Data Sheet

PrecisionAccess

Trusted Access Control

Defeats Cyber Attacks

- **Credential Theft:** Integrated MFA defeats credential theft.
- **Server Exploitation:** Server isolation defeats server exploitation.
- **Compromised PC:** Trust assessment blocks access to enterprise apps from compromised PCs.
- **Man-in-the-Middle:** Mutual TLS, pinned certificates, and an unalterable encryption suite defeat man-in-the-middle attacks.

Transparent UX

- **Transparent MFA:** No phone to respond to. No token to enter. It defeats credential theft and it is transparent to the user.
- **Always On:** Sleep a computer. Wake it up, and it's connected – after another round of transparent MFA.

Total Visibility

- **Apps, Users, Devices:** See which users on which devices are accessing which applications at what time and from where.
- **Posture, Vulnerabilities, and Threats:** Determine the trust of each device before allowing it to access business-critical apps.

PrecisionAccess provides enterprises complete control over which users on which devices can connect to which applications, regardless of where the users and applications are located.

PrecisionAccess sits between the users and the enterprise apps to isolate the applications from unauthorized users and untrusted devices.

Trusted SaaS Access

Office 365 is vulnerable! It is vulnerable to credential theft and the compromised PCs of authorized users. Without multifactor authentication (MFA), adversaries *will* compromise your users. But MFA doesn't stop an adversary that has compromised the PC of an authorized user. PrecisionAccess defeats credential theft with an MFA that is transparent to users and defeats compromised PCs with Trust Assessment.

Next Gen Remote Access

Today's remote access VPN provides too much access. The remote users are "on the LAN." They use the DHCP and DNS of the LAN. They have access to many, if not all, of the applications. And they have access to switches, routers, and security products that make up the infrastructure. PrecisionAccess enables remote access but only provides access to authorized applications.

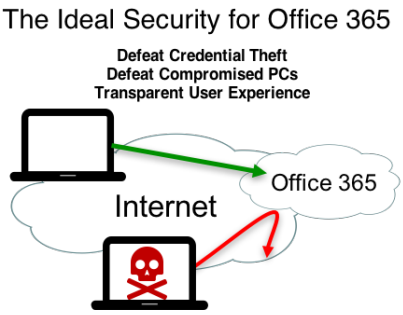
Zero Trust Network

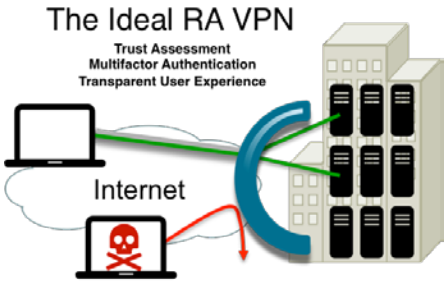
Due to phishing and other social engineering attacks, one should assume that the internal network is just as insecure as the Internet. Therefore, the internal network should be segmented. Segmentation begins with client-to-server segmentation. PrecisionAccess completely isolates servers from unauthorized users.

Features and Benefits of PrecisionAccess

The Ideal Security for Office 365

It is easy for an adversary to harvest a large number of employee email addresses and to brute force crack some of their passwords. However, it is painful to employees to use traditional MFA. For Office 365, MFA must be transparent to users. But MFA does not stop an adversary that has compromised a PC and added a backdoor to it. To secure Office 365 the security product must defeat credential theft. it must defeat a compromised PC. And it must be transparent to the user. PrecisionAccess does this.



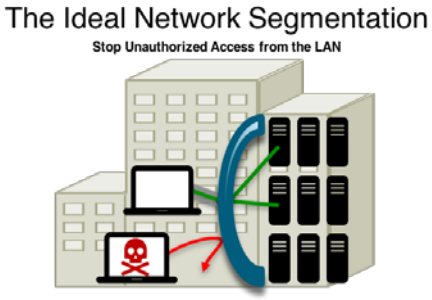


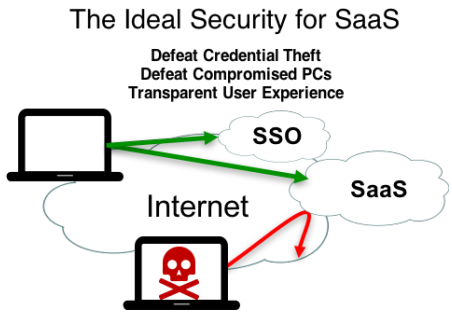
The Ideal Remote Access VPN

The ideal Remote Access VPN combines the encrypted tunnels and MFA of the traditional Remote Access VPN, but makes the remote access more secure by operating as an application-layer tunnel such that the user is not "on the LAN." The result is that the user can access authorized applications, but nothing else. Then, PrecisionAccess adds "always on" and "transparent MFA" to create a transparent User Experience (UX). PrecisionAccess does this.

The Ideal Network Segmentation

Most enterprises suffer from excessively flat networks. Years ago, it made it easy to provide employees access to all of the enterprise applications. Today, it also makes it easy for adversaries to access all of the enterprise applications. Access for the adversary begins on the LAN: at a branch office, via Wi-Fi, via remote access, or via a compromised PC. Therefore, the ideal network segmentation must segment the LAN from the Data Center. PrecisionAccess does this.



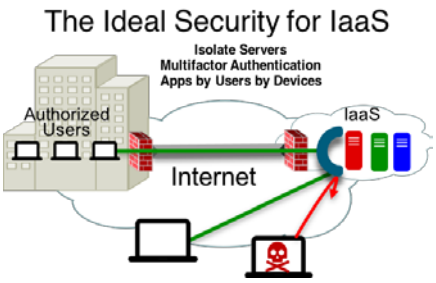


The Ideal Security for SaaS

Today's enterprise SaaS applications implement Single Sign-On (SSO) via SAML and WS-Fed. If an adversary obtains access to the credentials of an authorized user, the adversary has access to all SSO applications. Similarly, if an adversary compromises the PC of an authorized user, the adversary has access to all SaaS application. The ideal security for SaaS defeats both of these attacks, AND provides transparent access to the users. PrecisionAccess does this.

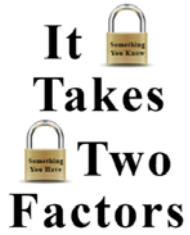
The Ideal Security for IaaS

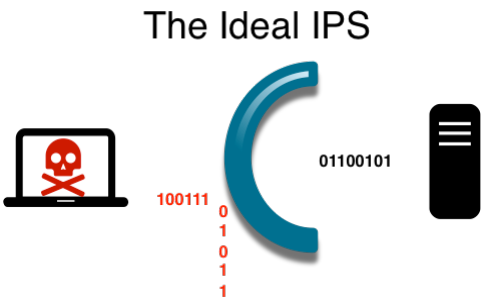
For DevSecOps, it's secure access via a jump box (Bastian host). For Lift 'n Shift, it's secure access for admins and users. Both begin with isolating the servers from all unauthorized users. Then, both require MFA for user authentication. Ideally, it would be nice to know which users accessed which applications and on which devices. PrecisionAccess does this.



The Ideal MFA

Credential theft is a major concern today because passwords are so easy to steal and so easy to crack. Fortunately, the MultiFactor Authentication (MFA) that is an integral component of PrecisionAccess completely defeats password theft and password cracking. But just defeating those attacks is not enough. Rather, MFA must also be easy to use, easy to deploy securely, easy to add to existing applications, and proven to work. PrecisionAccess does this.



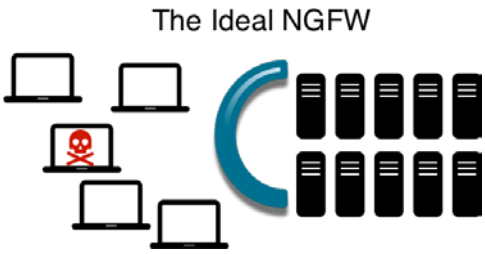


The Ideal IPS

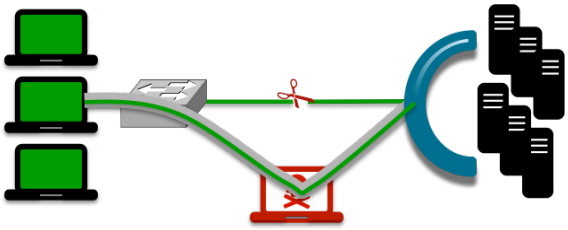
The ideal intrusion Protection System (IPS) has 100% true positives (it blocks all attacks on servers and infrastructure). It has 0% false negatives (it doesn't miss any attacks). And it has 0% false positives (it doesn't block anything that is not an attack). In addition, when new attacks are discovered it automatically defends against them – even 0-day attacks. And: it works for all applications and protocols; it operates at line rate so it doesn't DoS the network; it's easy to add to all applications; and it's cost effective – both CapEx and Opex. PrecisionAccess does this.

The Ideal NGFW

The ideal Intrusion Next Generation Firewall (NGFW) is a stateful firewall that is user-aware. It knows who every user is on every device. It knows the user's location and the amount of data each user downloads from each application. And it knows each device's posture, vulnerabilities, and threats. In addition, the ideal NGFW is application-aware. It uses the principle of least privilege to only allow connectivity from authorized users to authorized applications. Furthermore, the ideal NGFW integrates a remote access VPN gateway and IPS with the firewall. PrecisionAccess does this.



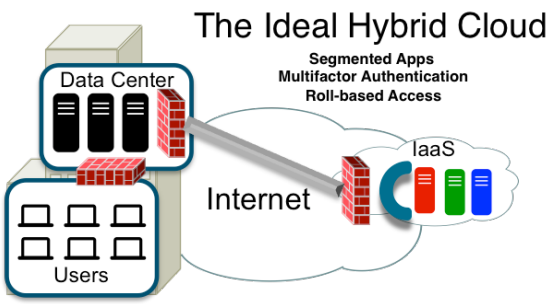
The Ideal Man-in-the-Middle Defense

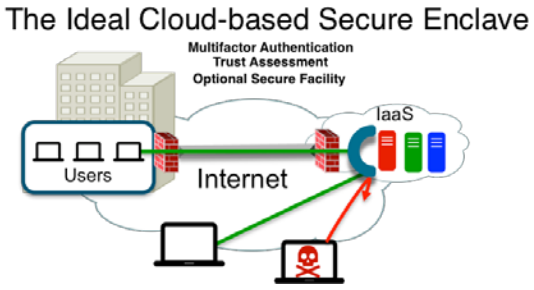


There are two main components to the man-in-the-middle attack. First, the adversary intercepts communication from the victim and relays it to the server. Second, the adversary obtains cleartext of the communication between the victim and the server. It's not feasible to prevent the former. To prevent the latter, one must encrypt unencrypted traffic and prevent the decryption of encrypted traffic. PrecisionAccess does this.

The Ideal Hybrid Cloud

The ideal Hybrid Cloud enables enterprises to extend their data center into an IaaS environment AND allows them to segment the applications in the cloud instead of extending their internal big flat network into the cloud. In addition, the ideal Hybrid Cloud automatically requires MFA for all applications that get developed and/or moved to the cloud. Finally, it applies role-based access to those applications such that the segmented applications can only be reached by authorized users. PrecisionAccess does this.

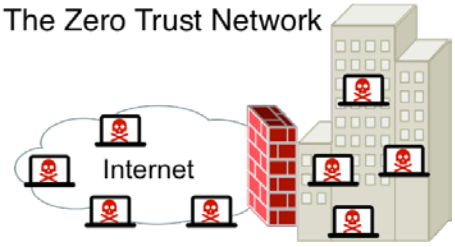




The Ideal Secure Enclave

A Cloud-based Secure Enclave is a virtual container within a public cloud with no unauthorized connectivity outside the container and no exposure of internal IP addresses or infrastructure. Typically, it's a self-contained Virtual Private Cloud (VPC) with role-based access from the Internet. The ideal ones include MFA and a trust assessment of the devices of authorized users, such that risky devices do not receive access. Some secure enclaves require access from a controlled facility, others do not. PrecisionAccess does this.

The Ideal Solution to the Zero Trust Network



Adversaries can infiltrate the internal enterprise network in many ways, and, once inside, they can often directly connect to just about every server anywhere in the network. Therefore, astute security practitioners realize that the internal network is no more trustworthy than the Internet. This concept is referred to as the "Zero Trust Network." After arriving at this realization, security architects segment everything – removing paths of connectivity from everything, and then creating connectivity only where it is needed. Since the adversary's first vector of attack into the internal network is either the stolen credentials of an authorized user or the compromise PC of a device on the network, segmenting users from applications is the first order of business. PrecisionAccess does this.

The Ideal NAC

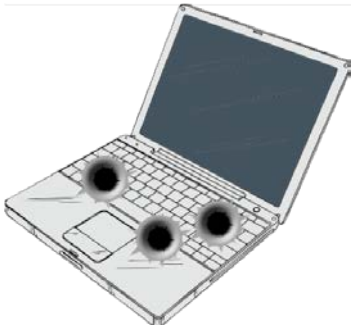
The ideal Network Access Control (NAC) isolates unauthorized devices from enterprise applications and provides deep visibility into authorized endpoints. But, the ideal NAC also provides fine-grained access such that only authorized users on trusted devices can connect to enterprise applications, and, very importantly, it does not require any upgrades to the networking infrastructure. Finally, the ideal NAC applies equally well to the cloud as it does to the enterprise data center. PrecisionAccess does this.

The Ideal Posture Assessment

The ideal Posture Assessment goes way beyond “is AV running” and “are the AV signatures up to date.” The ideal Posture Assessment distinguishes managed from unmanaged devices. It maintains a list of every software application that exists on every device and which applications are running – a list that can be searched across all endpoints. It knows the state of the firewall and disk encryption, and it knows the values of each of the registry entries. PrecisionAccess does this.

The Ideal Vulnerability Assessment

The ideal Vulnerability Assessment compares every software application on every device against the database of Common Vulnerabilities and Exposures (CVE), and uses the Common Vulnerability Scoring System (CVSS) to assign a priority to patching the vulnerability. And the ideal Vulnerability Assessment goes beyond just software vulnerabilities to look at open ports and what processes are running on those open ports. And it goes beyond that to look for a number of other known configuration errors. PrecisionAccess does this.



The Ideal Threat Assessment

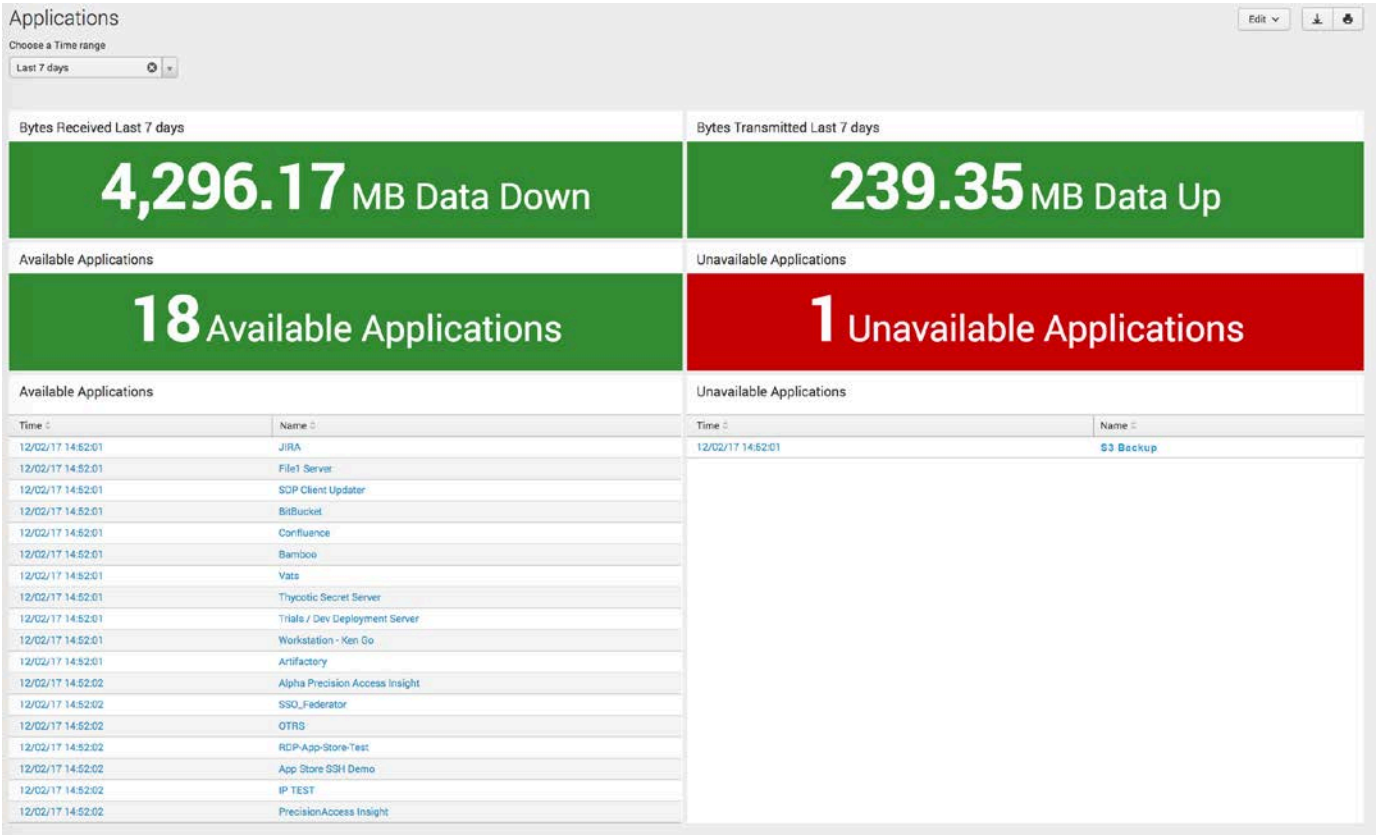
The ideal Threat Assessment continuously monitors the behavior of the device – looking for any of the behaviors indicated in the Mitre Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) matrix, and, then, rating those behaviors to the probability that the PC has been compromised. PrecisionAccess does this.

PrecisionAccess Insight

PrecisionAccess Insight™ (PA Insight) provides actionable, real-time visibility into the protected applications, users, and devices. It collects JSON objects from PrecisionAccess components and processes them in a Splunk application. Vidder provides the PA Insight Splunk application, and the Splunk server free with each PrecisionAccess installation. When discussing the maps, graphs, and tables of PA Insight, they are collectively referred to as individual "panels," and a "page" consists of multiple panels. Below, you see a small sample of the well over 100 panels of that application.

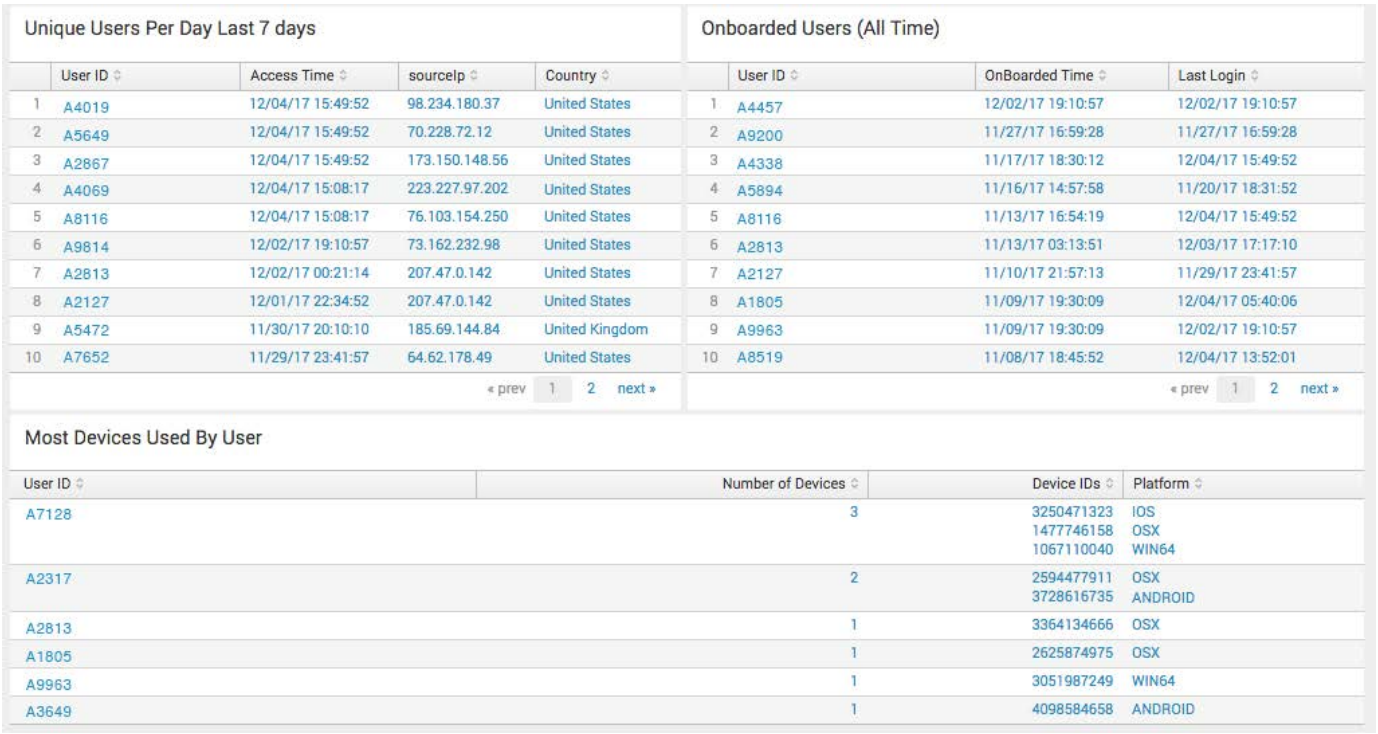
Applications Page

The Applications page provides general information about all protected applications – including the total amount of bandwidth consumed over a selectable time period and whether each application is available or not. Clicking on the name of an application provides additional information about that application including the bandwidth consumed by it and the number, identity, and geographic location of each user accessing it.



Users Page

The Users page, combined with the subsequent drill down of a single user, provides information about each user's interaction with the protected applications and information about the devices they have onboarded to PrecisionAccess. No Personally Identifiable Information is collected. Below, you see who was an active PrecisionAccess user within a selectable time period, the user IDs of all users who have accessed the protected applications, and the number of devices each user has onboarded (note, a max number of devices per user exists).



Unique Users Per Day Last 7 days

	User ID	Access Time	sourceIp	Country
1	A4019	12/04/17 15:49:52	98.234.180.37	United States
2	A5649	12/04/17 15:49:52	70.228.72.12	United States
3	A2867	12/04/17 15:49:52	173.150.148.56	United States
4	A4069	12/04/17 15:08:17	223.227.97.202	United States
5	A8116	12/04/17 15:08:17	76.103.154.250	United States
6	A9814	12/02/17 19:10:57	73.162.232.98	United States
7	A2813	12/02/17 00:21:14	207.47.0.142	United States
8	A2127	12/01/17 22:34:52	207.47.0.142	United States
9	A5472	11/30/17 20:10:10	185.69.144.84	United Kingdom
10	A7652	11/29/17 23:41:57	64.62.178.49	United States

« prev 1 2 next »

Onboarded Users (All Time)

	User ID	OnBoarded Time	Last Login
1	A4457	12/02/17 19:10:57	12/02/17 19:10:57
2	A9200	11/27/17 16:59:28	11/27/17 16:59:28
3	A4338	11/17/17 18:30:12	12/04/17 15:49:52
4	A5894	11/16/17 14:57:58	11/20/17 18:31:52
5	A8116	11/13/17 16:54:19	12/04/17 15:49:52
6	A2813	11/13/17 03:13:51	12/03/17 17:17:10
7	A2127	11/10/17 21:57:13	11/29/17 23:41:57
8	A1805	11/09/17 19:30:09	12/04/17 05:40:06
9	A9963	11/09/17 19:30:09	12/02/17 19:10:57
10	A8519	11/08/17 18:45:52	12/04/17 13:52:01

« prev 1 2 next »

Most Devices Used By User

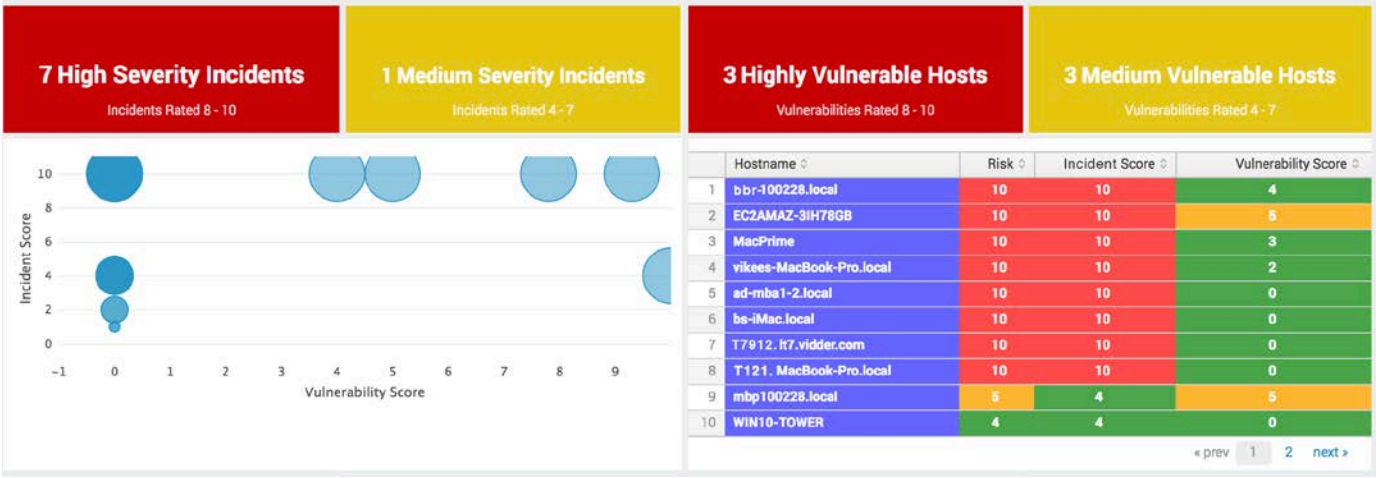
User ID	Number of Devices	Device IDs	Platform
A7128	3	3250471323 1477746158 1067110040	IOS OSX WIN64
A2317	2	2594477911 3728616735	OSX ANDROID
A2813	1	3364134666	OSX
A1805	1	2625874975	OSX
A9963	1	3051987249	WIN64
A3649	1	4098584658	ANDROID

Devices Page

The Devices page provides a great deal of information about the devices that have been onboarded. They are listed by OS, by by PrecisionAccess version, by location, and by user. And there are graphs to show changes in those attributes over time. In addition, there are 3 more pages describing the device. The Posture page provides a great deal of information about the software installed, and the processes running, on each device. The Vulnerabilities page identifies every known vulnerability of every application of every device. And the Incidents page details device behavior anomalies.

Threats Page

The Threats page summarizes the Posture, Vulnerabilities, and Incidents pages.

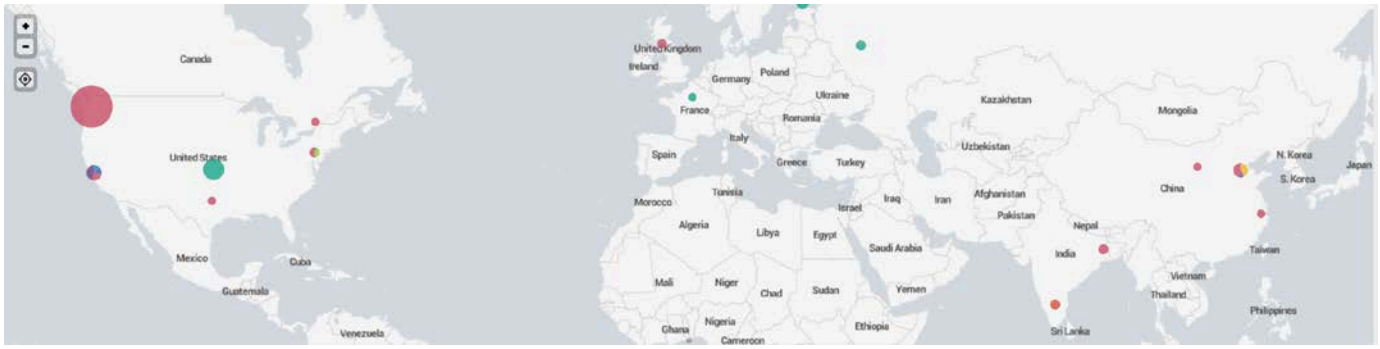


	Hostname	Risk	Incident Score	Vulnerability Score
1	bbr-100228.local	10	10	4
2	EC2AMAZ-3IH78GB	10	10	5
3	MacPrime	10	10	3
4	vikees-MacBook-Pro.local	10	10	2
5	ad-mba1-2.local	10	10	0
6	bs-iMac.local	10	10	0
7	T7912.lt7.vidder.com	10	10	0
8	T121. MacBook-Pro.local	10	10	0
9	mbp100228.local	5	4	5
10	WIN10-TOWER	4	4	0

« prev 1 2 next »

Attacks on PrecisionAccess

The attack vector of PrecisionAccess is very small. Gateways act like dynamic firewalls – starting with just one firewall rule, "Deny All." In addition, the IP addresses of the Gateways are provided to Clients by the Controllers – the addresses do not exist in DNS. Therefore, it is infeasible to find them by scanning the Internet. One would have to know ahead of time the location of the Gateways to even attempt to connect to them. But any attempt would be blocked with no returning information (i.e., no SYN-ACK or RST). The Controllers, however, are reachable from a TCP/IP connection point of view and will reply with a SYN-ACK. But, if a valid Single Packet Authorization (SPA) is not received almost immediately, they will drop the connection – they do not wait for TCP timeout, nor do they respond to any packet other than a valid SPA. And they record all failed attempts.



Above, you see the origins of the failed SPA attempts, where the size of the circle represents the number of failed attempts from that location. For the most part, the circles just represent scans of the Internet, but big circles may represent a determined adversary probing the corporate IP space. Therefore, this panel may provide important threat intel of an adversary performing reconnaissance. A set of drill down panels are provided to further investigate.

Summary of Features and Benefits of PrecisionAccess

Features	Benefits
Integrated MFA	Defeats credential theft
Server isolation	Defeats server exploitation
Trust assessment	Defeats compromised PCs
Mutual TLS, pinned certificates, unalterable encryption suite	Defeats man-in-the-middle attacks
Transparent MFA	No phone to respond to, no token to enter
Always on	Sleep a computer, wake it up, it's connected
PA Insight	Total visibility of apps, users, and devices

CONTACT US

910 E. Hamilton Ave. #410
Campbell, CA 95008

Phone: 408.418.0440
Fax: 408.706.5590

Information: info@vidder.com
Sales sales@vidder.com
EMEA Sales: emea@vidder.com

PrecisionAccess provides trusted access control across internal networks, clouds, and external users. Security is enhanced by continually ensuring that only trusted devices used by strongly authenticated users can access enterprise applications. Cost and complexity are reduced for IT via a single layer of software-defined enforcement. Complexity is reduced for users via a transparent user experience in the office and over the Internet.