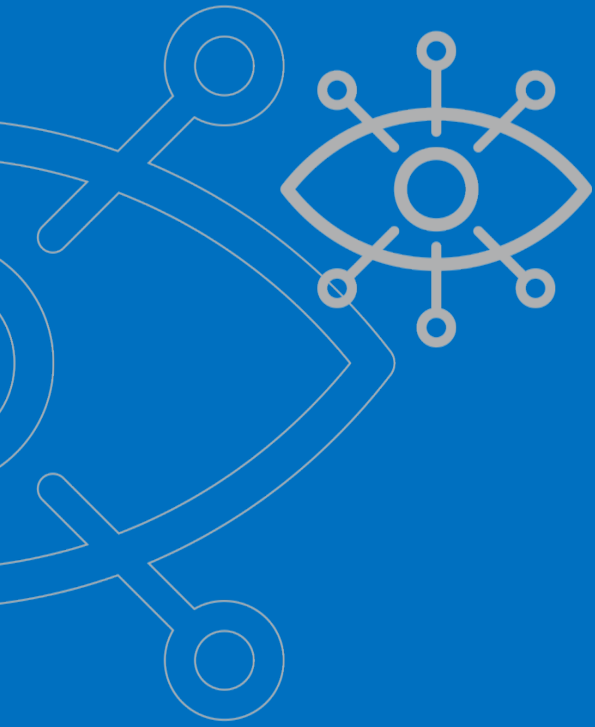
Visibility

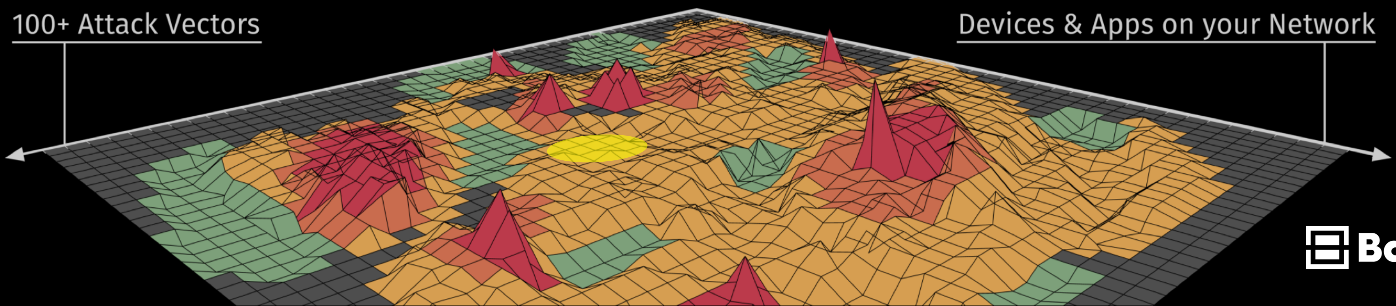
CYBERSECURITY'S MISSING LINK AND SUCCESS FACTOR



Visibility is cybersecurity's missing link

You know that poor cybersecurity posture puts your enterprise at risk but unfortunately, you only have a vague understanding of your massive, multidimensional attack surface.

Your extended network has a bewildering number of assets and each can be attacked in hundreds of ways. The pace of business and technology is constantly threatening to outpace your ability to secure your infrastructure – and without visibility, you're flying blind.



Balbix®

In spite of millions of dollars of annual security spending, most enterprises are just one bad click, one reused password, or a single unpatched system away from a cybersecurity disaster.

Visibility is a critical success factor too

Enterprise assets change constantly, with devices being added and retired, physical machines migrating to virtual, and various stakeholders installing and updating software (with or without approval).

Because the enterprise network is only as secure as its weakest link, gaining real-time visibility into your attack surface and breach risk is both a challenge and one of your most critical success factors.

Visibility needs to be comprehensive and continuous, extending to all types of assets and security issues across an increasingly complex landscape. Remember – you can’t manage what you can’t see.

Challenges with asset inventory

Maintaining an up-to-date enterprise inventory system is very challenging. The set of assets in the enterprise changes constantly with devices being added and retired, physical machines migrating to virtual and various stakeholders constantly installing and updating software (with or without approval). Inaccurate inventory makes managing compliance and cyber-risk very difficult.

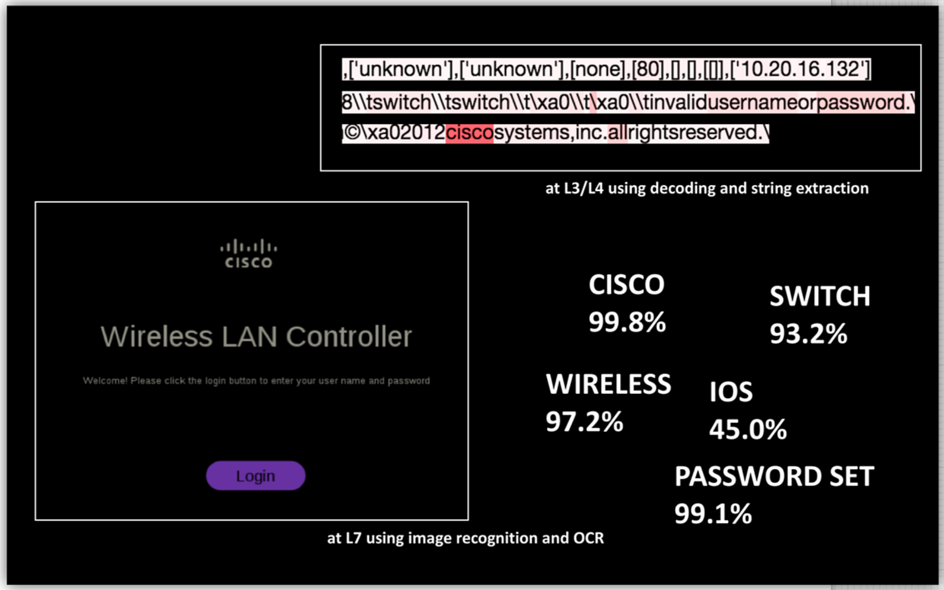
An outdated inventory is also frustrating and impedes the velocity of business. Unfortunately, applying manual effort to keep inventory updated is time and resource intensive and does not work at scale. Enterprise security teams don’t often control all assets, which makes the task of understanding assets and gathering insights about them even more difficult.

Traditional inventory tools typically track only managed assets. Non-traditional assets like IoTs are either left undiscovered or partially tracked by a motley collection of specialized tools, one for each asset category.

Challenges with asset inventory

We know that the best human experts can put together an accurate picture of the type and category of a device on your network by manually looking at a broad variety of data sources.

For example, from Layer 3 packet analysis, an expert may be able to extract media access control (MAC) organizational unit (OU) information that indicates that a device is a Cisco device.



```
,['unknown'],['unknown'],[none],[80],[],[],[[]],['10.20.16.132']
8\\tswitch\\tswitch\\t\xa0\\t\xa0\\tinvalidusernameorpassword.\
|©\xa02012ciscosystems,inc.allrightsreserved.\
```

at L3/L4 using decoding and string extraction
cisco
Wireless LAN Controller
Welcome! Please click the login button to enter your user name and password
Login
at L7 using image recognition and OCR
CISCO 99.8%
SWITCH 93.2%
WIRELESS 97.2%
IOS 45.0%
PASSWORD SET 99.1%

At Layer 4, they might see transport headers and protocol behavior that are consistent with the device being a switch with a management portal available at ports 80 and 443. From Layer 7 analysis of protocol behavior and a study of artifacts rendered in the web browser, we might be able to say that port 80 does not automatically redirect to port 443, and that the device is a wireless LAN controller made by Cisco. However, relying on humans for this analysis does not scale.

Addressing the problems of inventory with AI

At Balbix, we use AI to mimic this type of intelligent analysis by throwing L3, L4, and L7 data from different vantage points on your network into a sequence-to-sequence deep neural network which discovers, inventories and categorizes all devices, users, and applications. The system is real time, with entities analyzed the second they show up on your extended network.

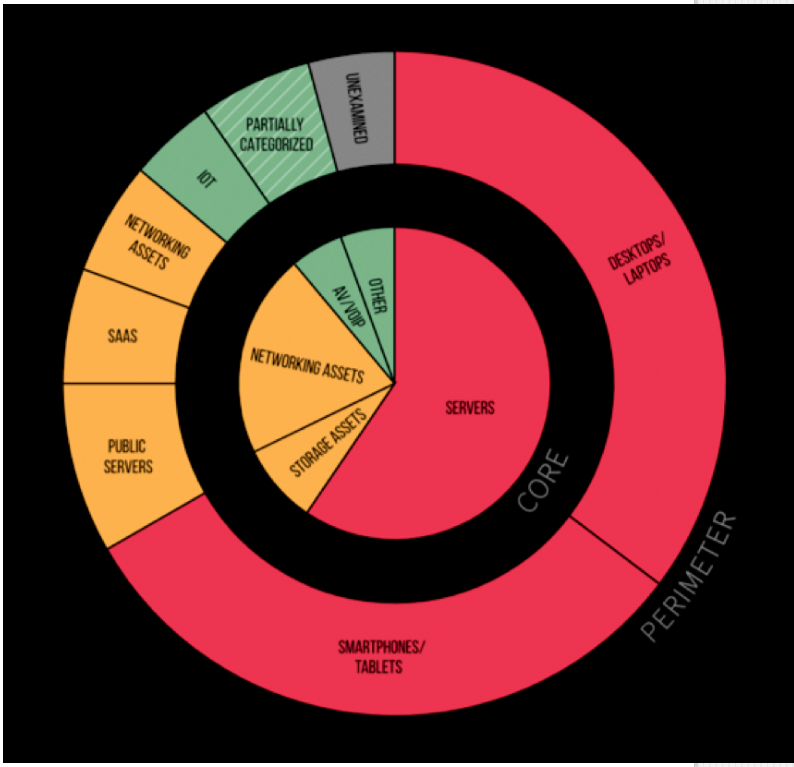
Now consider the challenge of associating users with devices. Typically, you can identify users associated with managed laptops and desktops either by linking them with Kerberos authentication or domain logon sessions of users. However, this approach does not work well for unmanaged bring-your-own devices.

Balbix uses time-domain correlation of Dynamic Host Configuration Protocol (DHCP) lease renewals, beginning-of-day traffic time, on-off times, and timing of Gmail push notifications to different devices to figure out if a smartphone and a laptop/desktop have the same owner.

Use AI to automatically discover and inventory all your assets

Balbix enables enterprises to maintain an accurate and up-to-date inventory of the organization's assets. This includes all devices, apps, and services; managed and unmanaged infrastructure; on-prem and cloud; fixed and mobile; IoT, ICS, etc., and how they are used by your users.

This inventory is available via real-time dashboards and search. Asset are also analyzed across 100+ attack vectors to identify ones that are most likely to be compromised. You can also set up automatic and continuous compliance watchdogs.

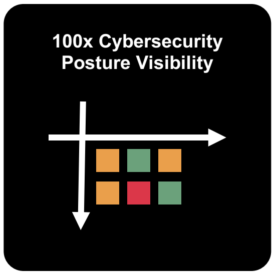


Visibility is the starting point to a strong cybersecurity posture

We have entered an era where cybersecurity is no longer a human-scale problem. There are many complex computations involved in understanding a multidimensional attack surface, and it will always be a moving target.

A robust cybersecurity posture starts with having visibility across all assets and attack vectors, and this needs to be continuous and in real time. It takes a collaboration between humans and innovative AI techniques to get comprehensive visibility into your attack surface and maintain a strong cybersecurity posture.

Click below to learn more



Gain 100x Cybersecurity Posture Visibility

LEARN MORE

Balbix®