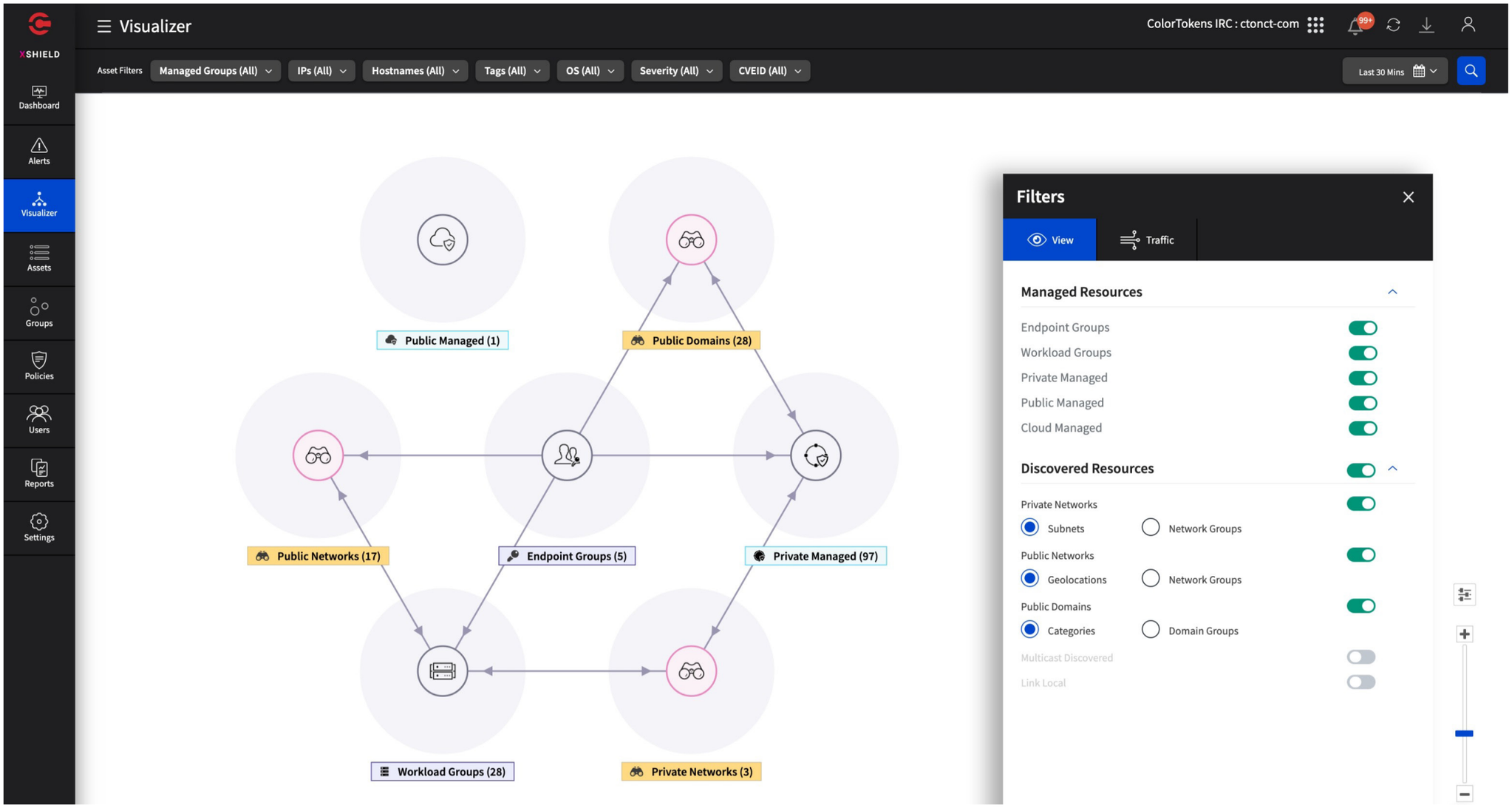


Figure 5: Business view using visual explorer

Stop Ransomware Today

Manage suspicious activities discovered on/from assets

The workloads/endpoints can be isolated and verified if they are in quarantine mode. Once the threat level is mitigated, administrators can restore the workloads/endpoints to their original state.

Investigate and Remediate

Monitoring your network for security incidents in real time reduces the breach impact. Visual Explorer and Flow Explorer help analyze unforeseen and unsafe traffic flows from insider and outsider threats. Xshield helps map application vulnerability and traffic flows in a distributed infrastructure. It blocks the C2 connection when micro-segmentation is enforced by quarantining assets early in the threat cycle.

Manage policy violations

The Visualizer displays blocked traffic, quarantining the affected workloads/endpoints from the network and verifying that workloads/endpoints are in a quarantine mode. Xshield helps block application access and lateral movement across a hybrid infrastructure by creating micro-perimeters.

Make ColorTokens your Zero Trust partner

ColorTokens provides a simplified, Zero Trust ("never trust, always verify") approach to secure an enterprise's most valuable network assets and endpoints against cyberattack. ColorTokens' Xtended ZeroTrust™ Platform is based on the NIST Zero Trust framework to address evolving new threats and compliance requirements. 100% cloud-delivered for fast time-to-value, the ColorTokens platform enables granular visibility, security, and control over endpoints, applications, and network assets to reduce attack surface and minimize the damage of breaches. Customers benefit from increased cyber-resilience to attacks, rapid containment of ransomware, and minimal business disruption.

Disclaimer

Gartner®, Hype Cycle™ for Network Security, 2021, Shilpi Handa, Pete Shoard, 14 July 2021 and this required disclaimer: GARTNER and HYPE CYCLE are registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.

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.**