# 10 Essential Use Cases for Attack Surface Management

How Cortex Xpanse helps you meet common security challenges with ease

paloalto® NETWORKS | CORTEX XPANSE®

INTRODUCTION

## The modern attack surface is intricate, complex—and growing fast. Hard-to-monitor attack surfaces span on-premises networks, diverse cloud infrastructures, supplier networks, and remote employee devices.

Every time a business unit adds a new infrastructure component, cloud environment, or service, the attack surface grows. Every merger or acquisition adds additional complexity. Every time an employee moves to a different remote workspace, the attack surface expands yet again.

Security teams must safeguard this complex landscape so it can thrive and deliver value to the business. But these exposed assets offer many opportunities to attackers, who relentlessly look for vulnerabilities and use any means necessary to exploit them.

Security teams need to identify every asset they own, maintain continuous visibility, and eliminate blind spots from their environment. Yet these teams are often understaffed and stretched thin. They don't know exactly how many assets they have and often rely on tools that require a great deal of manual work.

**Only 9%**

of organizations believe they actively monitor their entire attack surface.[1]

**Nearly 50%**

of high-/critical-level exposures introduced each month are a result of constant change in the cloud.[2]

[1] Jon Oltsik, "Look for attack surface management to go mainstream in 2022," CSO Online, February 11, 2022.

[2] *2023 Unit 42 Attack Surface Threat Report*, Palo Alto Networks, 2023.

## Fix the Unknown

Knowing exactly what you need to secure is the first step in outpacing your adversaries. For many teams, that often means scrubbing through spreadsheets and outdated configuration management databases. It includes tracking down the owners and business context for every unknown asset, which can take weeks or even months.

It involves contacting all regional offices and business units to develop a single source of truth. It requires creating a system to continuously verify and update this repository—because attack surfaces change constantly.

If that sounds like an impossibly complicated task, that's because it is. And even if you do manage to identify every asset, there are still more hurdles to overcome, such as:

- **Alert overload provides air cover for attackers.** Manually investigating every alert can keep teams occupied while adversaries do real damage.
- **Limited visibility makes immediate zero-day response a challenge.** There are often long gaps between the time critical zero days are published and when your team is able to prioritize and remediate those threats, which puts your business at risk.
- **Remediation is complex and time-consuming.** Successful remediation requires the ability to identify asset ownership and business context before any decision can be made.

## Why Is It So Important to Identify Every New Asset as Soon as Possible?

Organizations average one new serious exposure on the internet **every 12 hours.**[3]

Attackers start scanning for vulnerabilities **within hours** of publishing remote code execution exploits.[4]

On average, Xpanse prospects did not know about **30–40% of their publicly accessible** attack surfaces.[5]

[3] Rob Rachwald, "Cortex Xpanse Researchers Identify Missing Metric for a Modern SOC," Palo Alto Networks, May 19, 2021.

[4] Rachwald, "Cortex Xpanse Researchers Identify Missing Metric for a Modern SOC."

[5] 2023 Unit 42 Attack Surface Threat Report.

## Take a Proactive Approach to Attack Surface Management (ASM)

Attackers are opportunistically scanning your attack surface—and you need to understand it better than they do. Palo Alto Networks Cortex Xpanse® is an advanced attack surface management solution that proactively finds and fixes exposures on your internet-connected assets before attackers can exploit them. It creates a current, complete, and accurate view of your assets and applies threat and exploit intelligence to prioritize risks. With the help of predefined playbooks, you can identify service owners and auto-remediate exposures or fix them manually to secure and shrink your attack surface.

**Xpanse uses built-in automation to help you identify and resolve critical security issues. From preventing ransomware to reducing cyber insurance premiums, our team has identified 10 critical ASM use cases where Xpanse can help your organization secure your attack surface.**

OVERVIEW AND QUICKLINKS

# 10 Critical Use Cases That Can Be Solved with Xpanse

1 Prevent Ransomware Attacks ›

2 Eliminate Shadow IT ›

3 Respond Immediately to Zero Days ›

4 Improve Vulnerability Management ›

5 Perform Better M&A Due Diligence ›

6 Reduce Cyber Insurance Costs ›

7 Reduce Incident Response Timelines ›

8 Eliminate Web Content Insecurities ›

9 Secure Critical Operational Technology (OT) Systems and Services ›

10 Monitor and Improve Compliance ›

# Ransomware is one of the biggest threats facing the modern enterprise.

Perpetrators frequently use Remote Desktop Protocol (RDP) to get in. In fact, this attack vector is so prevalent that 85% of organizations analyzed in a 2023 report from Palo Alto Networks® had at least one internet-accessible RDP instance online during the month.[6]

The problem is bigger than RDP alone; that same report found that web framework takeover exposures, remote access service exposure, and IT and security infrastructure exposures together make up over 60% of all the exposures on the global attack surface.[6]

The Xpanse Active Response Module contains end-to-end remediation playbooks, which find and eliminate exposed RDP servers, insecure OpenSSH, and other remote access exposures, which are the gateway to ransomware. After remediating a threat, Xpanse automatically validates that the effort was successful by scanning assets, compiling audited actions, and placing investigation details into clear dashboards and reports.

Your organization can become more effective at identifying and stopping ransomware, without adding more hours or staff. You always know what Xpanse is doing and have the confidence that these playbooks are working in the background to keep ransomware out.

[6] 2023 Unit 42 Attack Surface Threat Report.

## CASE STUDY
## Financial Services Firm

A high-profile Fortune 100 financial services company used Xpanse to discover, monitor, and track all of its internet-connected assets. It uncovered a previously unknown system that exposed an RDP server on the public internet—putting its systems at risk of ransomware.

**With the help of Xpanse, it was able to take significant steps to reduce its attack surface:**

- **Remediated 20+** critical exposures
- **Eliminated or replaced 100s** of non-compliant certificates
- **Reduced 1,200** publicly accessible services on the internet to 175

READ THE FULL STORY

## 2 | ELIMINATE SHADOW IT

# SaaS apps and solutions have become massively popular across industries—yet many are used outside the purview of IT.

Users with the best intentions can accidentally misconfigure settings that expose the company to risk. Security teams often have no idea that company data is being stored in several different cloud service providers, or only find out in the aftermath of an incident.

Xpanse's AI-powered discovery capability helps you comprehensively discover and eliminate shadow IT with the ability to index over 4.3B IPv4 addresses across hundreds of port-protocol pairs—discovering risks on the internet that other solutions are unable to.

Whether your organization has hundreds of assets or hundreds of thousands, Xpanse leverages its unique asset identification method to meet any demand—and scale with you as your environment grows.

# Zero-day exploits use novel approaches that security teams haven't seen before—giving bad actors the element of surprise.

Teams struggle to address these attacks, as they target vulnerabilities in new ways. Oftentimes, these threats inflict serious damage before teams can wrap their heads around what they're dealing with.

**The Xpanse attack surface rules help you stay on top with over 700 policies that are updated frequently with new Common Vulnerabilities and Exposures (CVE) database entries and zero-day vulnerabilities fingerprints.** Thanks to the persistent efforts of our cybersecurity research team, sometimes Xpanse has insight into these threats before they are officially released.

As a result, Xpanse is able to identify and stop zero-day threats. By staying up to date with the information in this console, you'll be less likely to be caught off guard and better prepared to take action when needed.

## Tackles Zero-day Threats Head-on

Assess and reduce your exposure in just a click with risk-based prioritization.

**With over**

**700**

**up-to-the-minute policies,**

you're in the know about CVEs and zero day threats before they strike.

# Vulnerability management is a cybersecurity practice in which teams use various tools to continuously identify, assess, and prioritize vulnerabilities for remediation.

It sounds great in theory, but many vulnerability management scanners have a massive blind spot: They only scan known assets. That's because they tend to be IP-based, without the ability to discover assets in the cloud.

That's a major problem, as industry data indicates that **over 20%** of externally accessible cloud services change every month on average. Over time, it's easy to lose track of misconfigurations or new, unauthorized apps or services—allowing shadow IT to spread.[7]

Xpanse helps to level the playing field by looking at your entire asset inventory, known and unknown. Using patented technology, Xpanse pulls data on cloud- and internet-facing assets and removes stale, unrelated, and other false positive assets.

You can then see everything attributed to your organization—all domain certificates, services, and asset types—including non-standard port usage. Xpanse also identifies servers that might be misconfigured or ripe for targeting so you can make the appropriate fixes.

In-depth discovery across more asset types and environments ultimately leads to greater visibility, arming you with the information you need to prioritize security efforts and address the most critical risks first.

[7] 2023 Unit 42 Attack Surface Threat Report.

CASE STUDY

## Construction Company

A large construction company had a number of assets in the cloud and wanted to better understand them. Xpanse exposed multiple vulnerabilities its security team didn't even know existed.

**The company was able to reduce the risk of a data breach by gaining visibility and securing these previously unknown cloud assets, including Log4j vulnerabilities.**

- **28% of assets** uncovered by Xpanse were previously unknown
- **51% of public-facing assets** hosted in Amazon Web Services (AWS) were unknown
- **20% attack surface reduction** due to decommissioned assets

WATCH THE WEBINAR

## 5 | PERFORM BETTER M&A DUE DILIGENCE

# As the acquiring company, it is vital that you understand the potential security risks posed by the candidate's IT environment.

Every acquisition increases your attack surface, but a rigorous appraisal helps you better understand what you're getting into.

Pre-transaction, Xpanse helps you gain visibility into the entire asset inventory of the candidate allowing you to uncover not only the assets they know about, but also the ones they don't. It can identify the candidate's security posture, including existing or potential risks, so you can estimate what resources will be required to resolve them. It can assist in evaluating the candidate's compliance with cybersecurity standards and regulations, along with any weaknesses in its data security practices. This information is vital to M&A teams, as they need to determine how these factors might impact your organization—now and in the future.

Post-transaction, Xpanse helps your team assess and prioritize risks based on severity so that you can address the most critical issues first. You can search under a new subsidiary or newly acquired company and see a list of only the assets attributed to that organization or business unit. That way, you gain a clear picture of what needs to be done so that you can tackle the most important tasks first.

As your security organization manages the expansion, Xpanse can map the new business into a centralized view. Your teams are able to see everything within a single console and use that information to develop an integrated security posture. Ultimately, Xpanse serves as a vital tool for helping your team make informed decisions and better manage potential risks associated with an acquisition.

In-depth discovery across more asset types and environments ultimately leads to greater visibility, arming you with the information you need to prioritize security efforts and address the most critical risks first.

### CASE STUDY
## Healthcare Company

After a series of acquisitions and subsidiaries, a Fortune 100 healthcare company had cloud assets spread over many different providers—and lacked visibility into many of its assets, certificates, and domains.

**With Xpanse, it was able to consolidate cloud assets, remove stale IP ranges, and clean up its attack surface.**

- **70% reduction** in high-critical issues
- **Decrease from 10–15 to 5** cloud providers
- **14% attack surface reduction** due to decommissioned assets

WATCH THE WEBINAR

## 6 | REDUCE CYBER INSURANCE COSTS

# As cyberattacks become more frequent and costly, insurance companies are becoming more rigorous about vetting their customers.

Rates are based on your risk profile, and insurers conduct yearly or biannual audits to determine your position.

Xpanse helps you eliminate exposures and lower your risk profile—allowing you to negotiate lower insurance premiums. With a robust and comprehensive approach to attack surface management, Xpanse gives insurers the confidence that your organization is equipped to minimize blind spots, reduce alert volume, and focus your team on true threats.

**Xpanse demonstrates your preparedness in six key ways:**

1 | **Proactive risk mitigation and prevention**

2 | **Continuous monitoring and compliance**

3 | **Threat intelligence integration**

4 | **Incident response optimization**

5 | **Data protection and privacy measures**

6 | **Documentation and reporting**

Lastly, Xpanse provides you with evidence of your commitment to cybersecurity best practices—giving you an edge in insurance negotiations by demonstrating a proactive approach to security and risk management.

### CASE STUDY
## Global Retailer

With 700+ locations around the world, a global retailer had a massive and growing attack surface. A cybersecurity assessment by its insurer uncovered risks and blind spots—followed by a rate increase.

**The company turned to Palo Alto Networks® solutions, including Cortex Xpanse, to help it create transformational change:**

**30% reduction**

in cyber insurance premiums

READ THE FULL STORY

# When the worst case happens and you experience a breach, your team must work to pull together an incident timeline.

What happened first? What happened next? Creating a robust response plan requires a thorough understanding of the attack surface.

- **Xpanse accelerates incident response timelines by automating threat detection and prioritization,** providing real-time alerts, and integrating seamlessly with other incident response tools. This allows you to mount a coordinated, streamlined response process, leveraging automation to mobilize your teams more quickly and effectively.
- **Xpanse also helps you facilitate efficient collaboration** among security teams to ensure that you are sharing the right information with the right stakeholders in those critical moments.
- **Lastly, it uses historical data to identify patterns and trends** so you can prepare for similar incidents in the future.

## When Every Second Counts, Cortex Xpanse Delivers

Automated threat detection and prioritization

Real-time alerts

## The Result?

The average incident-remediation time is reduced from

**3 weeks** → **5 minutes**

## 8 | ELIMINATE WEB CONTENT INSECURITIES

# Sensitive content running on the web can expose your organization to risk.

Sensitive content includes personally identifiable information (PII), financial or payment data, and business information. If this kind of content is breached, it could trigger legal or regulatory action, reputational damage, and potential settlement costs. Content issues can also impact critical revenue generation capabilities for your business—for instance, requiring that you shut down an e-commerce site until the issue is fixed.

The Xpanse web ASM dashboard brings the powerful ability to crawl website data and determine if it is adhering to security best practices. You can set it up to frequently and proactively scan and analyze your public-facing web infrastructure to identify issues and potential exposures—taking the pressure off your internal teams.

**Xpanse empowers your organization by:**

- **Identifying** insecure and misconfigured websites
- **Tracking and measuring** risks caused by third-party libraries or dependencies attributed to web artifacts
- **Identifying websites** that serve sensitive content without adequate security protocols

Not only does it provide continuous monitoring of your web environment, but it also delivers automated responses to identified threats and vulnerabilities. Xpanse has the ability to implement security measures, block malicious activities, and trigger alerts to your teams when something needs their immediate attention or investigation. Your overall security posture improves with yet one more capability from Xpanse that helps you stay ahead of aggressive cyberthreats.

## 9 | SECURE CRITICAL OPERATIONAL TECHNOLOGY (OT) SYSTEMS AND SERVICES

# Many organizations don’t think of their operational systems as a target; after all, what would attackers want with facilities and internal controls?

An attack on operating technology can be part of a wider effort or can inflict extensive damage on its own. From schools and hospitals to power plants and energy grids, disruption of services can have terrible consequences, making OT safeguards just as important as those designed for networks and digital systems.

**Xpanse helps you improve OT security by scanning for misconfigured BACnet servers and identifying exposures in your building control management systems.**

By adding these systems to your central asset inventory, you can take advantage of active discovery, assessment, and response capabilities built into Xpanse. Your teams will be equipped to rapidly resolve issues and stay in compliance more easily with laws and regulations that apply to your industry.

**Operational technology is an area that is often overlooked, but OT systems are present on the networks of nearly every organization.[8]**

**60%**

said OT security complexity was top concern.

**25%**

had to shut down operations due to cyberattack.

**3 out of 4**

organizations have experienced a cyberattack on their OT environment.

[8] State of OT Security Report 2024

10 | MONITOR AND IMPROVE COMPLIANCE

## If your company operates in a heavily regulated industry, such as healthcare or finance, you must meet rigorous compliance requirements to operate in a safe and secure manner.

But compliance is never a static thing. Cloud usage grows. Companies make acquisitions or form subsidiaries. Assets begin to sprawl across environments. Along the way, it's easy to lose track of different assets and domains—which creates compliance gaps.

**Xpanse helps you discover all of your assets and map them to compliance frameworks for your industry.**

Very quickly, Xpanse determines whether any of your assets are in violation of a particular compliance certification, such as National Institute of Standards and Technology (NIST) and many others. It can also identify assets that should be decommissioned to help you reduce your overall attack surface. Lastly, Xpanse helps you secure unknown or unmanaged assets so you can bring them back under your control.

## WHY CONSIDER CORTEX XPANSE?

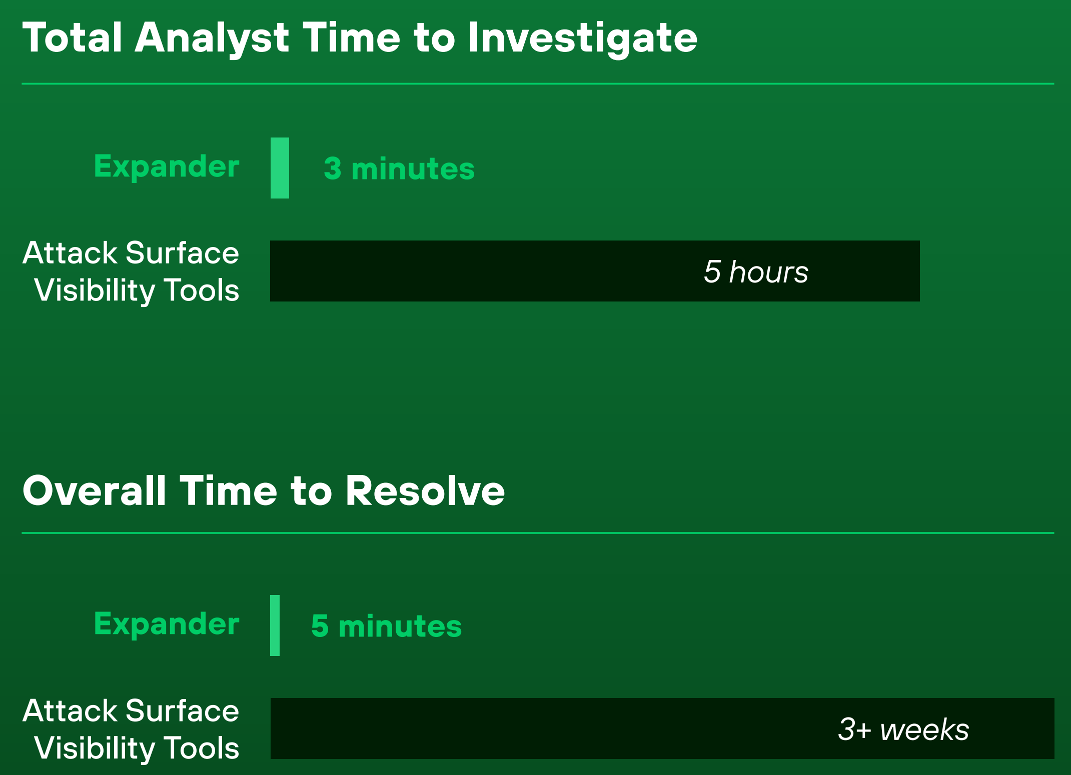
# There are many attack surface management products on the market, but most are limited to discovery.

Your team is left with the job of developing a unified view and finding and fixing the exposures. Xpanse is the Active ASM solution that goes beyond discovery to help you secure all your corporate assets against potential threats. It does this in three distinct ways: Discovery, Assessment, and Remediation.

## Faster Investigations, Quicker Responses, Fewer IT Tickets

Xpanse not only delivers a comprehensive ASM solution, but it also works rapidly, leveraging the latest automation technologies to investigate and respond to issues in minutes—not hours or weeks. Every day or hour you save can translate into significant savings and risk reduction.

## Actively Find and Fix Your Risks with Cortex Xpanse


Total Analyst Time to Investigate

Overall Time to Resolve

## Deployed at Scale by the World’s Most Demanding Organizations

Xpanse has been thoroughly field-tested and deployed at scale by the world’s largest and most demanding organizations, from U.S. nuclear weapons labs to all six branches of the U.S. military. Companies in highly regulated industries, from financial services to biotech and healthcare, rely on Xpanse to help them secure the growing attack surface and gain an edge on attackers.

**Learn more about Cortex Xpanse or Schedule a Demo.**

paloalto® NETWORKS | CORTEX XPANSE®

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com/cortex/cortex-xpanse