Exposure Management Readiness Checklist

Exposure management effectively combines a range of capabilities that many organizations already invest in. As a result, you might already be further along on the exposure management journey than you realize.

This checklist is a rundown of the product categories folded into exposure management and the core capabilities they provide. Organized into four categories — Visibility, Prioritization, Validation and Remediation — it can help you account for the relevant capabilities you already have in your cybersecurity tech stack and identify where you have gaps.

Many of the product types listed cover more than one category, and those are noted accordingly on each entry.

Visibility

One blind spot is all it takes for a cyber attacker to infiltrate your environment. The technologies in this section provide visibility into all the cyber assets, exposures and other elements that form your attack surface. Note that you don't need to implement every technology listed in this section. Some have overlapping capabilities, and others may not be relevant to your environment. Rather, you need to find the right mix that will give you full visibility of your attack surface.

IT asset discovery

Visibility	X
Prioritization	
Validation	
Remediation	

These tools automatically identify and inventory hardware and software assets within an organization's IT environment. However, some struggle to discover certain types of assets, and they also aren't designed to discover exposures, which is why other tools are needed for comprehensive attack surface visibility.

Unified endpoint management (UEM)

Visibility	X
Prioritization	
Validation	
Remediation	X

UEM tools help IT teams gain a comprehensive understanding of their endpoint environment — desktops, laptops, mobile devices and other internet-connected devices — and manage, configure and secure each endpoint.

Mobile device management (MDM)

Visibility	X
Prioritization	
Validation	
Remediation	X

MDM tools (in this case, short for mobile device management) are UEM tools that specialize in the discovery and management of mobile devices like smartphones and tablets.

Modern device management (MDM)

Visibility	X
Prioritization	
Validation	
Remediation	X

This type of MDM tool (in this case, short for modern device management) allows you to remotely monitor, provision, patch and secure a wider range of connected network devices than the other type of MDM tool, including but not limited to desktops, IoT sensors, wearables (e.g., smart watches), medical equipment and industrial machinery.

Network discovery

Visibility	X
Prioritization	
Validation	
Remediation	

These software solutions automatically detect and map hardware, software and virtual assets on a network. They're instrumental for creating a comprehensive view of a network infrastructure.

Network vulnerability scanners

Visibility	X
Prioritization	
Validation	
Remediation	

Network vulnerability scanners automatically detect and assess security vulnerabilities in network devices and systems, helping organizations identify potential risks.

IoT (Internet of Things) security tools

Visibility	X
Prioritization	
Validation	
Remediation	X

Though there's no industry-standard name or definition for tools that discover IoT assets and exposures, a number of such tools exist. A quick online search for "IoT security tools" should reveal a range of options.

Cyber-physical systems (CPS) protection platforms

Visibility	X
Prioritization	
Validation	
Remediation	X

CPS protection platforms are designed to discover, categorize, map and protect cyber-physical systems. These include industrial control systems (ICS) and smart building solutions that integrate physical and computational components.

Cloud security posture management (CSPM)

Visibility	X
Prioritization	
Validation	
Remediation	X

Organizations with considerable cloud infrastructure may choose to manage visibility over those environments with CSPM tools. These tools identify and catalog an organization's cloud assets — whether in private cloud, public cloud, hybrid cloud or multi-cloud environments — and continuously monitor them against security and compliance frameworks to identify vulnerabilities and threats.

Cloud workload protection platform (CWPP)

Visibility	X
Prioritization	
Validation	
Remediation	X

CWPP solutions automatically detect and address threats, vulnerabilities and errors impacting cloud-based workloads — applications and programs that run in the cloud — across virtual machines, containers and serverless functions.

Cloud-native application protection platform (CNAPP)

Visibility	X
Prioritization	
Validation	
Remediation	X

CNAPP solutions include the capabilities of CSPM and CWPP tools alongside other cloud-specific tools like cloud infrastructure entitlement management (CIEM) tools. They're basically a one-stop shop for cloud security.

External attack surface management (EASM)

Visibility	X
Prioritization	
Validation	
Remediation	

The "external attack surface" — in other words, all of your internet-facing assets — is often overlooked by organizations, but not by attackers. EASM tools identify all internet-discoverable assets, including domains, IP addresses and open ports, and associated exposures to give organizations an attacker's perspective. They can also be used to identify internet-facing assets and exposures of third parties your organization is involved with, like vendors and acquisition targets, in a non-invasive way.

Digital risk protection services (DRPS)

Visibility	X
Prioritization	
Validation	
Remediation	X

DRPS technology identifies digital risks associated with compromised enterprise assets that aren't considered conventional IT assets but which can still affect an organization's brand, reputation or security, such as domains, credentials, intellectual property and credit card details. These solutions offer monitoring capabilities for exposures across the open web, deep web, dark web and social media, plus remediation capabilities to fix those exposures.

Cyber asset attack surface management (CAASM)

Visibility	X
Prioritization	
Validation	
Remediation	

CAASM tools aggregate asset and exposure data from existing asset management and security tools using API integrations (CAASM tools don't offer native scanning capabilities). They correlate this data to create a complete picture of an organization's assets and exposures.

SaaS security posture management (SSPM)

Visibility	X
Prioritization	
Validation	
Remediation	X

By continuously scanning and assessing the security settings and configurations of software-as-a-service (SaaS) applications, SSPM tools can identify potential vulnerabilities and misconfigurations. They also employ automated remediation capabilities to correct security issues and enforce best practices.

Static application security testing (SAST)

Visibility	X
Prioritization	
Validation	
Remediation	

SAST tools analyze code for security vulnerabilities without executing the code. They're used early in the software development lifecycle (SDLC), because they don't require a working application.

Dynamic application security testing (DAST)

Visibility	X
Prioritization	
Validation	
Remediation	

DAST tools analyze running applications to identify security vulnerabilities and weaknesses. Dynamic application security testing typically takes place during the testing phase of the SDLC or even in production environments to ensure that applications are secure under actual operating conditions.

Mobile application security testing (MAST)

Visibility	X
Prioritization	
Validation	
Remediation	

MAST tools combine static analysis, dynamic analysis and penetration testing to identify vulnerabilities in mobile apps on platforms like Android and iOS.

Software composition analysis (SCA)

Visibility	X
Prioritization	
Validation	
Remediation	

SCA tools identify open-source components in a codebase, then check those components against known vulnerability databases to find any security issues or known exploits.

Identity and access management (IAM)

Visibility	X
Prioritization	
Validation	
Remediation	

The primary use case for IAM tools is to securely manage user identities and control access to critical corporate information, applications and networks. From an exposure management perspective, IAM tools help paint a picture of an organization's identity attack surface. They house identity and access data, such as user profiles, credentials, roles and permissions, and some also offer risk data around login attempts, access patterns and suspicious activities.

Identity provider (IdP)

Visibility	X
Prioritization	
Validation	
Remediation	

IdP is a component of IAM. IdP solutions focus primarily on verifying user identities and providing authentication services. In situations where a full-fledged IAM offering is unobtainable or otherwise unavailable, an IdP solution can be used to help provide visibility of an organization's identity attack surface.

Data loss prevention (DLP)

Visibility	X
Prioritization	
Validation	
Remediation	

DLP tools identify sensitive data that needs protection, such as personal information, financial data or intellectual property. They monitor how this data is being used and accessed, both inside and outside the organization, and can generate alerts and reports when suspicious activities are detected.

Data security posture management (DSPM)

Visibility	X
Prioritization	
Validation	
Remediation	X

A DSPM product can identify where all your data is stored — whether it's in databases, cloud services or other locations — and evaluate the security risks associated with that data, such as vulnerabilities, misconfigurations or weak access controls. These products also provide recommendations and tools to fix security issues and improve overall data security.

API protection products

Visibility	X
Prioritization	
Validation	
Remediation	X*

API protection products discover and inventory an organization's application programming interfaces (APIs). They also provide lists of recommended remediations for API exposures.

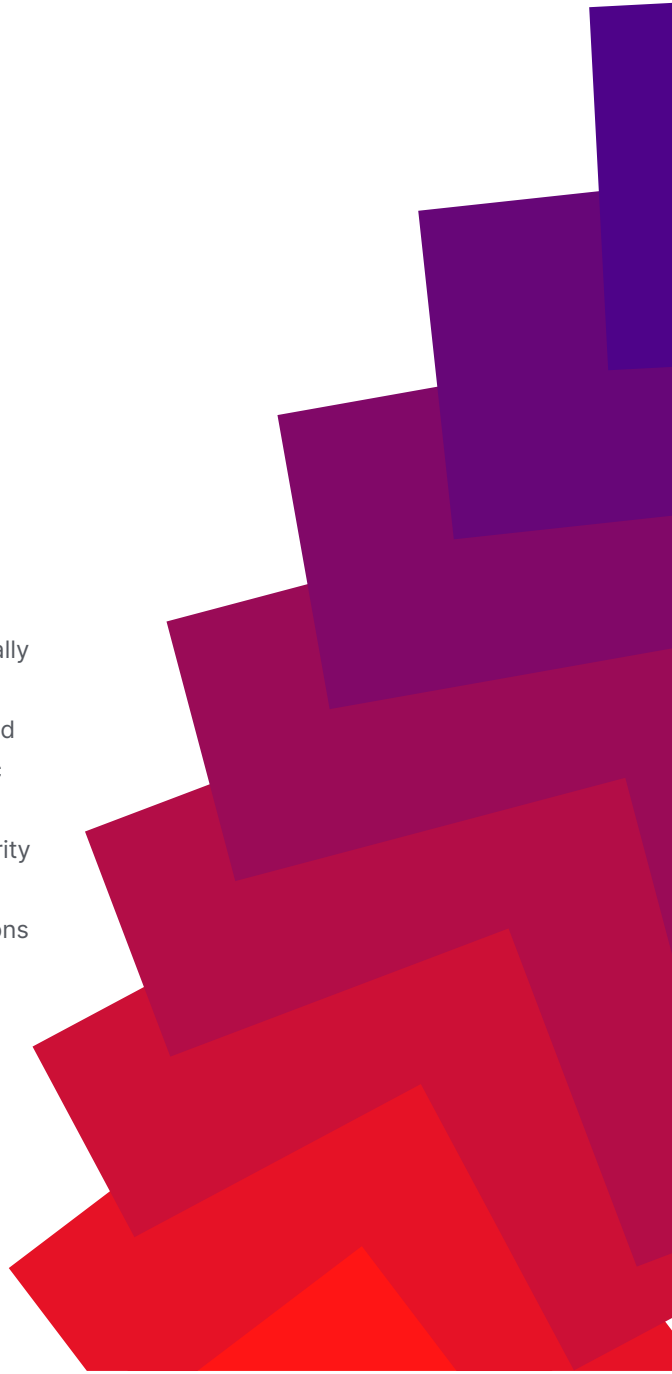
*API protection products offer remediation guidance, but not remediation action. Instead, they recommend manual actions you can take.

API security posture tools

Visibility	X
Prioritization	
Validation	
Remediation	X*

API security posture tools automatically identify and map all APIs in an environment, including undocumented or shadow APIs. They use both static and dynamic vulnerability scans to detect vulnerabilities and other security issues, then provide remediation recommendations to help organizations fix those issues and improve their overall API security.

*API security posture tools offer remediation guidance, but not remediation action. Instead, they recommend manual actions you can take.



Prioritization

Prioritization tools take the asset and exposure data pulled from visibility tools and make it actionable for your organization. You need a view of the landscape first — as the saying goes, you can't protect what you can't see — but it then falls to prioritization tools to help you figure out what to do about what you've found.

Note that some visibility tools claim they offer prioritization, and those claims are accurate, to a point. Many visibility tools can be used to prioritize remediation of exposures within their siloed scopes, but not of all the exposures an organization faces across its attack surface. For example, EASM tools only prioritize exposures associated with external-facing assets.

Exposure assessment platform (EAP)

Visibility	X
Prioritization	X
Validation	
Remediation	X

EAPs are an emerging product in the exposure management space. While exposure management is rooted in the merging of preexisting technologies, EAPs are purpose-built platforms that combine multiple exposure management capabilities. These platforms provide visibility of assets and exposures from across the attack surface — whether discovered via native scanning capabilities or ingested from third-party tools — plus prioritization of exposure remediation activities that accounts for asset criticality and business context, and the ability to orchestrate or execute those activities.

Risk-based vulnerability management (RBVM)

Visibility	X
Prioritization	X
Validation	
Remediation	

As the name suggests, RBVM tools prioritize vulnerabilities for remediation based on risk. They ingest and aggregate findings from scanners and other security tools, then correlate them against data points such as threat intelligence and asset criticality to help organizations arrive at a fully informed plan of attack. Some also offer native exposure scanning capabilities.

Application security posture management (ASPM)

Visibility	X
Prioritization	X
Validation	
Remediation	

ASPM tools are essentially RBVM tools for application security. They collect asset and exposure data from application scanners (e.g., SAST, DAST, SCA, container), which gets correlated with threat intelligence and asset criticality to prioritize exposure remediation activities. Some vendors combine RBVM and ASPM capabilities to offer customers a more unified view of cyber risk across their attack surface. Some also include native exposure scanning capabilities (e.g., SAST) in their ASPM tools.

Threat intelligence

Visibility	
Prioritization	X
Validation	
Remediation	

Threat intelligence products provide information about the threat landscape at large. Unlike the other prioritization products included in this document, they don't deal with data specific to an organization's environment. Rather, they provide a global view so that security teams can proactively prioritize potential threats before those threats have been identified in the organization's environment.

Validation

Validation serves as a check on prioritization. By verifying how potential attackers could actually exploit an identified exposure and how monitoring and control systems might react if that were to happen, validation helps an organization determine which exposures truly require remediation for the organization's risk level to stay aligned with its risk appetite.

Note that validation can be conducted using products — collectively known as adversarial exposure validation (AEV) technologies — or via manual processes, whether outsourced to a vendor or carried out by internal teams. Best practice is to combine varied validation methods for the most comprehensive results.

Whichever route you choose for validation, it's also best practice for a separate party than the one you use for prioritization to carry out validation to ensure unbiased results. Think of validation like getting a second opinion before undergoing surgery.

Attack path analysis (APA)

Visibility	
Prioritization	
Validation	X
Remediation	

Attack path analysis (APA) tools visually map the routes attackers can use to navigate an organization's environment. They allow security teams to determine what "paths" these cyber adversaries might follow within the environment to execute their attack. They also show what exposures are unexploitable dead ends.

Breach and attack simulation (BAS)

Visibility	
Prioritization	
Validation	X
Remediation	

BAS tools continuously validate an organization's exposures by simulating a wide range of cyber attacks. Unlike manual red teaming and pen testing, BAS software offers a fully automated approach to validation.

Red teaming

Visibility	
Prioritization	
Validation	X
Remediation	

Red teaming is where a group of ethical hackers, known as a red team, simulates real-world cyber attacks to test an organization's defenses, identify vulnerabilities and assess the effectiveness of its security measures.

Continuous automated red teaming (CART)

Visibility	
Prioritization	
Validation	X
Remediation	

Where red teaming involves ethical hackers manually simulating cyber attacks, CART tools automate those simulated attacks, offering frequent, real-time testing that can be more scalable and cost-effective. And where BAS tools test how well security controls handle known attack methods, CART tools focus on finding and safely exploiting vulnerabilities to see if and how an attacker could breach an organization's defenses.

Penetration testing

Visibility	
Prioritization	
Validation	X
Remediation	

Like red teaming, penetration testing — often shortened to "pen testing" — involves ethical hackers carrying out simulated attacks on an organization's systems. Where they differ is that pen testing focuses specifically on finding and exploiting exposures, while red teaming assesses overall security posture. Note that it's also wise to ask vendors, partners and other third parties for pen test results, since their attack surfaces are also part of your attack surface.

Automated penetration testing

Visibility	
Prioritization	
Validation	X
Remediation	

True to its name, automated penetration testing software conducts automated pen tests so that testing can be conducted more quickly and regularly than manual methods allow.

Penetration testing as a service (PTaaS)

Visibility	
Prioritization	
Validation	X
Remediation	

PTaaS is a cloud-based model where organizations can access penetration testing services on demand. PTaaS offerings combine both automated and manual testing techniques. And with PTaaS providers managing the testing process, organizations can conduct regular security evaluations without the need for an in-house team of security experts.

Bug bounty

Visibility	
Prioritization	
Validation	X
Remediation	

Some organizations incentivize ethical hackers to find and responsibly disclose vulnerabilities in their systems, software or websites by offering rewards or recognition — aptly called bug bounties — for that information.

Cyber range

Visibility	
Prioritization	
Validation	X
Remediation	

A cyber range is a virtual environment that allows organizations to simulate real-world cyber attacks and practice responding to security incidents in a controlled sandbox setting.

Remediation

Remediation is the final stage of the exposure management process. Once you've determined which exposures you must fix based on your risk appetite, remediation tools help you fix them.

Patch management

Visibility	X
Prioritization	
Validation	
Remediation	X

Patch management products apply updates or patches to software to fix vulnerabilities or improve functionality. Some also include discovery capabilities that provide visibility into operating systems and third-party applications.

Configuration management

Visibility	
Prioritization	
Validation	
Remediation	X

Configuration management tools automate the process of maintaining and enforcing consistent system configurations. And consistent system configurations ensure that all devices and systems within an IT environment are set up and operate according to predefined security policies and best practices.

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.