Intrusion Shield Cloud

Shield Cloud, powered by our Global Threat Engine, provides zero trust cloud-based security integrated with firewall functionality that automates the detection and prevention of communications with unauthorized servers, high risk domains, and untrusted destinations while providing next generation firewall functionality.

Why Shield Cloud?

The dynamic and persistent nature of cybersecurity threats means that today's attacks originate from or communicate to a broad range of Internet locations. Legacy security technologies and practices trust unknown risk locations by default, allowing communications or file downloads. They hope to detect malicious behavior after the malware has already begun attacking protected systems. To address these network security threats, we must reimagine our network security mindset to one of verify before trust. We have to know who our network is talking to and allow communication only with trusted IP addresses.

The Intrusion Shield Cloud solution provides unrivaled security for all networked devices by starting security at the lowest communication level. Using our Global Threat Engine, Shield Cloud allows communication packets to be sent or received with only low risk and pre-authorized Internet locations. Attacker reconnaissance, malware downloads, and malware commands are all stopped by preventing communications to their high-risk locations.

What is Shield Cloud?

Shield Cloud is a cloud native network security appliance that enables enterprises to monitor and control network communications for all devices on their cloud network. Shield Cloud ensures a device communicates with either trusted devices or allowed low risk devices on the Internet. Shield Cloud prevents both outbound communications to untrusted locations and inbound communications from untrusted locations in addition to performing traditional firewall functionality.

What can Shield Cloud do for you?

Shield Cloud stops attacker reconnaissance, ransomware, phishing, malware downloads, command and control, zero-day attacks, data exfiltration and other elusive threats by preventing communications with high risk and untrusted entities. Shield Cloud protects all cloud devices and physical networks accessed through Shield Cloud.

Reduce your attack surface and provide defense-in-depth supported by our Global Threat Engine that knows the threat risk expected from trillions of IP addresses and domains.

Network Security

Landscape

Network security works by establishing firewalls at network boundaries and then using rules to allow safe-passage for desired communications. Due to the limited number of rules and how they are defined these holes can be exploited by attackers, malware, and malicious communications. Next Gen Firewalls and IDPS systems try to identify an exploitation of firewall rules only after the network has been compromised.

Shield Differentiators

Shield Cloud protects all networked devices by reducing the attack surface and minimizing risks by only allowing communications with trusted devices. It provides protection for reconnaissance, phishing, bots, command-and-control, and data exfiltration while preventing the download of malware into your network.

Shield Cloud provides the equivalent of trillions of behavior rules to prevent the malware downloads and illicit communications before they reach into your network (verify before trust).

Malware and Ransomware Security

Landscape

Legacy protection tools allow communications and downloads from unknown, untrusted, and high-risk IP addresses. Malware and Ransomware enter your network from these communications and downloads.

Shield Differentiators

Shield Cloud risk scores every location (IP address and domain name) on the Internet and prevents communications with high-risk locations. As a result, malware and ransomware downloads and command and control communications are prevented.

Advanced Threat Security

Landscape

Network security appliances such as Next Gen Firewalls and IDPS systems have limited rules and allow communications with unknown locations by default. They use advanced analysis techniques that only identify malware and bad actors once in the network.

Shield Differentiators

Shield Cloud detects threats that elude firewall rules and IDPS prevention layers by automatically preventing communications with bad actors and other high- risk locations on the Internet. Full logging of communication attempts, both blocked and allowed, enables threat hunting and network forensics.

Phishing Security

Landscape

Email protection tools such as Microsoft, Proofpoint, and Mimecast still allow Phishing and SPAM emails into your inbox. If you click the link then your firewall allows you to download the malware.

Shield Differentiators

Shield Cloud stops phishing link communications from reaching their destinations by preventing communications with untrusted and high-risk locationa. This stops the malware download and prevents the attacker from learning that the link was clicked.

Level of protection Shield provides within the Mitre ATT&CK Framework

Step	ATT&CK	Description	Level of Protection
1	Reconnaissance	The adversary is trying to gather information they can use to plan future operations.	
2	Resource Development	The adversary is trying to establish resources they can use to support operations.	
3	Initial Access	The adversary is trying to get into your network.	
4	Execution	The adversary is trying to run malicious code.	
5	Persistence	The adversary is trying to maintain their foothold.	
6	Privilege Escalation	The adversary is trying to gain higher level permissions.	
7	Defense Evasion	The adversary is trying to avoid being detected.	
8	Credential Access	The adversary is trying to steal account names and passwords.	
9	Discovery	The adversary is trying to figure out your environment.	
10	Lateral Movement	The adversary is trying to move through your environment.	
11	Collection	The adversary is trying to gather data of interest to their	
12	Command and Control	The adversary is trying to communicate with compromised systems to control them.	
13	Exfiltration	The adversary is trying to steal data.	
14	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.	

The Mitre ATT&CK Framework details the primary steps an attacker takes to execute an attack on a victim network. This framework forms the Mitre ATT&CK cyber kill chain.

Shield Cloud protects the Network at every step within the Mitre ATT&CK cyber kill chain by preventing communications with untrusted devices on the Internet.

Target Customers

1. Net New Customers: opportunity to present the Shield family of security systems. Deliver uncompromised enterprise security for all business sizes.
2. Existing Customers: Upscale to the full Shield family of security systems, all powered by our Global Threat Engine.
3. Verticals: branch, small enterprise, midsize enterprise, large enterprise, datacenter, healthcare, retail/wholesale, travel and leisure, financial, government, MSSP

Competitive Benefits of Shield Cloud	
Shield Cloud	Unique Abilities – Firewall, Phishing protection, 0–Day protection, Safe Web browsing, Prevents high-risk downloads, stops bot communications, stops command and control, stops ransomware, zero-trust gateway
	Preemptive Approach – Preemptively stops communications with high-risk entities and prevents delivery of malicious files and malicious commands to end users
	Zero Trust Authentication Gateway – authentication is based on both a user and a device to mitigate user credential stealing for secure zero trust connectivity.
	Communication Logs enable threat hunting and forensic analysis
	Superior Threat Intelligence – Global Threat Engine provides a comprehensive, real-time, risk score
How to Compete	
Next Gen Firewall (AWS Guard Duty, Azure Firewall Premium, Palo Alto VM, Fortinet FortiGate, Cisco Umbrella, Barracuda, Sophos, etc.)	Attempts to identify malicious behavior occurring on the network through signatures and rules.
	Reactive approach identifies malicious activity based on behavior already occurring on the network. Allows communications by default, enabling communications and downloads from unknown risk locations enabling phishing, command-and-control, and malware/ransomware downloads.
	Allows outbound communications to all but well-known high-risk locations.
	Limited threat hunting and forensic analysis from performance degrading logging.
	Limited threat intelligence looking only for prior identified behavior signatures and well-known high-risk locations.
Darktrace Enterprise	Self-learning AI is modeled on the human immune system.
	Reactive approach identifies malicious behavior based upon learned signatures. Allows communications by default.
	Traditional VPN connectivity only. Allows outbound communications
	Limited communication logs.
	Limited threat intelligence looking only for prior identified behavior signatures and well-known high-risk locations.

Common Use Cases for Shield Cloud

A. Prevent malware/ransomware download
B. Stop phishing click downloads
C. Detect endpoint threats and existing malware
D. Stop illicit device scanning and reconnaissance
E. Stop malware command and control
F. Stop zero-day attacks
G. Prevent data exfiltration
H. Discover shadow IT
I. Protect mobile devices
J. Protect IoT and embedded devices
K. Protect BYOD devices while on the network

Vendors	Shield OnPremise	AWS Guard Duty	Azure Premium	Palo Alto VM 500	Fortinet Fortigate	Darktrace Enterprise
Phishing Protection	●	◐	◐	◐	◐	◐
Zero-Day Protection	●	◐	◐	◐	◐	◐
Safe Browsing	●	◐	◐	◐	◐	◐
Download Protection	●	◐	◐	◐	◐	◐
Command & Control Protection	●	◐	◐	◐	◐	◐
Anti-Bot Protection	●	◐	◐	◐	◐	◐
URL Filtering	●	●	●	●	●	●
Data Exfiltration	●	◐	◐	◐	◐	◐
Threat Hunting & Forensics Support	●	◐	◐	◐	◐	◐
Lateral Movement Detection & Protection	●	○	○	○	○	○
Anti-Virus/Malware Detection & Protection	◐	◐	◐	◐	◐	◐
Firewall Rules	●	●	●	●	●	●
Zero Trust Approach	●	○	○	○	○	○
Machine Learning	●	●	●	●	●	●
Annual Price per User						

ZT cloud solutions enable secure communications to the ZT cloud but do not protect the endpoints. AV/EDR protect the endpoints after malware is downloaded but do not provide ZT communications. Shield Endpoint provides ZT Communications, protects the endpoint, and supports AV/EDR.