



June 2021

INTRODUCTION TO BLASTSHIELD™

BLASTWAVE

BlastWave – The Company

BlastWave is a Company incorporated in the State of Delaware and headquartered in Mountain View, CA. United States of America. Founded in 2017, we have offices located in Dallas, TX. Varberg, Sweden and Edinburgh, UK. We have sales representation in the USA, UK, UAE, Kuwait, Japan, Korea and India. Our Software Development Centre is in Varberg, Sweden.

We are a privately held company with an initial \$8 million investment from private equity investors including Infinera, Rocket Strategies and InfluxData.

The Leadership Team of BlastWave comprises of:

- Tom Sego, Chief Executive Officer
- Charles Constanti, Chief Financial Officer
- Peter Alm, Chief Technology Officer
- Mike Kay, Chief Business Development Officer
- Paul Gracie, Vice President Sales

BlastWave Products

BlastWave's product is known as BlastShield™ which is an in-line IP sub-network (within an open IP network) that creates a zero trust protective shield around critical infrastructure assets and data by rendering them undetectable by modern network scanning and traffic analysis tools. The BlastShield™ Software Defined Perimeter (SDP) network is built based upon a peer-to-peer architecture and can be conveniently deployed supporting any IP capable device, and any protocol used by the automation industry today (TCP, UDP, Modbus, Fieldbus, OPC, etc.). The network can be deployed with zero configuration, as the BlastShield™ nodes automatically discover their peers and self-organize into a secure, resilient IP network.

The BlastShield™ network provides highly granular real-time access control and segmentation from a secure web orchestration platform hosted within the BlastShield™ network. Permission-based access into the BlastShield™ network is delivered through a BlastShield™ gateway access node using a cryptographic, two (2) surface, password-less process that binds remote access privileges to a policy and to the hardware.

The products are deployed as either a:

- Gateway Node – software image running on COTS hardware or VMWare ESXi platform that provides protection for single or multiple assets secured within the BlastShield network.
- BlastShield™ Gateway Agent – a software image hosted on a Linux server
- BlastShield™ Client – software image that can be deployed on Windows/Mac and Linux OS for single user access into the BlastShield™ network. BlastShield™ mobile is available for IOS iPhone and Android.
- BlastShield™ Orchestrator – VM image that can be deployed on premises or in the Cloud providing single point of control and policy management for BlastShield™ clients and Gateway Nodes.

What makes BlastWave Unique?

The BlastWave solution ***resolves the IP transport problem at the IP layer itself*** by hiding the network assets using a software defined no-password solution that cannot be tampered with. This solution is the only meshed overlay IP-based solution in existence today that covers the IP network end-to-end, from one asset to another, across the open IP network.

BlastWave's unique Peer-to Peer meshing capability means that there is no single point of failure in the network. Even if the Orchestrator is down, assets can still talk to each other via their secure connected "tunnel". Orchestrators can be dualled for further resilience.

BlastWave Gateways can run on COT's hardware and does not require expensive custom hardware configurations.

BlastWave Gateways can run on VMWare's ESXi platform and can be used to protect VM assets on the same server and/or the VM Management Interface to provide security and application service on the same physical system.

BlastWave can be deployed seamlessly in existing network configurations with no network changes required. The solution runs as an overlay to existing routing, switching and security policies providing an additional layer of security to that already in place.

BlastWave secures the following connection types:

- User to App
- User to Machine
- Machine to Machine
- Machine to App

BlastWave runs on Public/Private Cloud, hybrid and on-premises networks.

BlastWave Value Proposition

Cybercrime is the greatest threat to every company in the world and one of the biggest problems for mankind, the impact on society is reflected in the numbers. In 2019 cybercrime cost the world \$6 trillion, up from \$3 trillion in 2015. The rate of crime is rising exponentially, fueled by the rapidly growing number of connected devices. No longer is it only PC's and servers connecting, to networks, now we have sensors, cameras, building access devices, vehicle charging stations, streetlamps and traffic lights amongst many other items all offering an attack surface for the determined hacker to breach and launch an attack.

Many security vendors have concentrated on "trace and patch" solutions, which is more akin to closing the stable door after the horse has bolted. BlastWave offers a new paradigm which blocks the attacker before he/she can cause any damage or breach any defenses. Our solution works on the principle of; "if you can't see it, you can't hack it".

By securing devices within a closed BlastShield™ network we prevent unauthorized access. We conform to the CIS Control V7.1 best practices for maintaining security in all three Implementation Groups and the NIST 1.1 framework. Many companies fail to maintain security policies when installing new equipment, whilst this is not malicious intent, it does provide an open door for malicious actors to exploit. BlastShield™ closes that door.

The potential costs of a data breach for a company can be very heavy. The most recent IBM/Ponemon institute study calculated the cost of a breach at \$242 per record and more than \$8 million for an average breach in the USA.

BlastShield™ deploys as a Software as a Service (SaaS) solution, with each endpoint charged as an annual license. An endpoint is identified as any individual device or asset protected behind a BlastShield™ Gateway or any device running a BlastShield™ client or Agent. The cost of our solution for 1,000 protected endpoints is 1/16th of the cost of just one data breach for an average US company. A small price to pay for peace of mind and a restful night's sleep.

Vendor Relationships

BlastWave have established a number of relationships with IOT vendors, Device Manufacturers and industry giants, including but not limited to; Intel, Microsoft, Apple, Axis Communications, CITA Smart Systems, PTC, Schneider Electrics and many others.

Technical Support

BlastWave provides 7/24/365 technical and sales support globally. Access to our support site is granted to customers and partners and support requests can be made via phone, email and web message.

Culture and Sustainability

The culture of BlastWave is one of a shared belief that we can bring security to companies and organizations so they can carry out their legitimate business without fear of external or internal intrusion into their systems and processes, thereby creating a safer environment for them and their customers and partners.

As a software vendor, we take seriously the need to build sustainability into our products and our processes. We constantly review our practices to ensure that we make the minimum impact on the environment and strive to operate with a zero-carbon footprint.

Comparison with other technologies

BlastWave technology US patent application 15/930,005 has been recently approved. BlastWave is a new technological innovation, differing from traditional Virtual Private Network (VPN) solutions and Firewalls. BlastWave's innovation in cyber defense is ideal for IIOT environments especially for Energy suppliers. BlastWave offers unparalleled protection for Operational Technology (OT) networks. **BlastWave** is designed with a unique approach is based on:

- **Invisibility** of Infrastructure, rather than traditional end point isolation (or PSPF w/subnetting), rendering devices undetectable to unauthorized users,
- **Edge-to-Edge** secure mesh connection authenticated to a secure cloud managed policy, rather than merely a network topology map with end point encryption,
- Users are multi-factor authenticated to the **cloud orchestrated** groups and policies, rather than concentrator or gateway switch,
- Zero publicly exposed ports, rather than data flow through a VPN Server open to the internet.
- Overlay deployment for augmented cyber security protection implementation.

The differences between BlastWave and other technology solutions are as follows:

Invisibility

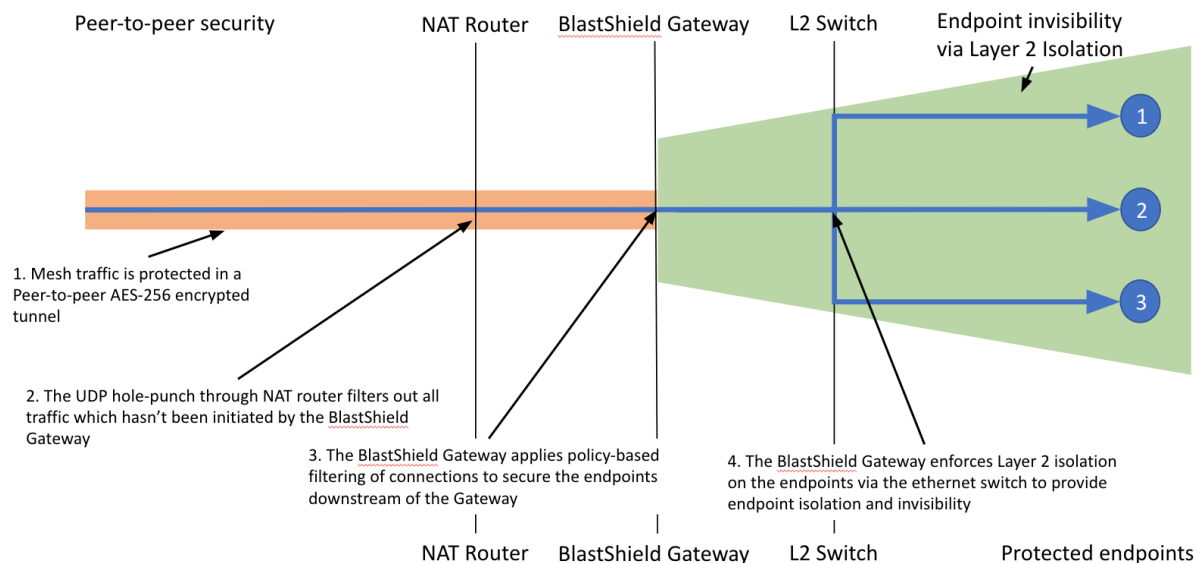
Using NAT (Network address Translation) to hide IP addresses behind a public IP address has been around for a long time and is widely used to secure addresses and, at the same time, create additional address ranges that are not visible to the public internet. NAT requires that rules are applied to the firewall, switch or router to accept or deny traffic based on various parameters and these are configured from the router, firewall or switch's configuration manager or centralized management system.

By their very nature, the number of parameters that are available for configuration is extensive and this can lead to very complex rule creations that are highly prone to misconfiguration, conflict and human error. Human error caused 90% of cyber data breaches in 2019, according to a [CybSafe](#) analysis of data from the UK [Information Commissioner's Office](#) (ICO). According to the cybersecurity awareness and data analysis firm, nine out of 10 of the 2376 cyber-breaches reported to the ICO last year were caused by mistakes made by end-users. This marked an increase from the previous two years, when respectively, 61% and 87% of cyber-breaches were ascribed to user error.

Whilst using NAT on a firewall protects your private IP addresses, it does not make them invisible. The public address of the firewall is visible, and this is often the first point of attack for a determined hacker. By being able to identify the firewall type, the hacker is able to access

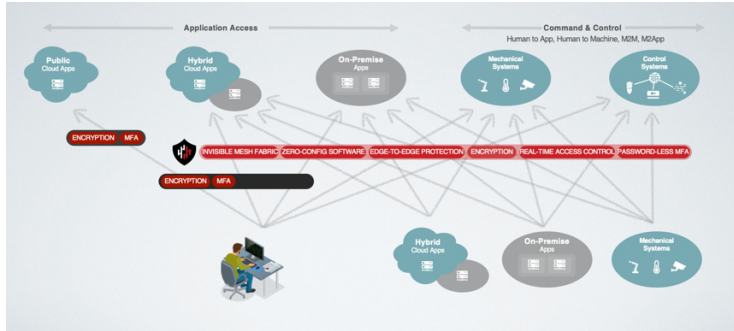
many, freely available, tools to determine which attack vector will offer the best opportunity for success.

A BlastShield™ Gateway **does not offer any publicly available IP address**, neither the protected endpoints behind the gateway nor the gateway itself (as this is secured behind the customers NAT Router). IP scanning of a BlastShield™ network by an unauthorised user shows no identification of any endpoint device, thereby rendering the attacker at a loss as to; what the devices are, if they are functioning, what platforms they are operating on or, indeed, any description of the hardware or mac address of the systems. IP scanning by a user authorized on the network would only offer visibility of the “protected” IP address of the users and assets that he/she/it is authorized to see by policy.



BlastShield™ endpoints can be any network attached device, thus the following connection pairings can be made:

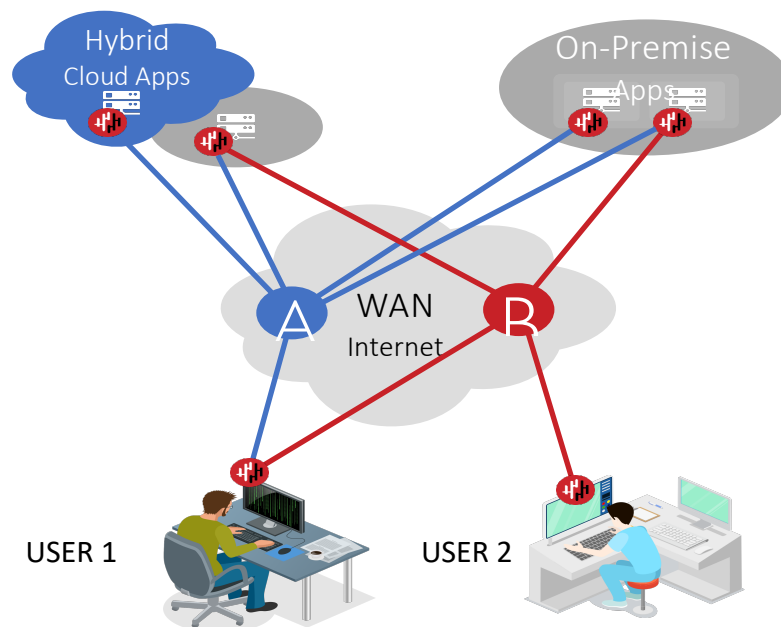
- User to Application
 - User to Machine
 - Machine to Machine
 - Machine to User
 - Machine to Application
 - User to User
- Or any combination in reverse



Simple and Easy Policy Configuration

The configuration of access to any BlastShield™ protected endpoint is greatly simplified, in comparison to using ACL's in a NAT'ed device, as it controlled by a simple to operate policy engine. Policies are configured based on Groups with a "From" and "To" structure that supports bi-directional control.

See example below:



In this scenario we have two users who need to connect to their corporate systems.

User 1 is authorized to connect to Services/App A and Application B, both of which are located both in the corporate Data Centre and in a Hosted Cloud environment.

User 2 is only authorized to connect to Application B in both environments.

Groups would be created to include a) assets/applications b) users

User 1 would be placed in the User Group 1 and User Group 2, User 2 in the User Group 2 only. Application assets associated with Application A would be in the Asset Group A and Application assets associated with Application B would be in Asset Group B

The Policy Configuration for each user would be:

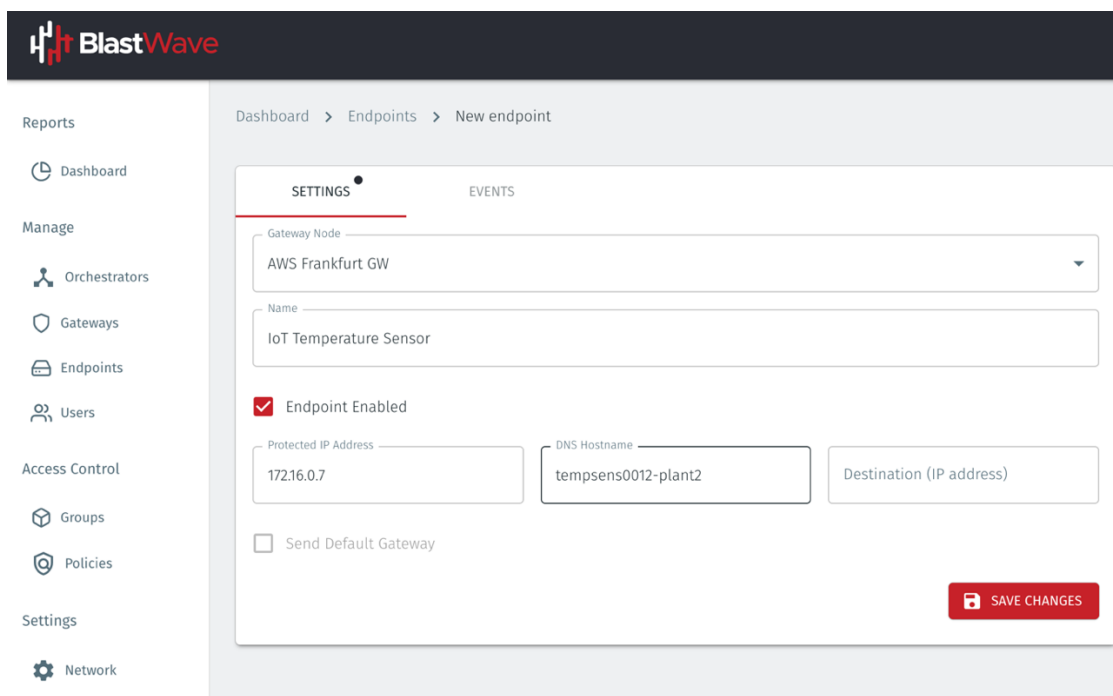
| Policy Name | From | To |
|----------------------|--------------|---------------|
| Application A Access | User Group 1 | Asset Group A |
| Application B Access | User Group 2 | Asset Group B |

In this way User 1 would have visibility and access to all assets whilst User 2 can only see and connect to assets associated with Application B.

Overlay

BlastShield™ is a true overlay solution. Unlike Meraki's and Fortinet's mesh solutions which offer mesh capabilities for their wireless and security products when using their own proprietary Meraki or Fortinet firewall or offer a "fabric" based approach, as long as all of the elements of the fabric are from the same vendor, BlastShield™ is an overlay, independent of any vendor tie-in, operational over all existing packet-based networks, network types, topologies, access and network devices.

BlastShield™ is deployed in minutes and users and endpoints can be provisioned in seconds from the central orchestration systems.



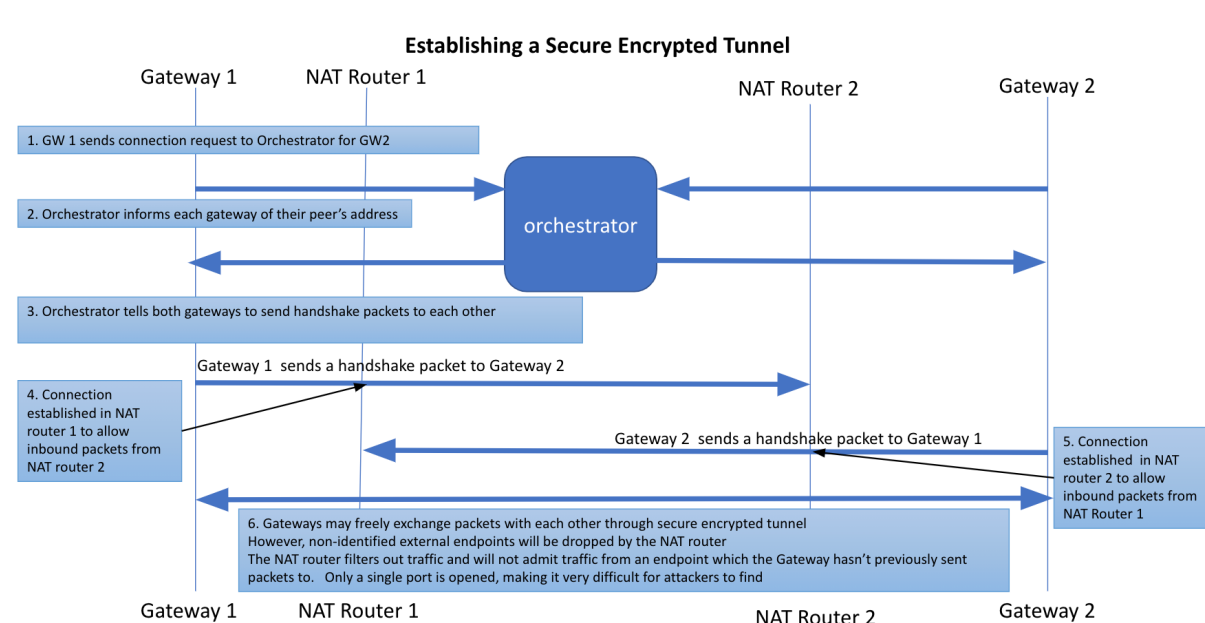
The screenshot displays the BlastWave management interface. On the left is a sidebar with navigation links: Reports, Dashboard, Manage (Orchestrators, Gateways, Endpoints, Users), Access Control (Groups, Policies), and Settings (Network). The main content area shows the breadcrumb 'Dashboard > Endpoints > New endpoint'. Below this is a 'SETTINGS' tab with a dropdown for 'Gateway Node' set to 'AWS Frankfurt GW', a text field for 'Name' containing 'IoT Temperature Sensor', a checked checkbox for 'Endpoint Enabled', and input fields for 'Protected IP Address' (172.16.0.7), 'DNS Hostname' (tempsens0012-plant2), and 'Destination (IP address)'. There is an unchecked checkbox for 'Send Default Gateway' and a red 'SAVE CHANGES' button at the bottom right.

The new device or endpoint is provided with a “protected” IP address which is then provisioned on the network. In two mouse clicks it can be added to a Group and then access is authorized to that Group’s policies. In this way, BlastShield™ provides “Real-Time” provisioning of access, or removal, from the network. No need to wait for lengthy change control procedures, which are prone to human error, resulting in significant cost and time savings and instant access for your users and systems.

Peer-to-Peer Mesh

BlastShield™ is unique in the market, in providing a Peer-to-Peer secure meshing software defined perimeter solution that is self-organizing and requires zero configuration. When an endpoint requests connectivity to another endpoint, the Orchestrator instructs both gateways and endpoints to form a military grade secure encrypted tunnel, using AES 256/Elliptical Curves encryption. Once the tunnel has been established data is exchanged in line with the policy.

For example, an HMI (Human Machine Interface/Workstation) may request data from a PLC that is gathering data from connected sensors and the PLC will respond. However, if the policy is set, such that the PLC may not initiate a session with the HMI or other unauthorized assets, access will be denied, and no tunnel will be established.



The Orchestrator is only required to set up a tunnel if there are no active sessions currently running or within one hour of the last active session. Unlike traditional SSL VPN's or Cisco's Secure Internet Gateway, the BlastShield™ mesh solution ensures that there is no single point of convergence that all traffic has to flow through, removing a bottleneck and a single point of failure.

Deployment Options

BlastShield™ deploys as software, it is extremely lightweight, taking up less than 40 Mb of memory. The OS is hardened to offer the minimum attack surface possible and is available on the following platforms:

- **BlastShield™ Orchestrator**
 - **Cloud**
Amazon Web Services,
Microsoft Azure*,
Google Cloud Platform*
 - **On Premises**
Virtual - VMWare ESXi 6.0 and above
- **BlastShield™ Gateway**
 - **Cloud**
Amazon Web Services,
Microsoft Azure*,
Google Cloud Platform*
 - **On Premises**
 - Virtual – VMWare ESXi 6.0 and above
 - Dedicated – COTS x86 running AES-NI with 2 x NIC cards
- **BlastShield™ Agent**
 - **Linux**
CentOS7 and CentOS8
Ubuntu 16.04 and 18.04
- **BlastShield™ Client**
 - Windows 10 and above
 - MacOS 10.14 and above
 - Linux
 - iOS 12.0 and above*
 - Android 6.0 and above*

*Microsoft Azure and Google Cloud Platform available on demand.

COST BENEFITS

BlastShield™ can also provide cost savings against existing technologies. The most obvious of these is the removal of an existing VPN Gateway and VPN Client licenses. For example, a Cisco ASA VPN Server with 250 clients will cost around \$25,000 plus licenses and support. However, that does not really give you peace of mind, nor a truly secure solution. A simple check on CVE shows there are at least 18 known [vulnerabilities in the Cisco VPN](#) client code and many other vendors have even greater numbers of issues. In addition to that, a VPN server provides an

encrypted tunnel between the VPN server and the client, all on-network connections are in the clear, providing lateral movement for any attacker who compromises a remote user.

With BlastShield™ all connections are encrypted with military grade AES-256 encryption Peer-2-Peer and edge to edge, fully restricting lateral movement anywhere on the network, inside or out.

To add MFA (Multi Factor Authentication), most VPN vendors will charge for the MFA client. For Fortinet's FortiToken, 200 tokens cost \$8,300 plus the cost of the FortiGate firewall and VPN licenses.

With BlastShield™, biometric password-less MFA is free, we also offer third party integration to existing or alternate 2FA and MFA services such as Yubikey's, and FIDO-2 compliant tokens or on modern next generation PC services such as [Shayype](#).

Further cost savings can be made through micro-segmentation, effectively every endpoint on the BlastShield™ protected network has a micro identity-based firewall in front of it, eliminating the need for additional firewalls on the network. This also reduces the complexity of firewall rules, a cost that is often forgotten when calculating RoI. It is estimated that the average enterprise firewall has over 100 rules applied. Configuring new rules that don't contradict previous rules can be difficult and time consuming, it also leads to human error and which, according to the UK Information Commissioner's Office (ICO) was the cause of around 90% of data breaches in 2019.

BlastShield™ has simplified the rules engine into simple identity-based policies of "to" and "from" which are bi-directional, eliminating one of the attackers' key requirements, the exfiltration of data. A BlastShield™ policy can ensure that a server that is not meant to initiate a connection to the internet, cannot do so. If users of SolarWinds or Microsoft Exchange servers hacked by Hafnium, had BlastShield™ in place, they would never have been compromised.

SUMMARY

In summary, BlastShield™ from BlastWave provides the optimum Secure Software Defined Perimeter for all of your assets. The benefits are:

- Deploys in minutes
- Deploys as software on Virtual Machines, as a Host Agent or on a COTS x86 server of the customer's choice
- Deploys as a client application on Windows, Mac, Linux, iPhone and Android* with secure Multi Factor Password-less Authentication
- Supports Mobile biometrics or FIDO-2 compliant authorization for ease of use
- Creates military grade secure encrypted edge-to-edge transport for all data in transit
- Deploys as an overlay with no restrictions or changes necessary on the existing underlay network
- Deploys as a mesh fabric with no single point of convergence or traffic bottleneck
- Offers split tunnel functionality to improve performance of non-private connections to public services
- Renders all protected assets as INVISIBLE from both unauthorized external and internal attack or access
- Offers simple identity-based policy management for control and access from a single pain of glass without the need to change any existing routing or firewall rules
- Provides real-time access and control for internal, remote and third-party access to the protected network.
- Can be deployed as a direct SSL VPN replacement with easy migration to a full Software Defined Perimeter networking solution for all network attached assets

For further information, or a demonstration, please contact us at www.blastwave.io or email us at doug@blastwave.io or call (415) 310-0810

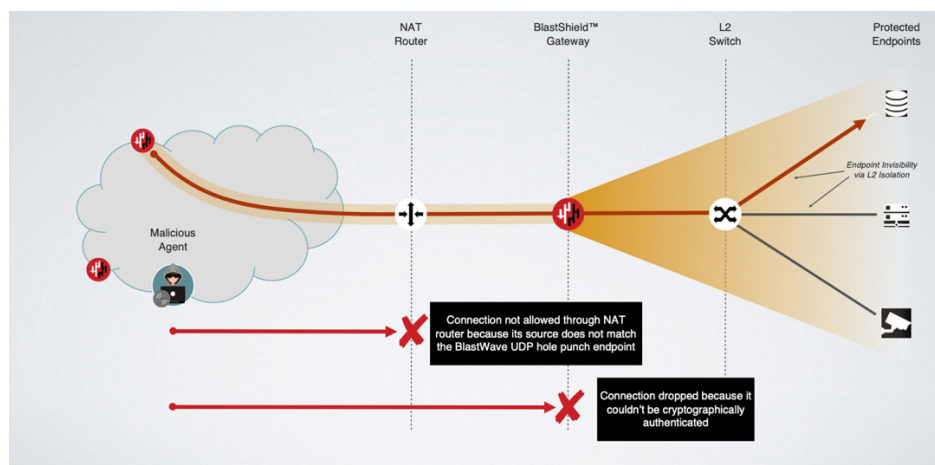
Exhibit A: Technical Explanation of BlastWave's Solution Addressing the Existential Threat of Hafnium Attack.

It is now suspected that over 60,000 companies, central government departments and state government organizations, have been infected by malware, placed there by a foreign Advanced Persistent Threat (APT) group, known as Hafnium.

The attackers have used vulnerabilities in the Microsoft Exchange Server code to insert malware which allows them to gain administrative access to the Exchange Servers, thereby allowing them to mirror email messages, create unauthorized users and generally access all of the Exchange Servers administrative functions. We also understand that they have created the ability to access the servers again in the future, at a time of their choosing.

Our patent pending technology has been designed to allow only authorized users to access critical systems, based on a policy-based identity management solution that runs as an overlay to existing networks and cyber defenses. Without going into too many details, authorized users are required to authenticate themselves when accessing the network using password-less multi-factor authentication. This can be carried out by using facial recognition or thumb print on the users own mobile phone, or by any FIDO2 compliant device issued to the user.

Once connected to the network, BlastWave's Orchestration system sends authorization messages to the target server/service and to the user device, granting them the authority to set up a secure, military grade, encrypted tunnel between both endpoints. Without this biometric identification and previously granted policy, access is denied to users trying to access the service. This prevents Hafnium or anyone else from being able to establish a remote connection to the Exchange Servers. BlastShield™ policy ensures that the remote user trying to establish administration rights to the server is denied by our overlay policy manager. Without BlastShield™ credentials, the attacker is blocked from any connection.

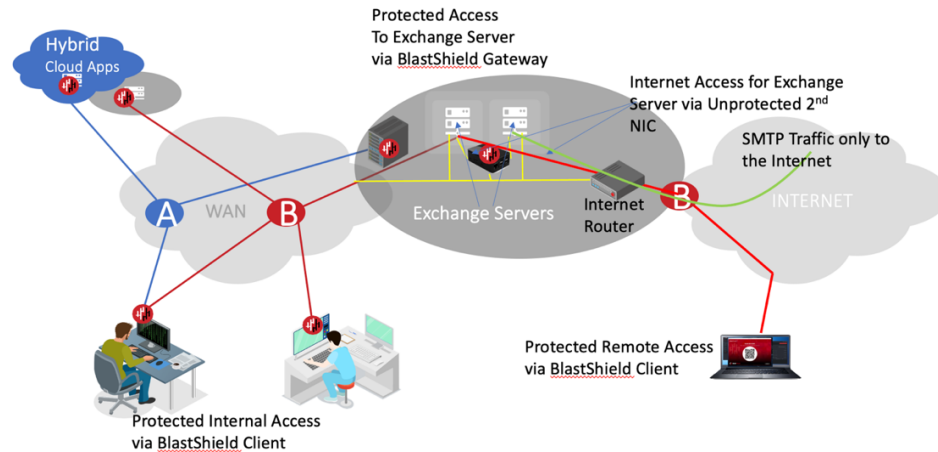


Our solution has been designed with simplicity in mind and deploys as an overlay to the existing network infrastructure. It is also deployed solely as software, either directly on to a server or a user's PC or laptop. In cases where the software instance cannot be installed directly, we can install our software on to any X86 server to act as a secure gateway in front of your critical asset.

The solution can be set up within a matter of hours depending on network complexity. Users need no expert computing knowledge to be able to access and use the BlastWave solution. For companies and organizations who have already been infected, deployment will immediately stop the exfiltration of data from their systems. For those that have not been infected, we will stop the initial connection made to the Exchange Server by the APT

Group. It should be noted that other APT Groups in Russia and Iran are suspected of making use of these vulnerabilities, so the extent of this breach is unknown.

Shown below, is a diagram explaining how BlastWave's BlastShield™ product can protect Microsoft Exchange Servers from the Hafnium attack.



Internal users inside the company's network will access the Exchange Server using their secure encrypted connection, only authorized users by policy will be able to connect.

Remote users will access in the same way and will have to provide their biometric information on connecting to the network, otherwise all protected systems will appear "invisible" to them. As we use biometrics, no usernames or passwords can be stolen, no replay attacks can be launched and attackers have to access the user's laptop, mobile device or FIDO2 key and their biometric profile in order to successfully connect, so theft of a user's phone or laptop alone does not enable the thief to gain access.

BlastWave is able to set up a demonstration of our solution in a matter of minutes. We make our solution available for testing and scrutinization by any government department, nominated penetration tester or test labs that you trust to provide advice on security solutions.

Our solution is provided as a Software as a Service license and companies can take action immediately to protect their Exchange Servers by downloading our clients and host/gateway instances from the BlastWave download servers. Access can be provided to our Support Portal where customers can find videos and tutorials that explain how easy it is to set up a BlastShield™ protected network that will make their critical assets and services "invisible" to APT attackers from Day 1. In this way Government Departments and Agencies, along with key critical private companies and contractors can become protected from Hafnium and the many other APT organizations.