DATA SHEET

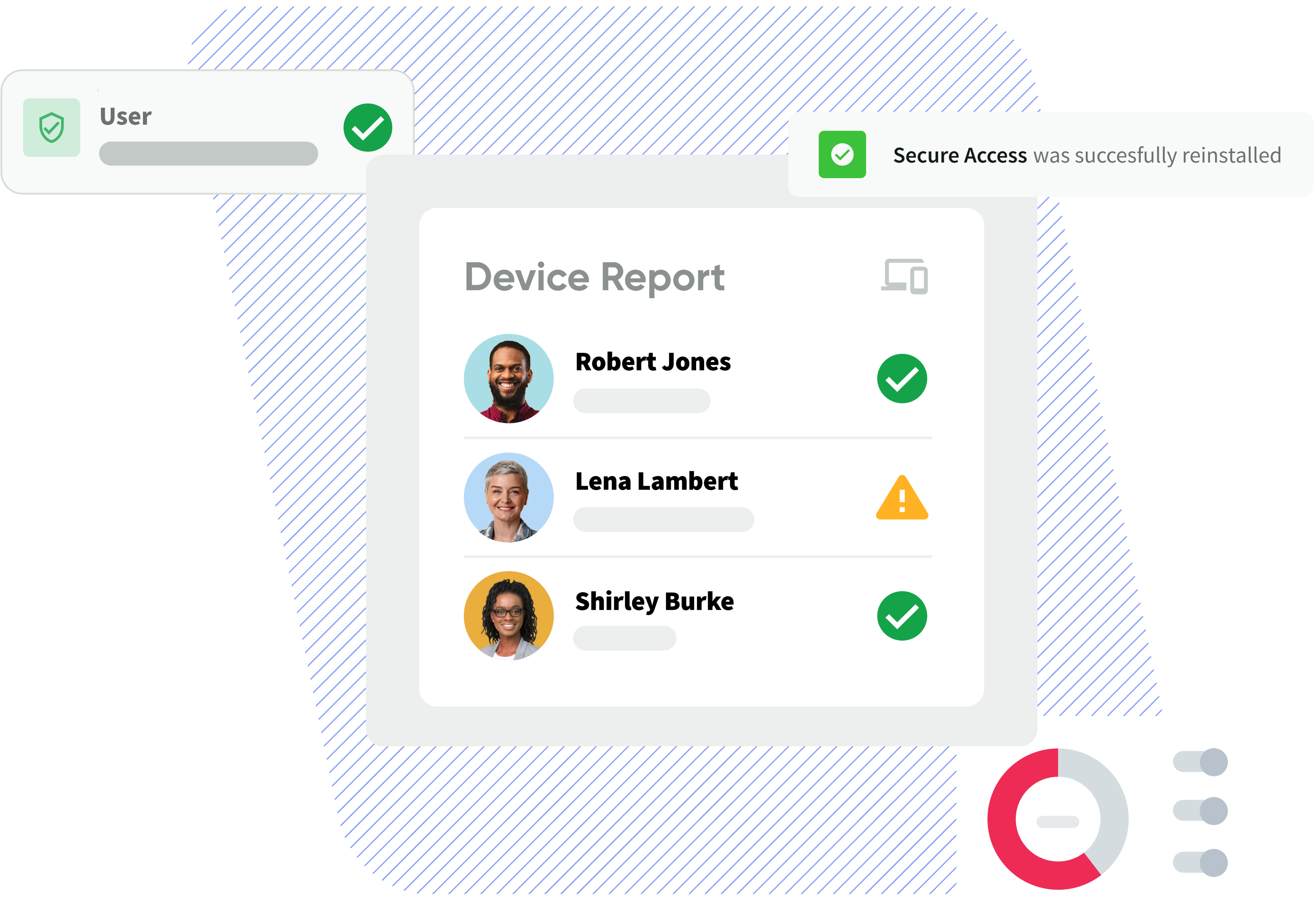
Absolute Secure Access Enterprise

Comprehensive, resilient SSE with Safe Connect and Compliance for optimized, always-on secure access to private apps, cloud, and web.

Businesses of all sizes rely on secure access for the modern workforce, whether from an office, coffee shop, at home or on a tarmac. Applications deliver critical information that help workers stay productive and keep your business safe from malware and data exfiltration so you can stay ahead of the competition.

Absolute Secure Access Enterprise is the only comprehensive Security Service Edge (SSE) solution that adds Safe Connect and Compliance for always-on secure access to protect hybrid workers from threats while keeping your data safe. We ensure devices accessing public and private clouds are secure and compliant, while delivering an optimized and productive user experience for the anywhere workforce. Backed by firmware-embedded resilience, organizations are assured their SSE remains resilient, always on, and fully operational.

It offers comprehensive protections from web-based threats like zero-day attacks, malware, and malicious code and prevents data loss and leakage. AI-powered anomaly detection offers security teams proactive alerts to suspicious behaviors — safeguarding workers and organizations that are increasingly at risk from a hostile threat landscape.



Harness the Power of an SSE Solution

The remote workforce is more reliant on secure connectivity than ever before, and today, digital information is the lifeblood of the business. Protecting against threats and data exfiltration, while ensuring resilience, is a business imperative. At the same time, IT departments are faced with the daunting challenge of encouraging increasing mobility without sacrificing security or productivity. Absolute Secure Access Enterprise combines state-of-the-art mission-critical application access with secure web gateway features* and endpoint security that protect workers from the untrusted internet – and protect your business from an increasingly hostile threat landscape.

Key Use Cases

- **Secure Access for Hybrid, Mobile, and Field Workers** Persistent, resilient, and reliable secure access for workers on their device of choice – even in challenging conditions. Connection maintained while traversing networks and pausing device activity.
- **Advanced Cyberthreat Protection** Complete protection from zero-day threats, malware, malicious code, spyware, ransomware, and possible data loss and leakage for all workers regardless of their location — and keeping organizations safe.
- **AI-powered Deep Visibility Inside & Outside Corporate Perimeter** 70+ dashboards provide proactive and reactive alerts and rich analytics on anomalous behavior as well as user, device, network and application performance, from cellular to public Wi-Fi.

Endpoint Visibility, Control, and Resilience

Secure Access Enterprise also includes Endpoint Compliance that gives IT the upper hand with additional features to ensure endpoints – the most common attack vector — are as secure as possible. This enables IT to resolve issues faster, identify threats before they become issues, and reduce potential future attacks. Specifically, IT teams can assess endpoint compliance across a variety of factors such as device location, the health of security vitals (e.g., Encryption and Anti-Malware) as well as other mission-critical applications. In addition, they can remotely respond whenever devices stray from compliance by executing a freeze or flagging devices that go missing

Key Capabilities Include

- ✓ Get complete hardware reporting, including encryption status and on-board AV protection status
- ✓ Track missing devices with geolocation information to safeguard devices
- ✓ Perform on-demand freeze / unfreeze when threats have been detected
- ✓ Enable Secure Access client repair / reinstall for optimal organizational resilience

With Endpoint Compliance, IT finally has endpoint security controls in a converged secure access package to protect against device risks and compliance, assuring your organization of optimal protection and maximum productivity.

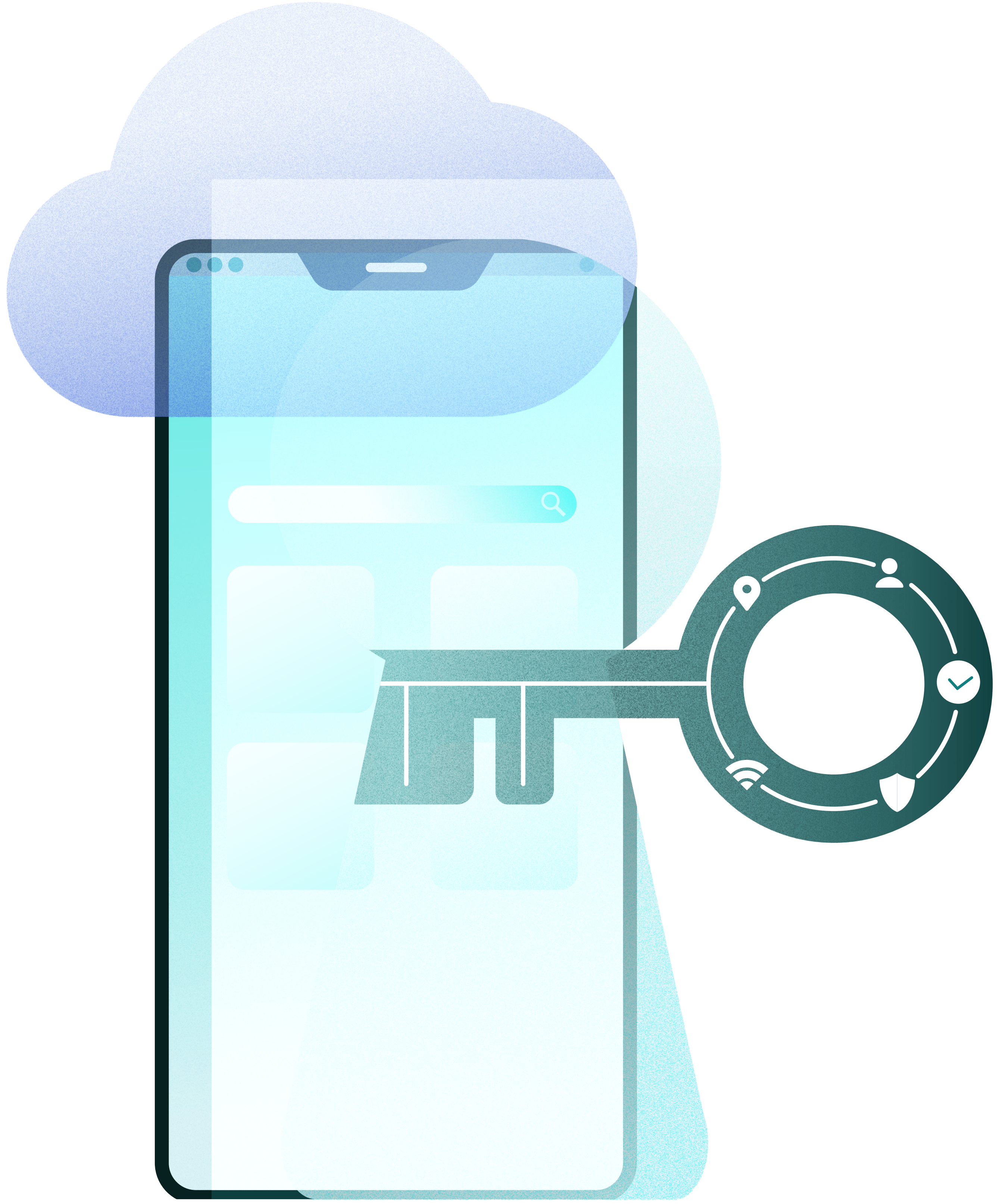
*Powered by Ericom

Zero Trust Network Access (ZTNA)

Absolute Secure Access Enterprise delivers persistent, resilient, and reliable connections — even in challenging conditions — with comprehensive security for today's demanding hybrid and mobile environment. Using their device of choice, workers can connect to applications and browse the web, click email links, and download files — without exposing your organization to malware, zero-day attacks, or other malicious code that could hinder business operations and worker productivity.

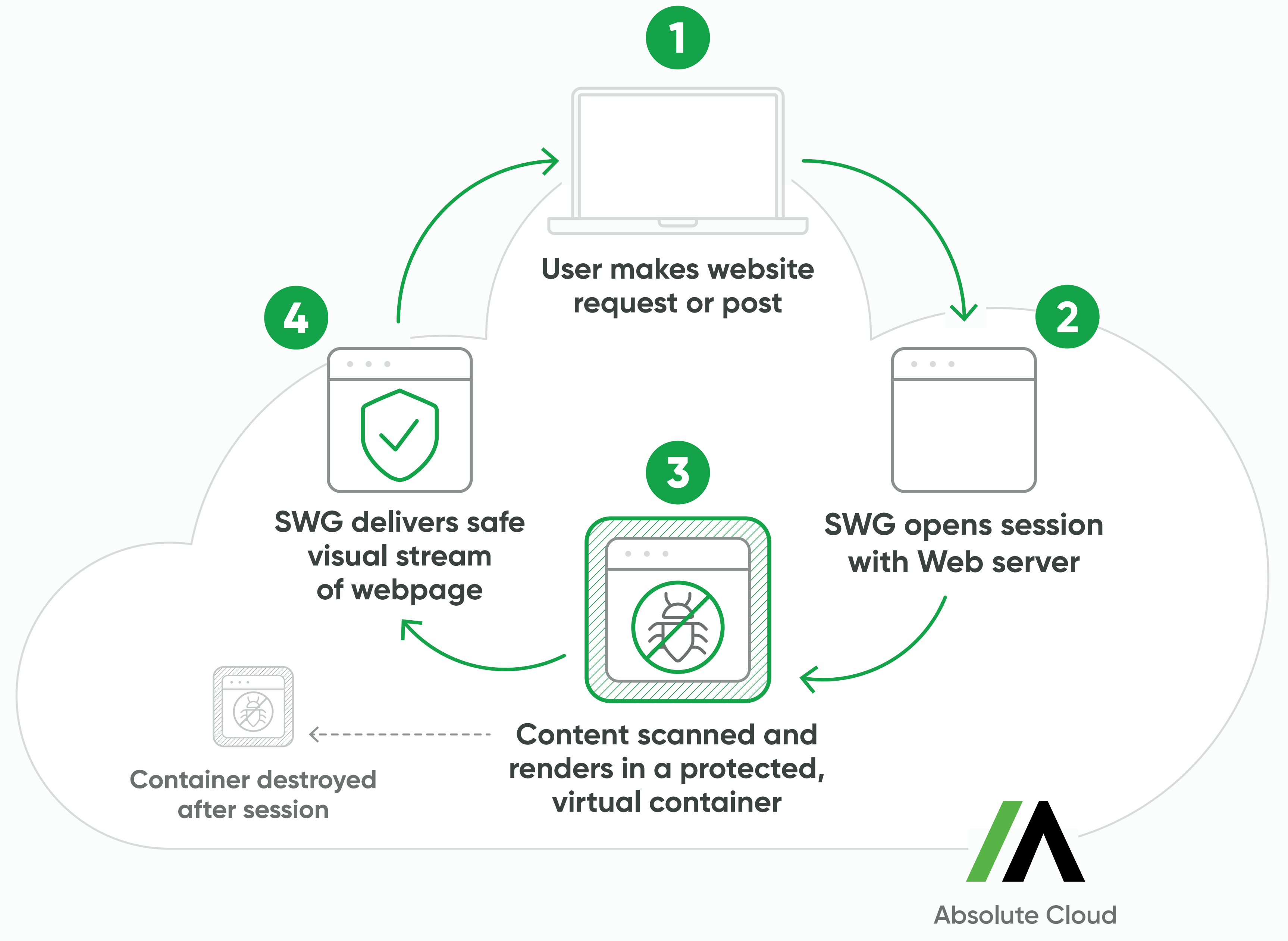
Key Capabilities

- ✓ **Secure, Persistent, Resilient Connections** Endpoint-to-application tunnel encryption and session resilience that doesn't falter, even if the network does
- ✓ **Distributed Firewall** Each endpoint functions as distributed firewall preventing intrusions across the organization
- ✓ **Conditional Application Access** Enforce conditional access to any online destination based on risk and compliance
- ✓ **Network Access Control (NAC)** Ensure only devices with healthy security and management controls are allowed to connect, both inside and outside the tunnel, and take action if needed (warn, remediate, disconnect, quarantine)
- ✓ **Network, Audio, and Video Optimizations** Streamlined, always-on connections even in remote areas
- ✓ **Dynamic Endpoint Policy Enforcement** Enforce policies inside and outside the tunnel for best protection based on device, location, time of day, and other parameters
- ✓ **Prioritize Mission-Critical Applications** Prioritize business apps by deprioritizing unnecessary apps on slower networks
- ✓ **Full Software Defined Perimeter** Applications are hidden from unauthorized users, reducing the "blast radius" if an attacker gets in



HOW IT WORKS

Absolute Secure Web Gateway


1
User makes website request or post
2
SWG opens session with Web server
3
Content scanned and renders in a protected, virtual container
4
SWG delivers safe visual stream of webpage
Container destroyed after session
Absolute Cloud

Secure Internet Access (Secure Web Gateway)

Absolute Secure Access Enterprise gives IT administrators the unique capability of enforcing policy (and viewing activity) inside and outside the secure, optimized tunnel. This offers unprecedented visibility, security, and control as well as preventing any chokepoints, bottlenecks, or unnecessary data backhaul. Users get streamlined application access — even in challenging conditions — while IT can monitor activity and refine policies for the safest, most productive experience.

Further, Secure Access' web protections are tightly integrated with our powerful policy engine, allowing fine-grained control with all common HTML5 browsers.

Key Capabilities

- ✓ **Protect Against Known and Unknown Threats** Scan for malware, malicious content, and zero-day attacks and remove hidden executable malware with Remote Browser Isolation (RBI)
- ✓ **Apply Multiple AV Scans** Protect devices and organizations from known threats and keep organizations safe from malicious content
- ✓ **Content Disarm and Reconstruct (CDR)** Isolate files before downloading, protecting against zero-day threats not detected otherwise by anti-virus scans
- ✓ **Insulate Users from Risky Websites** Execute web content in the cloud — away from local devices — and govern access to known bad sites and content through AI-powered categorization
- ✓ **Prevent Data Loss and Leakage** Enforce regulatory compliance and protect intellectual property with integrated Data Loss Prevention (DLP)
- ✓ **Increased scrutiny with SSL/TLS inspection** for low-risk traffic, keeping sensitive data secure and organizations safe

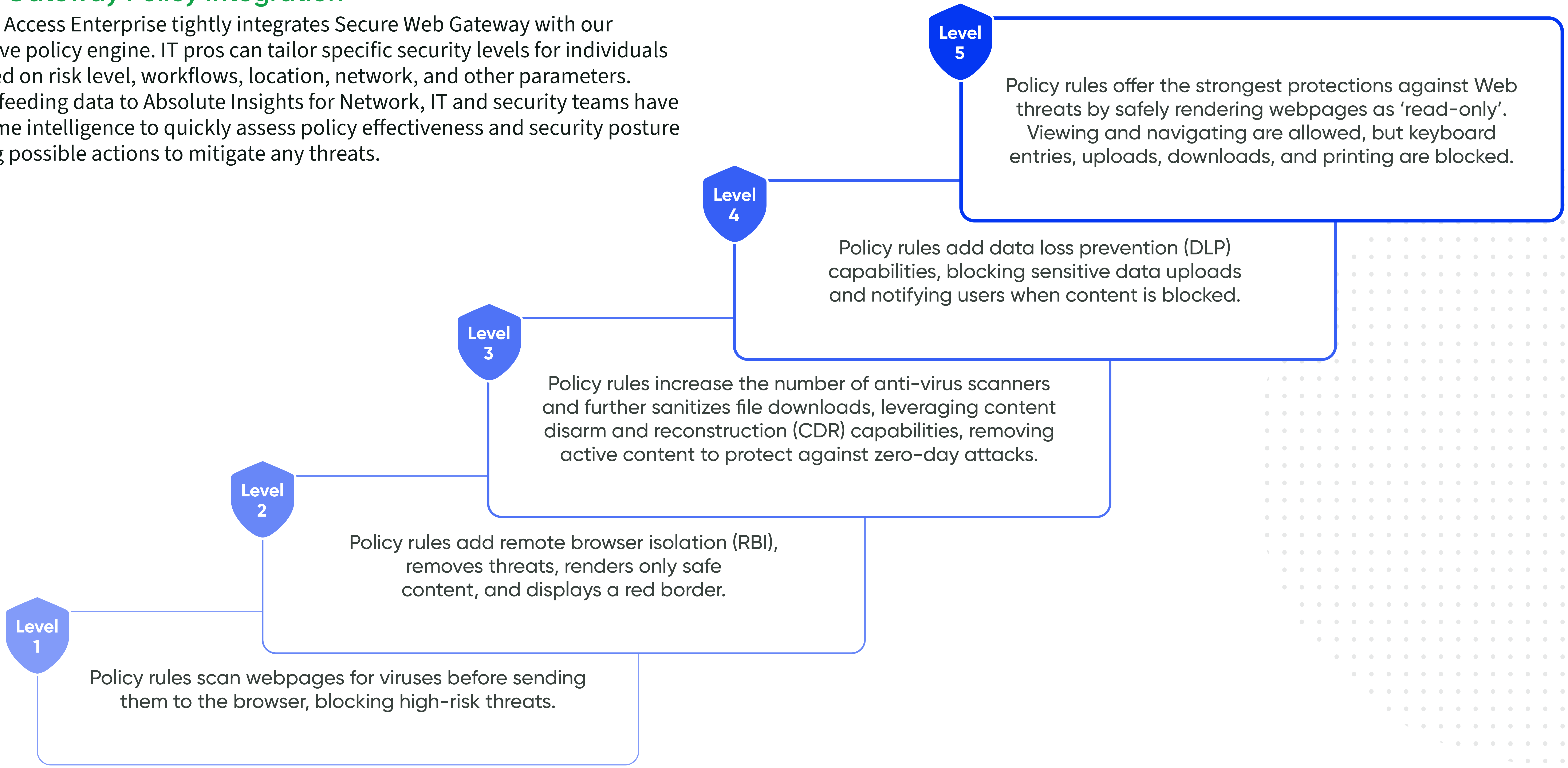
Cloud Access Security Broker (CASB)

Enterprise Secure Access includes an integrated forward and reverse proxy to protect inline SaaS applications from unauthorized access and usage.

- ✓ **Protect SaaS Applications** Integrated CASB capabilities for inline protection of SaaS applications
- ✓ **Visibility of "Shadow IT" usage** Ensure that your workforce is using approved AI websites to protect sensitive data

Secure Web Gateway Policy Integration

Absolute Secure Access Enterprise tightly integrates Secure Web Gateway with our dynamic, adaptive policy engine. IT pros can tailor specific security levels for individuals and groups based on risk level, workflows, location, network, and other parameters. Additionally, by feeding data to Absolute Insights for Network, IT and security teams have access to real-time intelligence to quickly assess policy effectiveness and security posture while identifying possible actions to mitigate any threats.



Level 5

Policy rules offer the strongest protections against Web threats by safely rendering webpages as ‘read-only’. Viewing and navigating are allowed, but keyboard entries, uploads, downloads, and printing are blocked.

Level 4

Policy rules add data loss prevention (DLP) capabilities, blocking sensitive data uploads and notifying users when content is blocked.

Level 3

Policy rules increase the number of anti-virus scanners and further sanitizes file downloads, leveraging content disarm and reconstruction (CDR) capabilities, removing active content to protect against zero-day attacks.

Level 2

Policy rules add remote browser isolation (RBI), removes threats, renders only safe content, and displays a red border.

Level 1

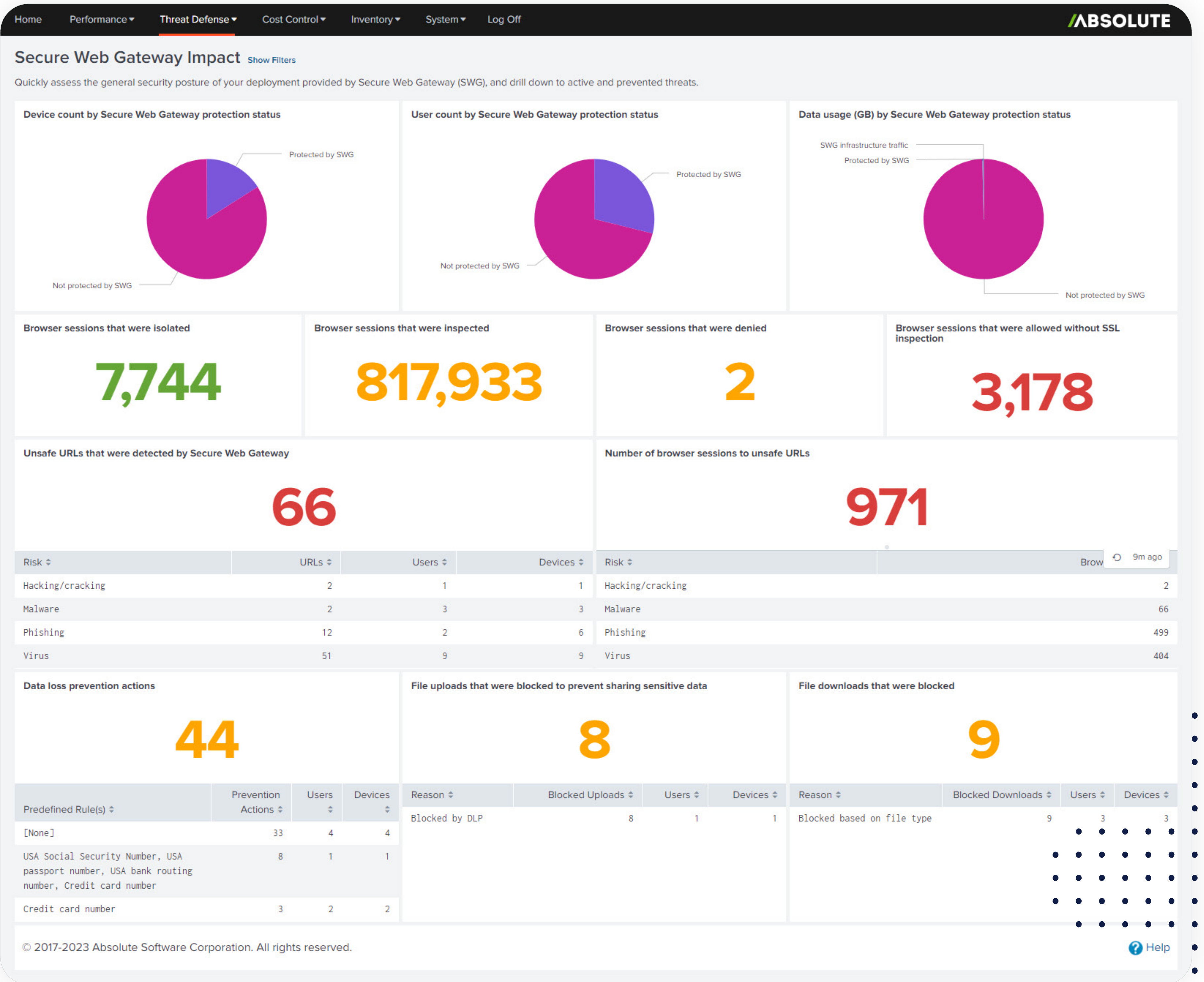
Policy rules scan webpages for viruses before sending them to the browser, blocking high-risk threats.

Digital Experience Monitoring (DEM) & Network Performance Monitoring and Diagnostics (NPMD)

The ability to gather real-time actionable data about worker experiences can have a major impact on an organization's success. Absolute Secure Access Enterprise provides comprehensive DEM and NPMD dashboards that give deep visibility into user and network behavior. Over 70 dashboards display near real-time, non-synthetic information about users, devices, applications, and network performance in a single pane of glass. Both IT and security teams can quickly assess the current and historical state of users and networks for troubleshooting, monitoring, and capacity planning with data from the past 90 days.

Key Capabilities Include

- ✓ Summarize the overall impact of security policies and actions, data loss and prevention, browser sessions, file transfers, and user feedback
- ✓ List granular information for network performance, cost control, security, and inventory management
- ✓ Get comprehensive views of your entire network
  - › From Layer 1 to application and flow data
  - › Device, connectivity, and application health
  - › Telemetry and diagnostics for traffic inside and outside the tunnel
  - › Carrier signal quality maps
  - › Mobile router network telemetry
  - › Mobile router GPS quality
  - › Hop-by-hop latency and transaction time monitoring
  - › Vehicle modem integrations
  - › AI-based flow-level diagnostics
- ✓ Display configurable network diagnostics, including
  - › Application server connectivity and service connectivity diagnostics
- ✓ Quickly identify issues with real-time geo-enabled dashboards across cellular and Wi-Fi networks



Secure Web Gateway Impact Show Filters

Quickly assess the general security posture of your deployment provided by Secure Web Gateway (SWG), and drill down to active and prevented threats.

Device count by Secure Web Gateway protection status

User count by Secure Web Gateway protection status

Data usage (GB) by Secure Web Gateway protection status

Browser sessions that were isolated

7,744

Browser sessions that were inspected

817,933

Browser sessions that were denied

2

Browser sessions that were allowed without SSL inspection

3,178

Unsafe URLs that were detected by Secure Web Gateway

66

Risk ⇕	URLs ⇕	Users ⇕	Devices ⇕
Hacking/cracking	2	1	1
Malware	2	3	3
Phishing	12	2	6
Virus	51	9	9

Number of browser sessions to unsafe URLs

971

Risk ⇕	Brow
Hacking/cracking	2
Malware	66
Phishing	499
Virus	404

9m ago

Data loss prevention actions

44

Predefined Rule(s) ⇕	Prevention Actions ⇕	Users ⇕	Devices ⇕
[None]	33	4	4
USA Social Security Number, USA passport number, USA bank routing number, Credit card number	8	1	1
Credit card number	3	2	2

File uploads that were blocked to prevent sharing sensitive data

8

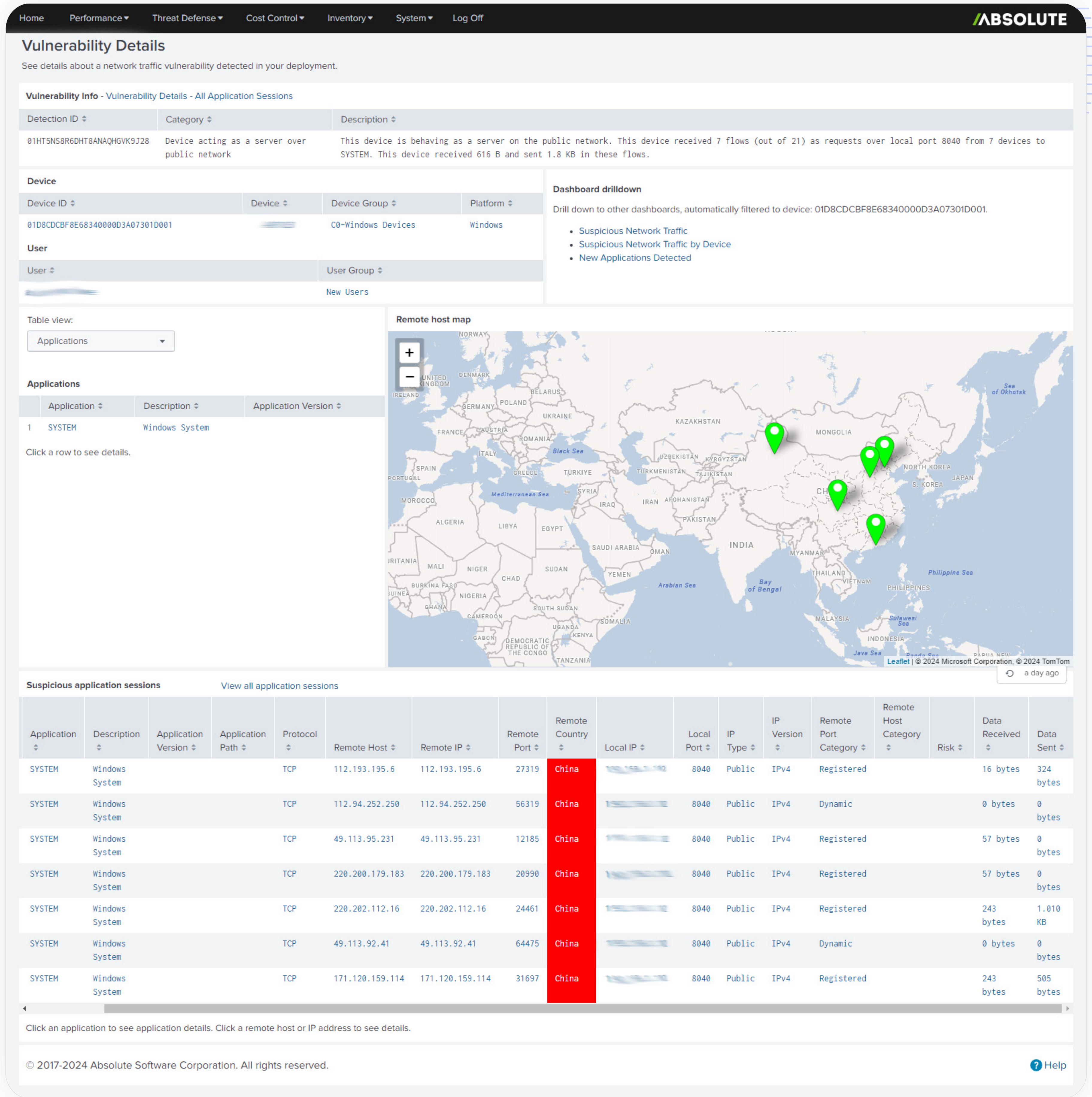
Reason ⇕	Blocked Uploads ⇕	Users ⇕	Devices ⇕
Blocked by DLP	8	1	1

File downloads that were blocked

9

Reason ⇕	Blocked Downloads ⇕	Users ⇕	Devices ⇕
Blocked based on file type	9	3	3

© 2017-2023 Absolute Software Corporation. All rights reserved.



Vulnerability Details

See details about a network traffic vulnerability detected in your deployment.

Vulnerability Info - Vulnerability Details - All Application Sessions

Detection ID ⇕	Category ⇕	Description ⇕
01HT5NS8R6DHT8ANAQHGVK9J28	Device acting as a server over public network	This device is behaving as a server on the public network. This device received 7 flows (out of 21) as requests over local port 8040 from 7 devices to SYSTEM. This device received 616 B and sent 1.8 KB in these flows.

Device

Device ID ⇕	Device ⇕	Device Group ⇕	Platform ⇕
01D8CDCBF8E68340000D3A07301D001	[redacted]	C0-Windows Devices	Windows

User

User ⇕	User Group ⇕
[redacted]	New Users

Dashboard drilldown

Drill down to other dashboards, automatically filtered to device: 01D8CDCBF8E68340000D3A07301D001.

- Suspicious Network Traffic
- Suspicious Network Traffic by Device
- New Applications Detected

Table view:

Applications ▾

Applications

	Application ⇕	Description ⇕	Application Version ⇕
1	SYSTEM	Windows System	

Click a row to see details.

Remote host map

Leaflet | © 2024 Microsoft Corporation, © 2024 TomTom

a day ago

Suspicious application sessions View all application sessions

Application ⇕	Description ⇕	Application Version ⇕	Application Path ⇕	Protocol ⇕	Remote Host ⇕	Remote IP ⇕	Remote Port ⇕	Remote Country ⇕	Local IP ⇕	Local Port ⇕	IP Type ⇕	IP Version ⇕	Remote Port Category ⇕	Remote Host Category ⇕	Risk ⇕	Data Received ⇕	Data Sent ⇕
SYSTEM	Windows System			TCP	112.193.195.6	112.193.195.6	27319	China	[redacted]	8040	Public	IPv4	Registered			16 bytes	324 bytes
SYSTEM	Windows System			TCP	112.94.252.250	112.94.252.250	56319	China	[redacted]	8040	Public	IPv4	Dynamic			0 bytes	0 bytes
SYSTEM	Windows System			TCP	49.113.95.231	49.113.95.231	12185	China	[redacted]	8040	Public	IPv4	Registered			57 bytes	0 bytes
SYSTEM	Windows System			TCP	220.200.179.183	220.200.179.183	20990	China	[redacted]	8040	Public	IPv4	Registered			57 bytes	0 bytes
SYSTEM	Windows System			TCP	220.202.112.16	220.202.112.16	24461	China	[redacted]	8040	Public	IPv4	Registered			243 bytes	1.010 KB
SYSTEM	Windows System			TCP	49.113.92.41	49.113.92.41	64475	China	[redacted]	8040	Public	IPv4	Dynamic			0 bytes	0 bytes
SYSTEM	Windows System			TCP	171.120.159.114	171.120.159.114	31697	China	[redacted]	8040	Public	IPv4	Registered			243 bytes	505 bytes

Click an application to see application details. Click a remote host or IP address to see details.

© 2017-2024 Absolute Software Corporation. All rights reserved.

User and Entity Behavior Analytics (UEBA)

Secure Access Enterprise includes AI Threat Insights, a proactive anomaly detection engine. It leverages the power of multi-dimensional Machine Learning (ML) and artificial intelligence to provide comprehensive advanced threat detection and UEBA. It monitors each organization's user, device, network, and application behavior and forms a comprehensive baseline from activity inside and outside the tunnel.

Then, using advanced generative AI algorithms, it continuously monitors user and devices for deviations from their behavior baseline, providing early detection of suspicious activities, including:

- Data exfiltration
- New applications generating network traffic
- Unsafe application and web browsing behavior
- Malicious network port scanning
- Possible denial of service attacks
- Abnormal device network usage
- Device usage at unusual times
- Higher amounts of data than expected
- New or anomalous network usage patterns
- Device acting as a server
- Device refusing server-like requests

As new threats emerge and behaviors evolve, AI Threat Insights automatically modifies its baselines, ensuring that an organization's defenses remain continuously updated. And it generates configurable alerts in the Secure Access console with rich context and direct links to detailed Insights for Network dashboards, empowering security teams to prioritize and investigate potential threats. It is available for SaaS deployments only.

Premium Support Included

Unlike vendors that charge extra to speak to Technical Support, Absolute firmly believes that customers should have 24 × 7 × 365 phone support at no additional cost. Absolute also offers a complete knowledge base with documentation and guides as well as product help, also at no added charge.

Getting Started

Absolute Secure Access Enterprise is available for free trial and purchase for on-premises or SaaS deployments. It is our most powerful package, designed and optimized for mobile work environments, and encompasses the features of **Absolute Secure Access Core** and **Absolute Secure Access Edge** as well as **Absolute Insights for Network**.

ABSOLUTE®

Absolute Security is partnered with more than 28 of the world's leading endpoint device manufacturers, embedded in the firmware of 600 million devices, trusted by 21,000 global enterprises, and licensed across 14 million PC users. With the Absolute Security Cyber Resilience Platform integrated into their digital enterprise, customers ensure their mobile and hybrid workforces connect securely and seamlessly from anywhere in the world and that business operations recover quickly following cyber disruptions and attacks. Our award-winning capabilities have earned recognition and leadership status across multiple technology categories, including **Zero Trust Network Access (ZTNA)**, **Endpoint Security**, **Security Services Edge (SSE)**, Firmware-Embedded Persistence, **Automated Security Control Assessment (ASCA)**, and **Zero Trust Platforms**.

Request a Demo