Attack Surface Checklist

Modern attack surfaces are constantly increasing in size and complexity. Whenever a new cyber asset is introduced to your environment, new attack vectors are introduced as well.

Use the checklist below to determine which elements of your attack surface are well accounted for and where you may have visibility gaps. Classify each element as follows:

- Known known: Cyber assets that you know are part of your attack surface.
- Known unknown: Cyber assets that you know are part of your attack surface but which you may not have visibility of and/or don't have under management.
- Unknown unknown: Cyber assets that may or may not be part of your attack surface — you don't know.
- n/a: Cyber assets that you know with 100% certainty are not part of your attack surface.

The checklist will keep track of all your responses and collect them on one sheet at the end of this document (p. 11) so you can get a sense for your attack surface at a glance.

Note that certain types of assets may fall under multiple categories (e.g., a device could be considered both a mobile device and an endpoint device). And that's fine! The goal here is to be as thorough as possible — every blind spot you close is one less opportunity for a cyber attacker to infiltrate an environment.

Endpoint devices

Company-issued or employee-owned (BYOD) devices that connect to a network. Mostly include Android, ChromeOS, iOS, Linux, Mac and Windows devices.

Known known	☐
Known unknown	☐
Unknown unknown	☐
n/a	☐

Examples:

- Desktop computers
- Laptops

Management tool(s):

- IT asset discovery
- Modern device management (MDM)
- Unified endpoint management (UEM)

Mobile devices

Company-issued or employee-owned (BYOD) endpoint devices that connect to a network, typically via Wi-Fi, and are designed to be easy to transport. Mostly include Android and iOS devices.

Known known	☐
Known unknown	☐
Unknown unknown	☐
n/a	☐

Examples:

- Smartphones
- Smartwatches
- Tablets

Management tool(s):

- IT asset discovery
- Mobile device management (MDM)
- Modern device management (MDM)

Rugged devices

Mobile devices that have been outfitted to withstand conditions that would damage standard mobile devices, such as those found at construction sites, manufacturing facilities and warehouses. Mostly include Android, iOS and Windows devices.

Known known	☐
Known unknown	☐
Unknown unknown	☐
n/a	☐

Examples:

- Rugged mobile computers
- Rugged tablets
- Rugged wearables

Management tool(s):

- IT asset discovery
- Mobile device management (MDM)
- Modern device management (MDM)

Internet of Things (IoT) devices

Nonstandard endpoint devices outfitted with sensors and software so they can exchange data with other devices and systems over a network or the public internet. Depending on use case, they may also be known as enterprise internet of things (eIoT), extended internet of things (XIoT), industrial internet of things (IIoT) or internet of medical things (IoMT) devices.

Known known	☐
Known unknown	☐
Unknown unknown	☐
n/a	☐

Examples:

- Asset tracking devices (e.g., RFID tags)
- Industrial sensors
- Smart appliances (e.g., toasters, refrigerators, light bulbs)

Management tool(s):

- IT asset discovery
- Modern device management (MDM)
- Purpose-built IoT security tools (varied)
- Unified endpoint management (UEM)

Cyber-physical systems (CPS)

Systems that link computational and physical resources that coordinate closely to carry out their tasks.

Known known	☐
Known unknown	☐
Unknown unknown	☐
n/a	☐

Examples:

- Building management systems (BMS)
- Industrial control systems (ICS)
- Operational technology (OT)
- Robotics systems

Management tool(s):

- IT asset discovery
- Cyber-physical systems (CPS) protection platforms
- Modern device management (MDM)

Network devices

Devices that support communication and interaction between other devices on a network. Network devices form the network infrastructure.

Known known	☐
Known unknown	☐
Unknown unknown	☐
n/a	☐

Examples:

- Routers
- Switches
- Firewalls
- Access points

Management tool(s):

- Network discovery tools

Servers/data center devices

Devices that support the processing, storage and dissemination of data. Considered the backbone of services such as email communications and websites.

Known known	☐
Known unknown	☐
Unknown unknown	☐
n/a	☐

Examples:

- Servers (e.g., email servers, print servers, web servers)
- Storage systems

Management tool(s):

- IT asset discovery
- Modern device management (MDM)
- Unified endpoint management (UEM)

Fixed-function devices

Devices designed to fulfill narrow use cases. Often customer-facing.

Known known	☐
Known unknown	☐
Unknown unknown	☐
n/a	☐

Examples:

- Point of sale (POS) systems
- Self-help kiosks

Management tool(s):

- IT asset discovery
- Modern device management (MDM)
- Unified endpoint management (UEM)

Cloud services

Cloud computing delivers on-demand access to computing resources over the internet and is orchestrated via private cloud (also known as “internal cloud” or “corporate cloud”), public cloud, hybrid cloud and multi-cloud environments.

Known known	☐
Known unknown	☐
Unknown unknown	☐
n/a	☐

Examples:

- Cloud containers
- Cloud data storage solutions
- Private cloud underlying compute resources (e.g., CPU and storage)
- Public cloud services (e.g., AWS, Google Cloud Platform, Microsoft Azure Cloud Services)

Management tool(s):

- Cloud-native application protection platform (CNAPP)
- Cloud security posture management (CSPM)
- Cloud workload protection platform (CWPP)

Software-as-a-service (SaaS) applications

On-demand applications deployed via a cloud computing service model in which the service provider manages all underlying infrastructure.

Known known	☐
Known unknown	☐
Unknown unknown	☐
n/a	☐

Examples:

- Microsoft 365
- Salesforce
- Slack

Management tool(s):

- SaaS security posture management (SSPM)

Code

A set of instructions written in a programming language that tells a computer what to do. The building blocks of software.

Known known	☐
Known unknown	☐
Unknown unknown	☐
n/a	☐

Examples:

- Code for custom software developed for internal or customer use
- Code for proprietary software developed for commercial sale

Management tool(s):

- Container scanners
- Dynamic application security testing (DAST)
- Mobile application security testing (MAST)
- Open-source software (OSS) scanners
- Software composition analysis (SCA)
- Static application security testing (SAST)

Commercial-off-the-shelf (COTS) software and applications

Computer programs purchased and used by an organization that have been purchased from a third party or that come installed on a device.

Known known	☐
Known unknown	☐
Unknown unknown	☐
n/a	☐

Examples:

- Operating systems (e.g., Windows, macOS, Linux)
- Productivity suites (e.g., Microsoft Office)
- Third-party applications (e.g., Zoom)

Management tool(s):

- IT asset discovery
- Patch management

Internet-facing assets

Cyber assets directly accessible from the public internet. These assets make up the so-called “external attack surface.”

Known known	☐
Known unknown	☐
Unknown unknown	☐
n/a	☐

Examples:

- Certificates / domains
- Dev and QA environments (IP addresses)
- Websites (web servers)

Management tool(s):

- External attack surface management (EASM)

Digital assets

A combination of assets, such as dark web data and social media, that aren’t considered conventional IT assets but can affect an organization’s brand, reputation or security.

Known known	☐
Known unknown	☐
Unknown unknown	☐
n/a	☐

Examples:

- Online forums
- Social media accounts

Management tool(s):

- Digital risk protection (DRP)

Identity and access

"Identity" refers to the digital identity of a person associated with an organization — their name, job title, manager, direct reports, phone number and other such information. "Access" represents the resources and data that person has permission to view and/or edit based on factors such as their job title or security clearance.

Known known	☐
Known unknown	☐
Unknown unknown	☐
n/a	☐

Examples:

- User identities
- Access levels

Management tool(s):

- Identity and access management (IAM)
- Identity provider (IdP)

Data

Data generated or collected by an organization for use in planning, decision-making and daily operations.

Known known	☐
Known unknown	☐
Unknown unknown	☐
n/a	☐

Examples:

- Customer credit card information
- Intellectual property (IP)
- Patient medical records
- Personally identifiable information (PII) (e.g., customer contact information)

Management tool(s):

- Data loss prevention (DLP)
- Data security posture management (DSPM)

Application programming interfaces (APIs)

Sets of rules and protocols that allow different software applications to communicate with each other.

Known known	☐
Known unknown	☐
Unknown unknown	☐
n/a	☐

Examples:

- HubSpot APIs
- Salesforce APIs
- Slack APIs

Management tool(s):

- API protection products
- API security posture tools

Third-party assets

Modern organizations often interact closely with multiple outside organizations, sharing systems and data. When two parties become so intertwined, so do their attack surfaces.

Known known	☐
Known unknown	☐
Unknown unknown	☐
n/a	☐

Examples:

- Resale partner's website
- Marketing agency's cloud infrastructure
- Supply chain partner's dev environment

Management tool(s):

- External attack surface management (EASM)

	Visibility			
Asset category	Known known	Known unknown	Unknown unknown	n/a
Endpoint devices	☐	☐	☐	☐
Mobile devices	☐	☐	☐	☐
Rugged devices	☐	☐	☐	☐
Internet of Things (IoT) devices	☐	☐	☐	☐
Cyber-physical systems (CPS)	☐	☐	☐	☐
Network devices	☐	☐	☐	☐
Servers / data center devices	☐	☐	☐	☐
Fixed-function devices	☐	☐	☐	☐
Cloud services	☐	☐	☐	☐
Software as a service (SaaS) applications	☐	☐	☐	☐
Code	☐	☐	☐	☐
Commercial-off-the-shelf (COTS) software and applications	☐	☐	☐	☐
Internet-facing assets	☐	☐	☐	☐
Digital assets	☐	☐	☐	☐
Identity and access	☐	☐	☐	☐
Data	☐	☐	☐	☐
Application programming interfaces (APIs)	☐	☐	☐	☐
Third-party relationships	☐	☐	☐	☐

About Ivanti

Ivanti breaks down barriers between IT and security so that Everywhere Work can thrive. Ivanti has created the first purpose-built technology platform for CIOs and CISOs – giving IT and security teams comprehensive software solutions that scale with their organizations' needs to enable, secure and elevate employees' experiences. The Ivanti platform is powered by Ivanti Neurons - a cloud-scale, intelligent hyper automation layer that enables proactive healing, user-friendly security across the organization, and provides an employee experience that delights users. Over 40,000 customers, including 85 of the Fortune 100, have chosen Ivanti to meet challenges head-on with its end-to-end solutions. At Ivanti, we strive to create an environment where all perspectives are heard, respected and valued and are committed to a more sustainable future for our customers, partners, employees and the planet. For more information, visit ivanti.com and follow @GoIvanti.

ivanti

For more information, or to contact Ivanti, please visit ivanti.com.