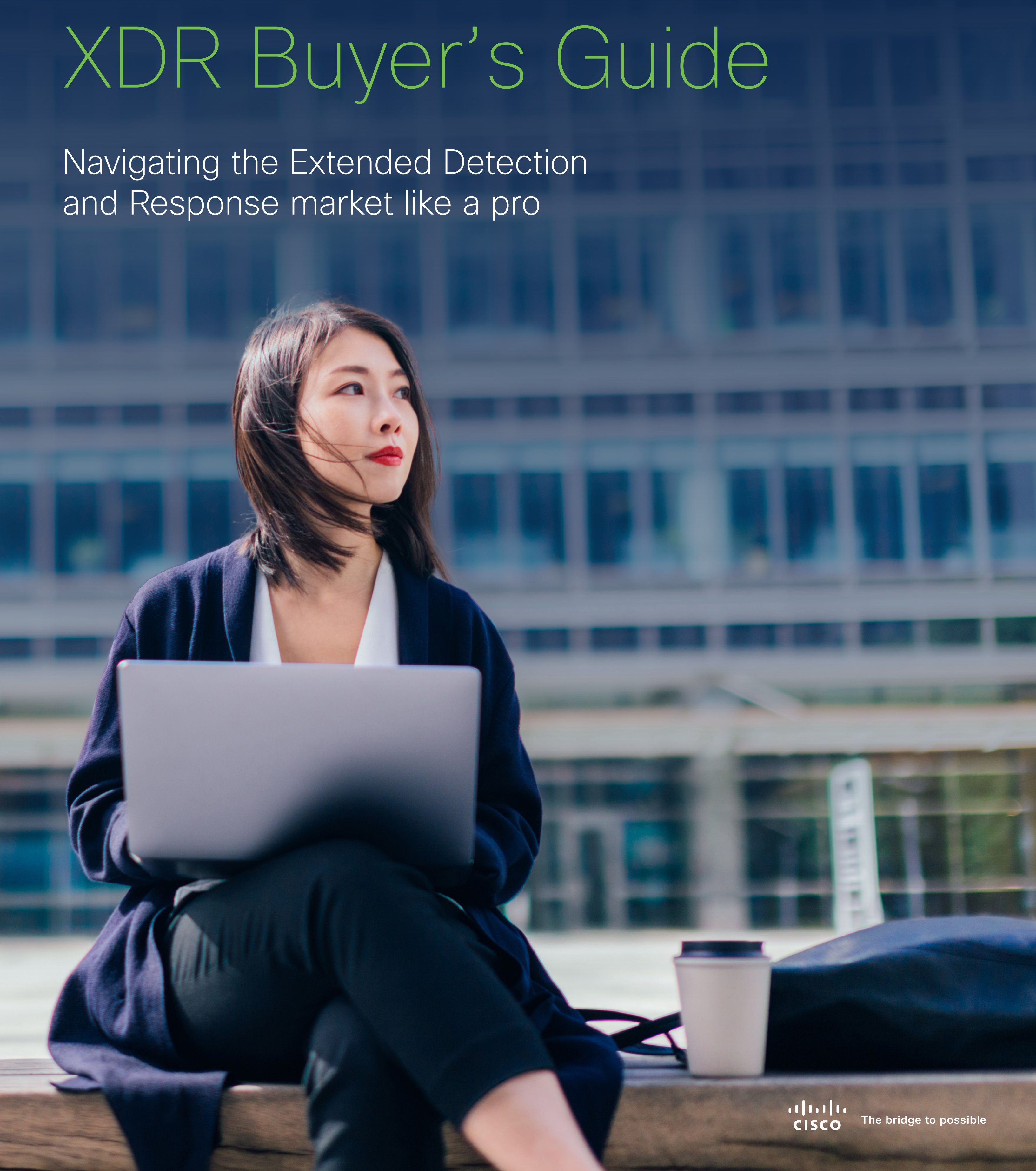
CISCO
SECURE

XDR Buyer’s Guide

Navigating the Extended Detection and Response market like a pro



CISCO The bridge to possible

Understanding Extended Detection and Response (XDR)

Why does the world need another security approach?

In today's hybrid, multi-vendor, multi-vector landscape, complexity is the biggest challenge. Security teams must protect an ever-expanding ecosystem, running operations across dozens of tools with inconsistent integration. IoT and hybrid work have led to an expanded attack surface. Phishing, malware, and ransomware are doubling and even tripling year over year. At the same time, businesses are more hyper-connected than ever before. A security breach to one company can impact a company's suppliers, partners, customers and even whole sectors of the economy.

This new normal calls for security resilience – the ability to protect the integrity of every aspect of the business to withstand unpredictable threats or changes and emerge stronger. And security resilience calls for more than what the past has offered.

The XDR advantage:

- Multi-vendor detection
- Reduced alert fatigue
- Elevated productivity
- Security resilience

What is the solution?

With threats becoming increasingly sophisticated, the old detection and response model, built upon self-contained point security solutions, doesn't go far enough. This is where XDR comes in. Extended Detection and Response (XDR) is a unified security incident detection and response tool. XDR solutions automatically collect and correlate telemetry from multiple security tools, apply analytics to detect malicious activity, then respond to and remediate threats. Effective XDR solutions are comprehensive, correlating data across all vectors – email, endpoints, servers, cloud workloads, and networks – enabling visibility and context across your environment into even the most advanced threats.

Why XDR?

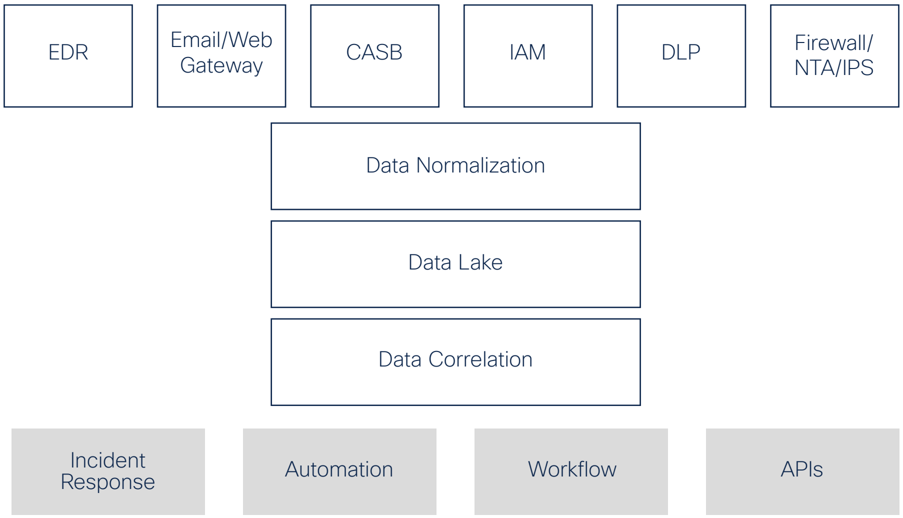
First, it allows teams to detect the most sophisticated threats with event correlation and multi-vendor detections across network, cloud, endpoint, email and more.

Second, it reduces alert fatigue by enabling teams to prioritize threats based on impact.

Third, it elevates productivity with task automation so teams can make more efficient use of SOC resources.

Fourth, it allows organizations to build security resilience by closing security gaps and anticipating what's next through actionable intelligence.

XDR conceptual architecture



5 key elements of XDR done right

1 Provides prioritized and actionable telemetry, everywhere you need it

Can you efficiently sift through the sea of alerts to triage threats?

Breadth of visibility and depth of insight are foundational to XDR. Many sophisticated threats don't just attack the endpoint, or the network alone – they attack across a variety of vectors, including email, endpoint, network, identity management, sandboxing and firewall. That's why you need an XDR solution with a broad range of telemetry and quality of data that can inform your XDR outcomes and provide a holistic and complete view of what is happening across your environment. But it's not just about gathering insights — incident management is equally important. For XDR to have the impact it promises, these insights must be prioritized. XDR solutions that offer risk-based prioritization — prioritizing incidents by greatest material risk — will allow you to act on what truly matters, faster. They should also offer recommendations for next steps, so that you can make informed decisions on the best course of action.

Key Functions and Capabilities	Related Product Areas
• Efficacy and accuracy to minimize noise from false positives • Aggregate and correlate alerts across the environment	Endpoint Detection & Response (EDR)
• Continuous real-time network monitoring	Network Detection & Response (NDR)
• Advanced analytics that generate prioritized alerts with context when unkown malware and other sophisiticated network attacks are detected	Extended Detection & Response (XDR)
• Continuous real-time email threat monitoring and automatic remediation prioritization	Email security

Questions to Ask Vendors

- How does your solution provide me with visibility across all my environments (endpoints, devices, network)?
- How does your solution deliver insights? Does your solution provide prioritized telemetry?
- How does your solution prioritize threats based on business impact and risk?
- What type of threat intelligence is feeding your detection? Where does that intelligence come from?
- How do you validate the data sources you use in your solution?
- How does this product handle sophisticated threats such as Wannacry, NotPetya and Turla?

2 Enables unified detection, regardless of vector or vendor

Does your XDR solution enable your security investments to work together as one coordinated unit?

As threats grow more sophisticated and span across a greater variety of attack vectors, ensuring consistent detection across your environment has never been more critical. Security teams today are dealing with an extraordinary level of complexity both in their security environment and in an ecosystem of global supply chains, attackers, and defenders. XDR solutions can help you do this by aggregating, correlating, and prioritizing detections based on severity and impact. But in order to do this, your security stack needs to work in unison. By selecting an XDR solution that is open, extensible, and cloud-first, you'll benefit from unified detection and event correlation across your environment instead of adding additional layers of complexity. Each component in your security stack has unique detection elements – networking, email, firewall, etc. – that become more powerful when brought together. It is important to consider that XDR should encompass all six telemetry sources, including endpoint, network, firewall, email, identity, and DNS, to provide a comprehensive view of potential threats. Your XDR solution should easily integrate with your entire security stack with native backend to frontend integration, so coverage stays consistent even as vendors make portfolio changes or if you switch vendors. Finally, to optimize the threat detection capabilities of your security stack, it is worth exploring XDR solutions that can provide valuable local context and deliver accurate threat intelligence verdicts on which you can rely.

Key Functions and Capabilities	Related Product Areas
• Detect and block abnormal endpoint running program behavior, including exploit-based memory injection attacks • Determine indicators of compromise (IoCs) with MITRE ATT&CK mapping • Monitor file reputation to detect and isolate threats at the point of entry • Identify OS vulnerabilities in your environment, enabling administrators to prioritize remediation based on risk and reduce your attack surface	Endpoint Detection & Response (EDR), Vulnerability Management
• Use advanced analytics to quickly detect unknown malware, insider threats such as data exfiltration and policy violations, and other sophisticated attacks • Detect network attacks in real-time with high-fidelity alerts	Extended Detection & Response (XDR), Network Detection & Response (NDR)
• Detect and block unwanted email with reputation filtering • Identify and protect against deception-based email attacks such as social engineering, impostors	Email security

Questions to Ask Vendors

- How many of my existing investments can your XDR platform leverage?
- Is your XDR platform compatible with my solutions, regardless of vendor?
- Do your solutions have out-of-the-box integrations with one another?
- How are your detection technologies better than others that are on the market?
- What kind of threats does your solution help detect? Does it map alerts to the MITRE ATT&CK framework?

3 Supports fast, accurate threat response

Once identified, how fast can you confidently respond to threats?

Unifying insights from the network, endpoint, and email (to name a few) provides a more accurate understanding of what has happened, how it progressed and what steps need to be taken in order to remediate the threat. Ideally, you should be able to view threat impact and scope from one location, taking actions with just a click or two. Effective XDR requires native response and remediation capabilities, such as isolating a host or deleting a malicious email out of all inboxes. XDR should also make it easy to create custom response actions with opportunities to automate so that teams can evolve their security as time goes on.

Key Functions and Capabilities	Related Product Areas
· Quickly respond to endpoint threats once compromised	Endpoint Detection & Response (EDR)
· Identify and isolate the root cause of a network issue or incident within seconds	Extended Detection & Response (XDR), Network Detection & Response (NDR)
· Block malicious websites quickly with real-time click-time analysis	Email security

Questions to Ask Vendors

- What response actions does the product provide?
- Can remediation be performed on the endpoint using an XDR solution in one location and scaled to others?
- How does the product integrate with existing security tools that enable response?
- How does your solution accelerate remediation?
- From threat alert to remediation, what’s the response time (ex: for a phishing attack)?

4 Offers a single investigative viewpoint for a streamlined user experience

Is your threat detection, response and remediation managed from a single interface?

When evaluating XDR solutions, it's important to take the security analyst experience into account. SecOps teams have enough to manage – there's no need to slow them down with dozens of tools and a plethora of consoles. That's why we recommend XDR solutions that are designed to help analysts detect and respond to threats more quickly and effectively by providing a unified view of security data across multiple security tools and data sources. This can help streamline workflows and reduce the time and effort required to investigate and remediate security incidents. XDR solutions should provide a full lifecycle dashboard covering every threat vector and access point. It should facilitate threat hunting through models such as MITRE ATT&CK that will make hypothesis-driven threat hunting accessible for those new to the process – and make it easier to anticipate what's next. Another factor to consider is the impact of design on the analyst experience. It should elevate productivity, improve decision making times associated with key functions of detection, investigation and response and empower a beginner-intermediate analyst to perform advanced task within security operations by providing better context for alerts with progressive disclosure to quickly determine the scope and severity of a potential threat.

Key Functions and Capabilities	Related Product Areas
· Provides a full lifecycle dashboard covering every threat vector and access point · Delivers a unified toolset that extends across your ITOps, SecOps and NetOps · Access and manage data, analytics and automation from oneunified location	Extended Detection & Response (XDR)

Questions to Ask Vendors

- How does your solution help my team in their threat hunting endeavors?
- How does the solution integrate with existing security technologies such as SOAR and SIEM solutions?
- Can I use your XDR to understand the impact of a threat, discover the scope of the breach, and take single-click actions from one interface?
- Does your solution provide support for role-based security by restricting all or portions of system/sub-system access to authorized groups and individual users?
- Can you centralize and analyze telemetry from all my existing security technology?
- Does your solution streamline incident response workflows to bring down the overall investigation timeline?

5 Provides opportunities to elevate productivity and strengthen security posture

Do your XDR solutions increase threat detection and response efficiency, with less overhead?

An important element of building your company's security resilience is automation and orchestration. Your security staff have important tasks to complete. When faced with a security threat, there's no need for their time to be swallowed up following convoluted, manual and repetitive workflows. XDR solutions that elevate productivity by automating critical workflows – such as discovering an alert, correlating it, prioritizing and taking a response action quickly – will free up your teams across the full lifecycle. An effective XDR solution should reduce the mean time to respond by enabling an investigation that presents clear decisions and actions to allow analysts to respond in an automated and consistent way according to their policy and procedures. This means your SecOps teams can invest their time and energy towards more strategic and proactive security tasks, further strengthening your company's security posture.

Key Functions and Capabilities	Related Product Areas
• Automatic endpoint threat hunting, including low prevalence threats • Enable administrators to write and scan for custom indicators of compromise (IoCs)	Endpoint Detection & Response (EDR)
• Predictive network threat remediation enabled by behavioral analytics driven insights	Extended Detection & Response (XDR), Network Detection & Response (NDR)
• Automatically prioritize email threat remediation	Email security

Questions to Ask Vendors

- For your third-party integrations, do vendors' API changes break your automation scripts?
- How does your solution support monitoring to and from cloud-based workloads?
- Will I need to change environment or deploy new technology with the XDR solution?
- Does your XDR solution offer pre-built and out of box integrations with third-party security technology?
- Does the XDR solution bring down the analyst time needed to investigate and resolve an incident?
- Does your XDR solution inform your policy management to build resilience?

Cisco XDR

XDR is a crucial component of security resilience

Today, uncertainty is a guarantee. In response, companies are investing in resilience across every aspect of their business, from finance to supply chains. But these will fall short without investment in security resilience – the ability to protect your business against threats and disruption, and to respond to changes confidently so you can emerge even stronger.

XDR is a crucial component of embracing security resilience for your business. Doing XDR right will increase your security posture by empowering security teams to prioritize threats by impact, detect threats sooner and accelerate response. Automation and orchestration capabilities facilitate this process, freeing up security teams so they can focus on what matters most.

The value of an integrated approach

50%
Decreased risk and cost of data breach

90%
Reduction of analyst effort per incident

90%
Increase in SecOps efficiency

85%
Reduction of attack dwell times

Source: The Total Economic Impact (TEI) Of Cisco SecureX, July 2021

Security Operations Simplified with Cisco XDR

Cisco is leading the way towards XDR with the most comprehensive security portfolio on the market. At Cisco, we have proactively invested in creating the most comprehensive security portfolio on the market, anticipating the security needs of the future, and integrating the components to make effective security simple and accessible for all teams, regardless of vendor or vector. We understand that building an XDR approach is a process, and we want your teams to break out of the vicious cycle of patchwork coverage from an industry supersaturated with point solutions. With Cisco XDR, we aim to discover the shortest path from detection to response with the least friction.

Designed by SOC experts for SOC experts, Cisco XDR simplifies security operations to help security analysts remain proactive and resilient against the most sophisticated threats. Our solution is open, extensible, and cloud-first, allowing you to leverage existing security investments and gain unified security detection across your entire environment.

At Cisco, we take the responsibility of protecting customers' assets seriously, as we are also customers of our customers. We want to partner with you in your security resilience journey through the Cisco Security Cloud, an open security platform that helps you protect your entire ecosystem, no matter what comes next. Join us and experience the power of comprehensive security.

Ready to build the security operations of tomorrow, today?

Explore Cisco XDR

Key XDR Elements and Capabilities

Use this table (pages 9–10) for quick reference during conversations with XDR vendors.

Key Element	Key Capabilities	Aligned Cisco Product(s)
Provides prioritized and actionable telemetry, everywhere you need it	· Built-in endpoint detection and response (EDR) that can be completely managed, proactive threat hunting · Integrated risk-based vulnerability management that enables quick vulnerability identification, risk scoring, prioritization, and remediation	Secure Endpoint
	· Continuous cloud activity analysis · Advanced analytics including behavioral modeling and machine learning algorithms · One view across your security infrastructure for unified visibility and aggregated, actionable intelligence	Cisco XDR
	· Advanced outbreak filters with real-time click-time analysis	Secure Email
Enables unified detection, regardless of vector or vendor	· Run-time detection and blocking of abnormal running program behavior · Ability to make advanced OS queries on the endpoint in real-time · Built-in threat hunting that maps to the MITRE ATT&CK framework	Secure Endpoint
	· Detect attacks across the cloud in real-time with high-fidelity alerts enriched with context (including user, device, location, timestamp, and application) · Detect and isolate threats with confirmed detections · Detect rogue entities with NDR and automate quarantine with endpoints · Detect internal hosts communicating to an external host · Provides a complete audit trail of all cloud transactions for more effective forensic investigations · Built-in integrations with other XDR solutions in the portfolio · Integrate with third-party solutions through built-in, pre-packaged, or custom integrations for a connected backend architecture and consistent frontend experience · Built-in integrations with other technologies across cloud, endpoint, network and applications (including other third-party technologies)	Secure Network Analytics & Cisco XDR
	· Antispam, URL-related protection and control, high-performance virus scanning, outbreak filters and reputation scanning for domain functionality · Forged email detection that protects against BEC attacks targeting executives · Automated malware analysis and sandboxing	Secure Email
Supports fast, accurate threat response	· Access always-on protection with threat intelligence and insights pooled from dedicated global Security Operations Centers (SOCs) for broad customer base	All Cisco Secure products

Key XDR Elements and Capabilities

Key Element	Key Capabilities	Aligned Cisco Product(s)
Supports fast, accurate threat response (cont.)	· Access always-on protection with threat intelligence and insights pooled from dedicated global Security Operations Centers (SOCs) for broad customer base	All Cisco Secure products
	· Continual monitoring of all endpoint activity, providing run-time detection and blocking of abnormal behavior	Secure Endpoint
	· Identify and isolate threats in encrypted traffic without compromising privacy and data integrity · Trigger "response" workflows from one location · Threat response that aggregates contextual awareness from security product data sources along with global threat intelligence from Talos® and third-party sources via APIs · Create forensic incident investigation casebooks	Cisco XDR
	· Persistent protection against URL-based threats via real-time analysis of potentially malicious links · Continuous leveraging of real-time Talos® monitoring, analytics and threat intelligence to identify previously unknown threats or sudden changes	Secure Email
Offers a single investigative viewpoint for a streamlined user experience	· Gather and correlate global intelligence in a single view, enabling accelerated threat investigation · Create custom response actions to reduce response time · Automate enrichment from multiple data sources, overlayed with threat intelligence	Cisco XDR
Provides opportunities to elevate productivity and strengthen security posture	· Automatic identification and threat analysis of low prevalence executables · Ability to write custom IoCs to scan for post-compromise indicators across the entire endpoint deployment.	Secure Endpoint
	· Behavioral modeling, multilayered machine learning, and global threat intelligence · Automatically classify new device roles as they are added to the network · Integration with an XDR solution to enable automation across every threat vector and access point	Secure Network Analytics & Cisco XDR
	· Automatically trigger dynamic reputation analysis and provide visibility into where email malware originated, what systems were affected, and what the malware is doing · Take action on both inbound and outbound email based on remediation insights	Secure Email
	· Automate routine tasks using prebuilt workflows that align to common use cases · Share playbooks between SecOps teams · Automated triage and prioritization of alerts from other security portfolio solutions	Cisco XDR

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA), Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands