cisco SECURE

10 ways Cisco delivers XDR capabilities today

The purpose of this eBook

Over the past 10 years, our mission at Cisco Secure has been to develop, acquire and integrate a security portfolio that simplifies operations, accelerates team success, and positions organizations to secure their futures. Other vendors have recognized the critical nature of this effort and followed suit in their own manner. The result of these efforts are solutions that bring detection and response tools together into a platform that promises a myriad of benefits. Gartner has recently defined a market category for these offerings – Extended Detection and Response (XDR). As is often true with new security concepts, vendors are quickly adopting this terminology to showcase their products' capabilities.

This is where things get tricky. Some vendors are using it as a marketing strategy for their existing solutions, others explicitly naming their products “XDR”. With the same term being used in multiple ways it can be hard for buyers to understand what it actually means.

> Cisco has a broad portfolio. We take a comprehensive view to protect our customers...integration is an essential element to our platform strategy and is key to delivering real automation, visibility across all major threat vectors, and improving efficacy while reducing the response time to security events.
>
> Gee Rittenhouse,
>
> SVP Cisco Security Group,
>
> 2019

Table of Contents

1. The need for XDR
2. Gartner's definition
3. Cisco's perspective
4. 10 XDR use cases to achieve better security outcomes
    1. Precise monitoring around user and entity behaviors whether on-prem or not, managed or not
    2. Reduced detection times, even for subtle or hidden attacks via insider, unknown, or encrypted threats
    3. Enriched alerts with cross-product context that streamline operations
    4. Visualized root cause analysis from execution to access, lateral movement to exfiltration, and more
    5. Accelerated decision-making with improved coverage of MITRE ATT&CK matrix
    6. Faster outbreak control with improved coverage of, and automated, MITRE ATT&CK mitigations
    7. Automated “See once, block everywhere” with shared indicators and intelligence
    8. Scaled data retention in the cloud for better forensic analysis
    9. Improved compliance posture by detecting regulatory, zero trust, and custom policy violations
    10. Radical openness that puts any vendor lock-in to shame
5. Next steps

We want to cut through the noise and provide some clarity on XDR.

Read on to:

- Understand the needs driving XDR adoption
- Explore Gartner's definition of the category
- Learn how Cisco delivers XDR use cases with our solutions
- Discover ways to start your XDR journey

Modern security goals:

- Integrate **security data** and tools
- Standardize processes and **eliminating time-consuming tasks**
- Enable **cross-team collaboration**
- Reduce **time to detection**
- Accelerate processes through **playbook-driven automation**
- Employ **proactive measures** regularly
- Achieve **compliance** consistently

Your security goals probably feel out of reach, but that's not your fault

If you're like most security teams, strong detection and response is a mission-critical pursuit that is often illusive. No matter how much you invest, there's constantly a need for "one more layer" of security. Threats continue to increase in sophistication, the perimeter continues to expand, work habits continue to be challenged, and business resiliency needs to be prioritized more than ever. As the attack surface grows, detection gets harder and dwell times go up, putting businesses at risk.

What's wrong with isolated solutions?

- Data logged by security tools is **analyzed in isolation** – lacking the fidelity to detect hidden attacks.
- Alerts are **prioritized in isolation** – finding too little malicious intent for teams to act.
- Security teams **respond in isolation** – often one layer at a time and without enough context or coordination.

With the plethora of security tools available today, why isn't the paradigm shifting? Because all of your security solutions were likely designed and built in isolation and they don't natively integrate with one another in any meaningful ways. Since effectively defending against modern threats is predicated on gaining a complete-enough picture across all control points, having a patchwork of non-integrated point solutions simply doesn't make the cut anymore.

Services are usually available to bring multiple different point solutions together, but they're generally expensive. These siloed technologies prevent streamlined security processes and result in important decision being made in isolation and with only a fraction of the available data.

In theory, adding a new SIEM (Security Information and Event Management) or SOAR (Security Orchestration, Automation, and Response) tool to a security environment can provide some incremental benefits including analytics and automation. However, In practice most security teams don't have the time, knowledge, or staff on hand to perform the level of calibration required to integrate their detection and response capabilities through these tools. And even when they do, adding a new layer of security to the environment requires an unpredictable amount of recalibration. While valuable in certain contexts, the integration achieved through SIEM or SOARs aren't enough to overcome the underlying incompatibilities between your security solutions that are preventing you from detecting threats rapidly and reducing response times.

This translates to teams that are buried in alerts, unable to improve metrics like mean time to detection (MTTD), mean time to remediation (MTTR), and end up struggling to make time for other critical tasks like identifying opportunities for automation and fine-tuning critical policies.

Data Breach 2020
Ponemon

Enter XDR

XDR solutions were designed to alleviate the challenges of too many vendors, too little integration, too little coordination, and too little time.

Gartner defines Extended Detection and Response (XDR) as a unified incident detection and response platform that automatically collects and correlates data from multiple proprietary security components. This means that XDR solutions operate across various layers of detection and response tools, normalize their different datasets, run high-fidelity analyses, and coordinate actions to make it easier for teams to understand the full scope of security issues and remediate quickly and efficiently.

The strength of an XDR system is rooted in three critical capabilities:

First, it must **centralize collections** of historic and real-time **event data** in common formats and make it available for **fast indexed searches** over indefinite periods through high-performance and **scalable storage** resources.

Second, it must use **multiple machine learning techniques** to analyze huge amounts of telemetry data from multiple products to **detect subtle malicious activity**.

Lastly, it must offer **automation capabilities** to take care of routine tasks that **accelerate response** — or even proactively improve protection and posture.

XDR vs. SIEM or SOAR

While similar in function to SIEMs or SOARs, XDRs are differentiated in three ways.

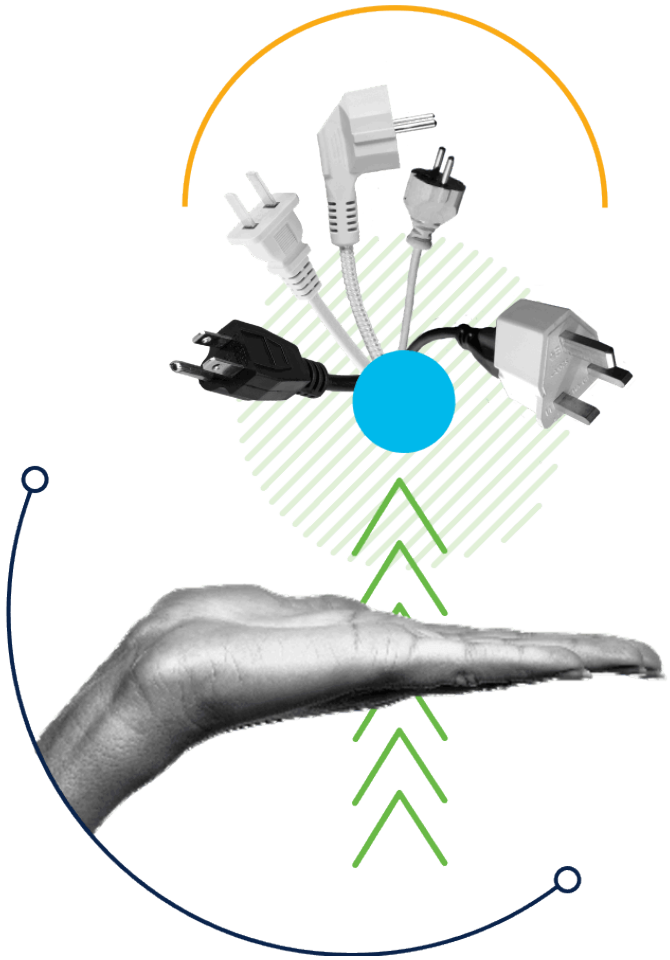
First, the level of turnkey integration is much higher and does not require expensive, labor-intensive calibration.

Second, XDRs are focused solely on threat detection and incident response and have much better detection and analysis labs.

Third, they are generally built on cloud-native architectures and deploy rapidly.

In summary

XDR solutions enable more efficient and effective security operations, while lowering the overall total cost of ownership of the solutions they integrate. This making the promise of these systems highly compelling for any enterprise company.

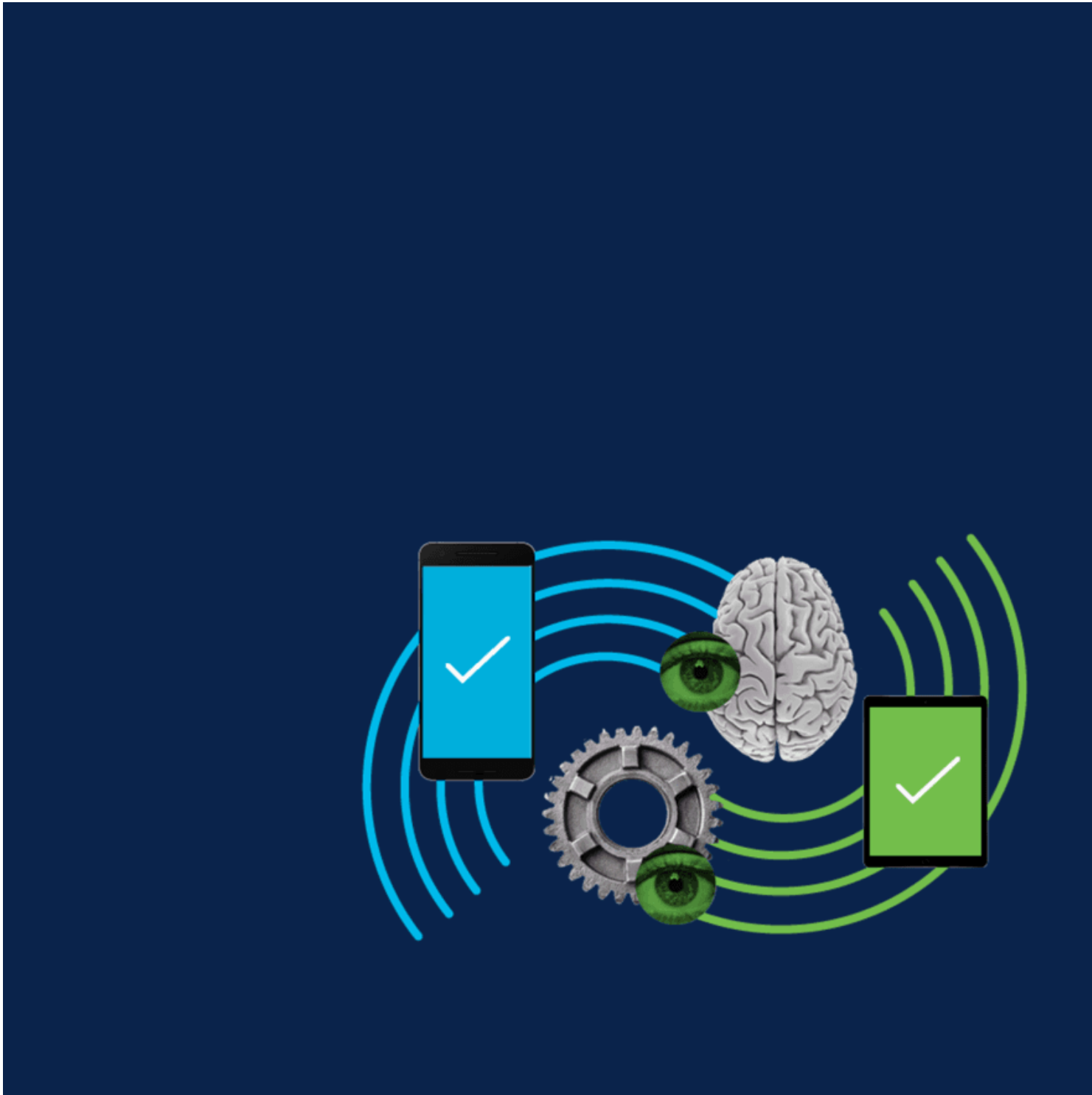


Don’t trust everything labeled XDR

While a unified detection and response platform is a simple concept to grasp, it is difficult to execute one in practice. According to Gartner, unifying data sets together meaningful ways is the central challenge of building an effective XDR platform. Again, security solutions are often built stand alone and generally lack APIs, compatible database structures, and data normalization functions; even when made by the same vendor. While APIs are improving, understanding the different data sets and getting the right syntax in place to offer a single view of across your entire environment requires an incredible amount of work.

Bottom line, XDR is not a solution that can be slapped together quickly. Unfortunately, that hasn’t stopped vendors from trying to do just that. Many that sell stand-alone Network Detection and Response (NDR) or Endpoint Detection and Response (EDR) solutions are increasingly forming “partnerships” to make XDR claims. However, due to the loose and non-native integrations between these partnerships, they cannot deliver on the promise of the XDR.

The broadest, most integrated set of XDR capabilities on the market



A proper interpretation of XDR

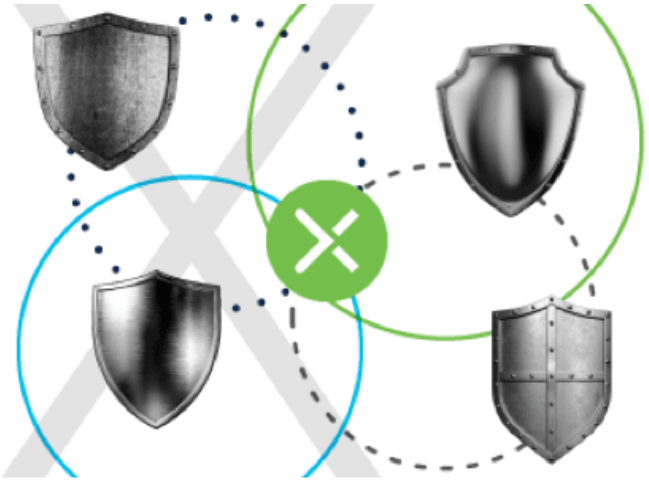
It's Cisco's perspective that in order to deliver a robust XDR solution, it's essential to have three components in balance.

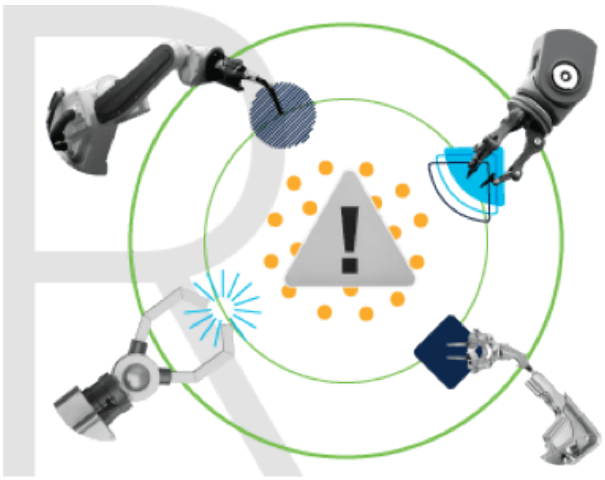
The solution must bring together many different control points and data sources – "**X**".

It must make detection smarter and faster with machine learning-enhanced analytics – "**D**".

And it must reduce dwell times through easier investigations, faster responses, and more automation – "**R**".

Any imbalance between these three elements will not deliver the advertised promises of XDR. As we've already pointed out, analytics aren't as effective when they are used in isolation. Likewise, if you have a bunch of integrated solutions, but lack robust detection analytics – you're similarly out of luck.





Cisco delivers the broadest XDR capabilities through...

Built-in eXtensions – Simplify breach defense by natively connecting detection to response with capabilities integrated within each other products' consoles across the broadest portfolio.

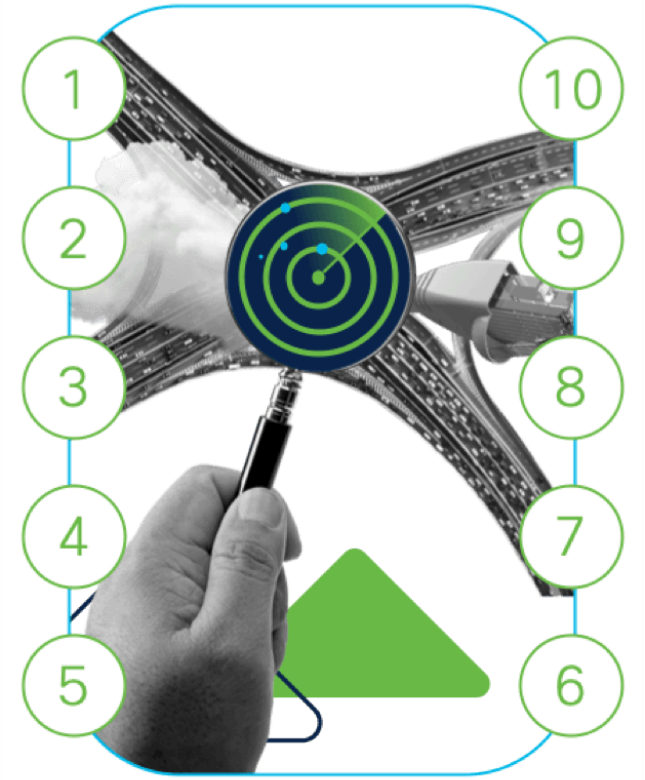
Intelligent Detections – Identify malicious intent and risk exposure more accurately by connecting machine learning-enhanced analytics across the most data sources.

Confident Responses – Reduce threat dwell times by pinpointing root causes with visual investigations and by connecting playbook-driven automation across the most control points.

We've been integrating our solutions for over 10 years.

Cisco enables the XDR capabilities mentioned earlier across the network, cloud, and endpoint control points with our proprietary Network Detection and Response (NDR) and Endpoint Detection and Response (EDR) solutions. Our EDR delivers visibility, quick detection and easy response for all managed devices in your environment. To cover all unmanaged devices and cloud-native systems, our NDR analyzes traffic flows between any entity. With the two, you can see more broadly and with greater understanding. The critical element of differentiation for Cisco is that our platform, SecureX, unifies data, analytics and automation across NDR, EDR and beyond, to offer a simpler and broader approach to XDR. With Cisco, you can boost operational productivity with more intelligent detections and more confident responses built in.

10 XDR use cases to achieve better security



1. Precise monitoring around user and entity behaviors whether on-prem or not, managed or not
2. Reduced detection times, even for subtle or hidden attacks via insider, unknown, or encrypted threats
3. Enriched alerts with cross-product context that streamline operations
4. Visualized root cause analysis from execution to access, lateral movement to exfiltration, and more
5. Accelerated decision-making with improved coverage of MITRE ATT&CK matrix
6. Faster outbreak control with improved coverage of, and automated, MITRE ATT&CK mitigations
7. Automated “See once, block everywhere” with shared indicators and intelligence
8. Scaled data retention in the cloud for better forensic analysis
9. Improved compliance posture by detecting regulatory, zero trust, and custom policy violations
0. Radical openness that puts any vendor lock-in to shame

cisco SECURE

10 XDR use cases to achieve better security

1. Precise monitoring around user and entity behaviors whether on-premises or not, managed or not

Ensuring detection and response capabilities across all devices – managed and unmanaged – is a key need for all organizations, especially during times when work conditions are in flux and moving remote. Cisco's EDR technology gives detailed visibility, tracking, and control over all managed devices and then uses NDR to manage the rest.

NDR uses entity modeling to classify any device or entity within the network or cloud – servers, printers, MRI machines, thermal controllers, containers, etc. – and establishes a baseline of normal behavior using over 100 different behavioral models and more than 400 machine learning classifiers.

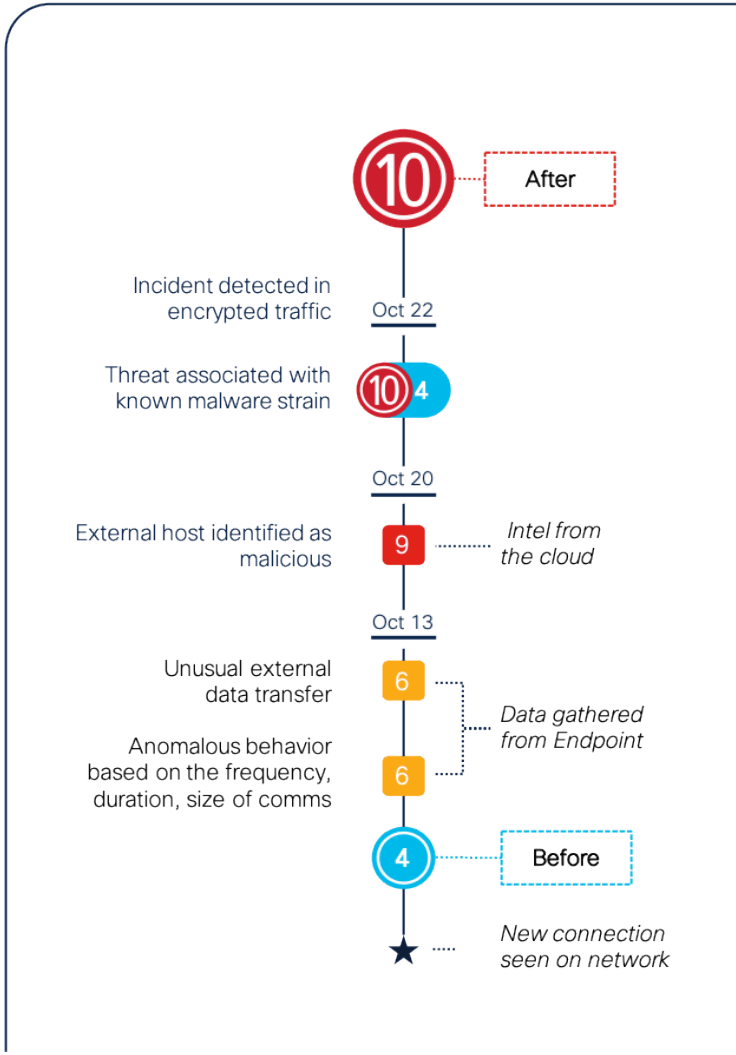
Once classified, it can detect rogue, alarming, abnormal entities, and suspicious traffic flows, even in encrypted traffic. And because SecureX offers visibility into both managed and unmanaged devices, we're able to detect and block malicious activity that involves both – like if an HVAC system used a laptop to send information. Additionally, all device activity is monitored and recorded for future investigation, so that in the event of a breach, all historical information at the network, device, and file level is instantly available to teams.

Teams that have adopted SecureX have reported an 85% reduction in the time required to remediate attacks, saving themselves 4-6 hours per week for investigation or 100 hours per workflow for automation.

> Cisco provides us with full visibility into things such as fake devices, DHCP servers, and anomalous flows between devices and servers"
>
> Jason Skaggs
>
> Security Manager
>
> Little River Casino Resort

2. Reduced detection times, even for subtle or hidden attacks via insider, unknown, or encrypted threats

Time is always of the essence when security is concerned. Cisco Secure solutions deliver extended detection in both passive and active ways by combining weak signals from multiple security components into strong signals of malicious intent to alert you to threats that would have otherwise been missed. Multilayered machine learning engines (supervised, unsupervised, statistical, and behavioral) run in the environment at all times. To classify entities against threat actor models, these engines detect anomalies and correlate them with attack patterns and known campaigns, even within encrypted traffic. The activity descriptions and behavioral and forensic profiles for emerging threats you'll see from these machine learning engines also provide the layers of inference used to reach the verdict.

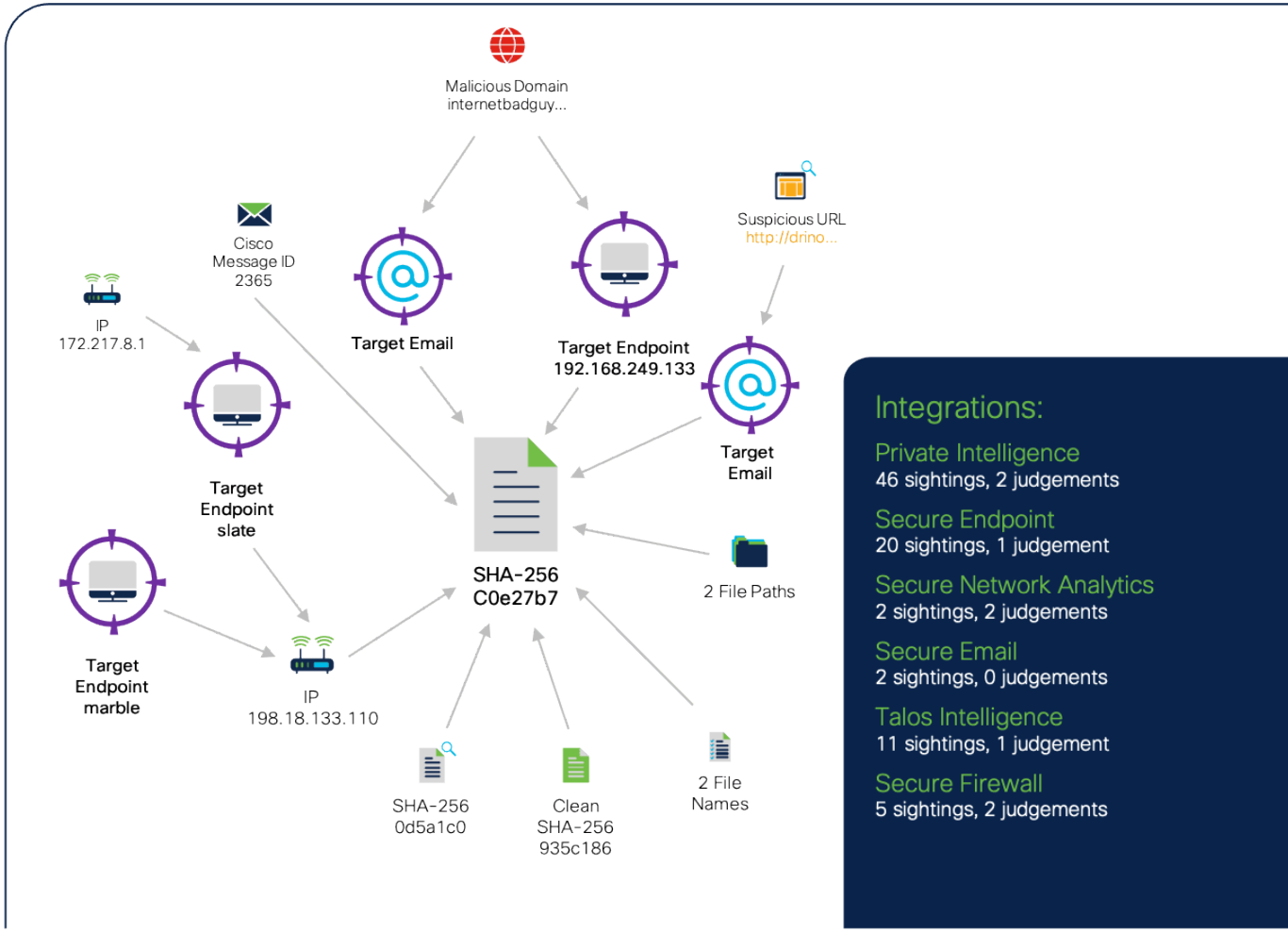


The net of this is that you are able to identify suspicious behaviors that you didn't even know you should have been looking for – like scanning, beaconing hosts, data hoarding and more – in real-time and respond to them immediately. Furthermore, when you need to accelerate specific investigations, you can proactively threat hunt for malicious, hidden artifacts in real time, quickly telling incident responders a narrative of how an attack was spotted, how it evolved, and what to do next to remediate the situation before it becomes a real problem. Simply type the name of an artifact into the search engine of our security platform and explore detailed context, logs, and telemetry from the entire network down to the endpoint level. You'll immediately know if that artifact has been seen within your environment, what geographies it's associated with, the communications related to it, which devices were involved, and more. Customers have reported that with these XDR capabilities in their environments, detection times were reduced by 95% and dwell times by 85%.

> With Cisco, we increased our network visibility by 100% and are now able to catch 50% more network threats. We used their technology to avoid WannaCry attacks and saved around $1M by keeping our networks online."
>
> Nagy Gyula
>
> Senior Security Expert
>
> Magyar Telekom Plc

3. Enriched alerts with cross-product context that streamline operations

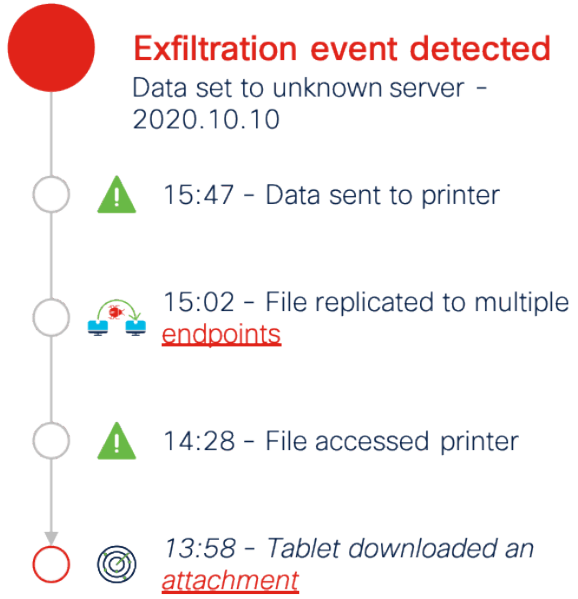
SecureX and the Cisco Secure portfolio optimize your team's bandwidth to make the waves of useless alerts that typically burden security teams a thing of the past with one of the lowest false positive rates in the industry. Before any alerts are created, Cisco Secure indexes a detailed view of the environment – network, endpoint and cloud – running continuous file and traffic analyses to understand every asset, including its posture, associated user identity, relevant policy settings, and typical behavior patterns.



This information is augmented via a detailed view of all activities that took place on each endpoint – including when files first appeared, how they have behaved since arrival and all relevant interconnections with other security layers connected to the platform. Multi-layered machine learning then correlates threat behaviors seen in the environment with those seen globally to discover anomalous and malicious network or cloud activity that is indicative of a breach. When an alert is generated, all this information is available in a consistent location and with just a few clicks, teams can explore a full picture of the situation.

4. Visualized root cause analysis from execution to access, lateral movement to exfiltration, and more

It's difficult to understand something that isn't laid out in a way that makes exploration easy. SecureX delivers a clear, easy-to-read interface that surfaces possible compromises by event and hosts, displays alerts that are prioritized with threat severity scores, and recommended remediation efforts. Drill down into an alert and you'll see visual forensics showing every device, traffic flows, and a file trajectory that shows all associated artifacts – from email attachments to web requests.



Now that you see the root cause, you can easily control the outbreak.

Check out use case 6 to see how we help you do that.

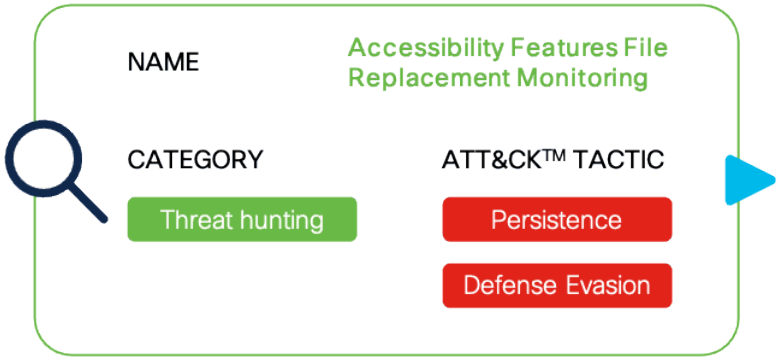
Because our patented retrospective security technology tracks the movement of every file and flow, forensic data is available at any time. With this continuous monitoring, new threat information is correlated with historical data to automatically quarantine files the moment they start to exhibit malicious behavior. This automated response to the latest threats means faster time to detection and greatly reduces the proliferation of malware. In the event of a breach, security teams can see when it started, when it was discovered, what type of tactics were used, and a summary of the malware – or fileless malware or a malicious insider – behind the actions. Additionally, they can explore what type of information was exfiltrated, when and where it was sent, and are given recommended steps for remediation.

> Cisco gives us unprecedented visibility into our environment. It's like a time machine that allows us to analyze threats and intrusions even before they become known malware. Incident response has become a matter of minutes with the actionable alerts in the security console."
>
> Wouter Hindriks
>
> Team Lead Network & Security
>
> Missing Piece

5. Accelerated decision-making with improved coverage of MITRE ATT&CK matrix

Choosing the right alert to investigate is one part of the battle that we make easier with more nuanced and more accurate alerting. But that's just step one – next you must determine precisely WHAT is happening and HOW to act, which isn't always easy. This is why we've mapped our security solutions and key functionalities to MITRE ATT&CK – a framework focused on understanding the specific tactics, techniques, and procedures used by attackers to infiltrate systems. This makes it easy for teams to see the type of mitigations they have available, which ones to use, and when to use them.

For instance, when you click on an alert you can see any associated artifacts, where they fall in the MITRE ATT&CK framework and get recommendations on how to respond to the situation. You can also run global queries that map to specific MITRE categories so you can easily assess your security posture and remediate areas of hidden compromise.



Tactics	Defense Evasion
Techniques	Data from Local System Schedule Task/Job Scripting
Summary	Compromised by a Valak malware variant that uses screen capture, reconnaissance, geolocation, and fileless execution....[Expand]
Remediation	We recommend: • Isolation affected hosts from network • Perform forensic investigating • Upload suspicious files to Secure Malware Analytics

Why should I care about MITRE ATT&CK?

ATT&CK is a collection of the methods used by cyber attackers to get access to your environment. MITRE took these the hundreds of tactics and mapped them to a relatively short list of 41 mitigations.

These mitigations make it easier to have security conversations and discuss mitigations like “restricting web-based content” rather than asking a litany of questions such as “how do we prevent access token theft?” or “how do you stop a drive-by compromise?"

To learn more check out this blog, this recent whitepaper, or visit cisco.com.

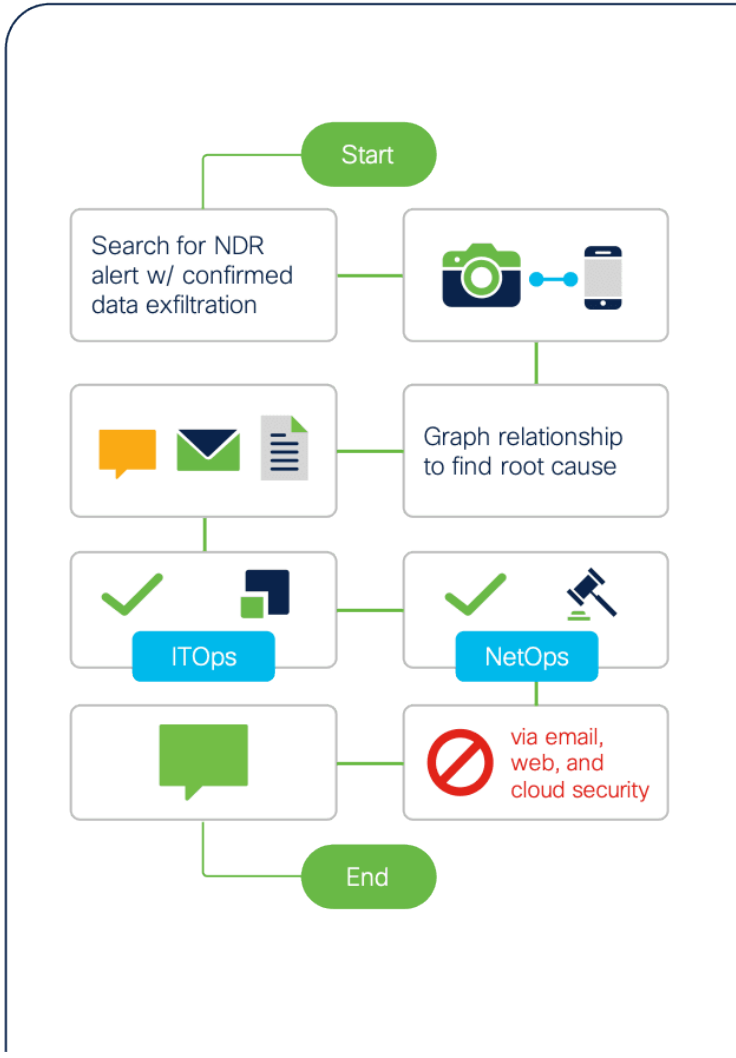
These queries can be inserted into broader security playbooks that are run on regular intervals. Because of the tremendous amount of work that Cisco has done, and continues to do, to map existing IoCs to MITRE ATT&CK, your team doesn’t need to have expertise on how different malware strains behave, the specific remediation steps, or MITRE itself. They’ll be able leverage the knowledge that we’ve coded into our security portfolio to make smarter decisions faster.

Additionally, SecureX offers threat hunting that leverages the expertise of Talos and our Research and Efficacy team to proactively identify threats in customer environments. The combination of these elements deliver high-fidelity alerting from automated, human-driven hunts. The 20 years of experience can more than make up for any lack of security knowledge or personnel.

> For us, using Cisco products is the closest thing to taking the worry out of cybersecurity, and we can go on with other stuff. That for us is a huge, huge gain."
>
> Calum Morrison
>
> Head of E-Health Operations
>
> NHSGGC

6. Faster outbreak control with improved coverage of, and automated, MITRE ATT&CK mitigations

A key component of XDR is its ability to accelerate and automate security responses. No team, no matter the size, has the time to follow up on every alert, leading to the dwell times that we see today. But with exfiltration happening within 3 hours of a breach, the moment a detection occurs, it's a race against the clock. With our security platform's orchestration feature, we share pre-designed workflows for threat hunting (SecOps), vulnerability management (SecOps and ITOps), or traffic optimization (SecOps and NetOps) with your teams. This means your teams don't need to create them from scratch and can learn by example. This way, when you need to build your own automated playbook or customize your samples, you can use our drag-drop canvas with an extensive library of built-in activities including response actions and approvals.

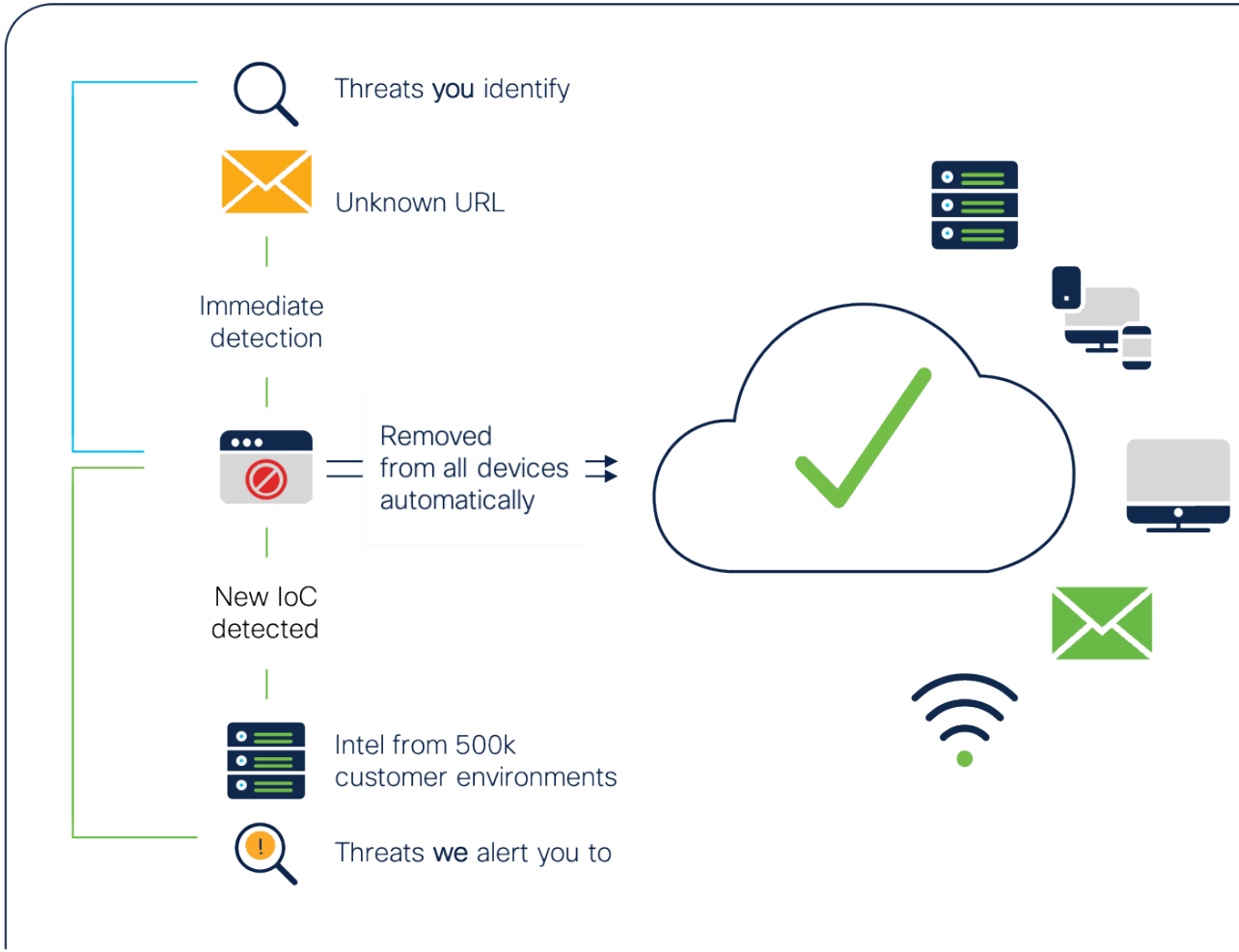


Now, remediation is simpler, and more process driven. With detailed file tracking across every endpoint and correlated with network, email and web activity, you can configure automated file blocking and exploit prevention via analysis results before execution or retrospectively. We've also automated policy actions like taking forensic snapshots, running file analyses, blocking files and domains, and moving entities to a more aggressive protection stance such as network access shutdown or quarantine, meaning your teams have more time to focus on making timely decisions. All of this is brought together into a single view so that you aren't jumping between consoles when time matters most. Our customers have reported that our security platform has helped them reduce time to remediate by 97%.

> When it comes to time-to-detection, Cisco has taken it from one day to one hour. And our time to remediate has gone from hours to minutes. It does it itself, so we don't have to do anything. I can't think of a case where a computer was infected and Cisco did not let us know or missed it...so far it have been 100% successful
>
> Neal Gravatt
>
> Sr Network Engineer
>
> Camden Property Trust

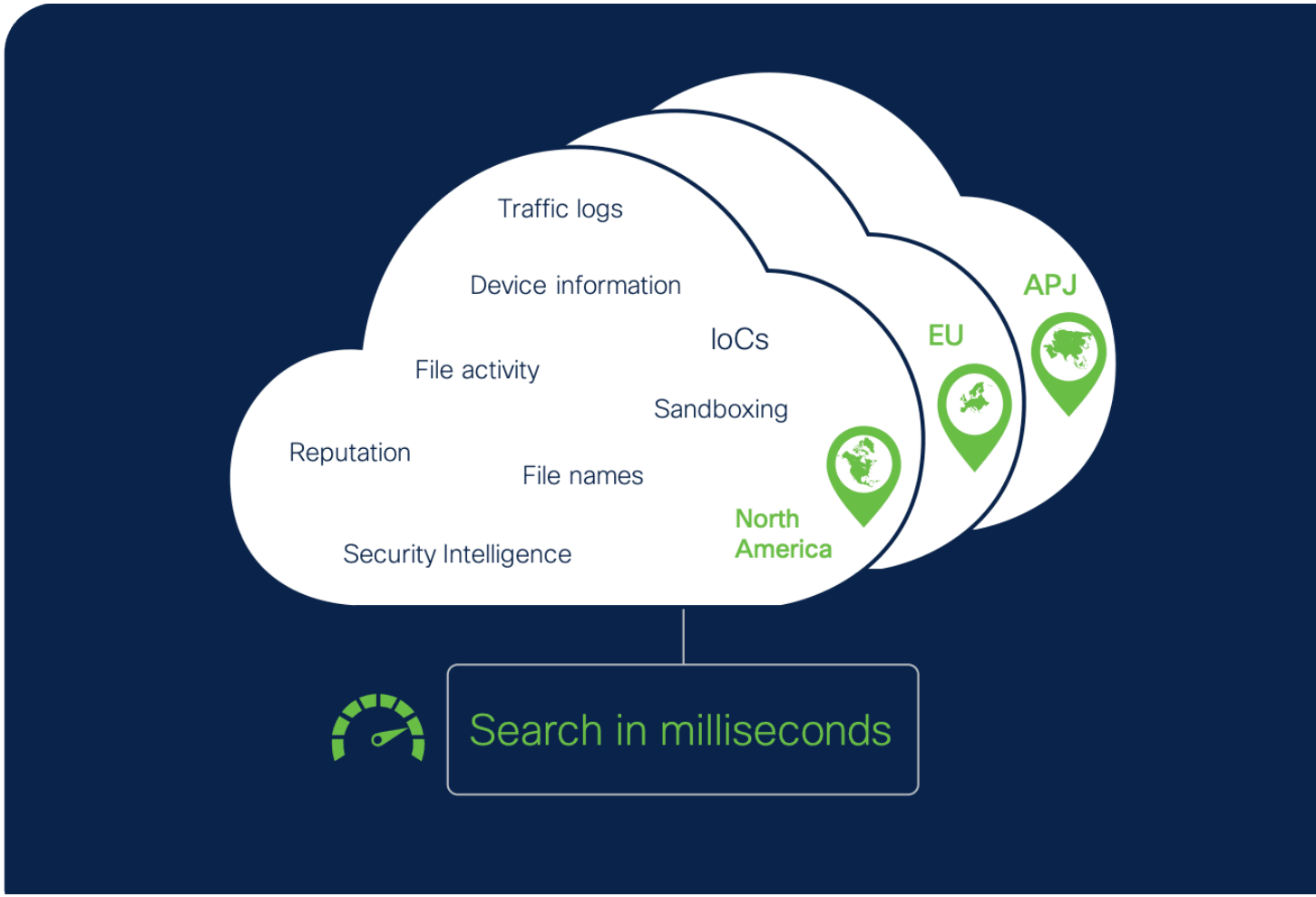
7. Automated “See once, block everywhere” with shared indicators and intelligence

A significant benefit of integrated security layers, a huge global customer base, and the largest non-governmental threat research organization in the world is the ability to act quickly and completely when something does get through. The moment a threat is detected and blocked in your environment, it is automatically removed from other compromised endpoints and blocked across the network, all endpoints, email, web and cloud – across 500,000 Cisco Secure customers. For example, if an endpoint device visits a URL and is compromised, the moment that URL is recognized as malicious, the domain is blocked for all devices and the compromised endpoint is isolated to prevent further proliferation.



8. Scaled data retention in the cloud for better forensic analysis

Storing, aggregating, and analyzing logs at scale is an extremely difficult proposition even for highly seasoned security teams. To make this easier and to deliver the speed of access required for modern security teams, Cisco Secure solutions offload key elements to the cloud. Traffic logs, analysis, historical data on endpoints, file names, file movements, and other patterns are all available at any time, yet are stored off your environment. In addition, our threat intelligence is also powered by the cloud, providing a massive repository of information that is available in real-time.



One example of this scale is how we keep track of every file seen on endpoints, attached in emails, downloaded via the web, or traversing the network or cloud. We continuously analyze any file that is unknown – those without a known good or known bad reputation – since files can initially appear benign but later behave maliciously. Cisco uses our cloud-native malware analytics to retrospectively alert teams when this happens. And in tandem with use cases #3 and #7, show the teams where we saw this file in the past and offer automated or single-click response workflows to remediate the situation.

9. Improved compliance posture by detecting regulatory, zero trust, and custom policy violations

Compliance is a complex issue for many organizations, both to define and achieve. Rules are easy enough to configure in a firewall but determining when and if there is a disconnect is a different story. Human error, lack of expertise and troubleshooting can and will easily lead to gaps in your compliance posture. With built-in analytics across the network, cloud and into endpoints, you'll get visibility into every communication occurring within and outside of your environment. This visibility exposes configuration risks by detecting permissive rules, aging API keys and native compliance alerts in cloud infrastructures. It also provides audit trails and policy violation alarms that can be tuned to business logic.

Did you know?

Cisco is a **two-time zero-trust leader** in The Forrester Wave: Zero Trust eXtended Ecosystem Platform Providers. Forrester gave Cisco the **highest scores possible** in the criteria of ZTX vision and strategy, market approach, ZTX advocacy and the future state of zero-trust infrastructure.

Because visibility extends to all individual endpoints, it's easy to check systems' statuses like OS versions, software vulnerabilities, and recent patches to assess risk exposure. What's more, these types of device and policy checks can be automated in SecureX through live device queries (using a Secure Endpoint feature called Orbital). Additionally, we're able to unify user and endpoint protection to enforce compliance in real time and achieve zero trust. By sharing telemetry from our endpoint agent to analytics and access solutions, we can take information like location, device, posture, and more, into account immediately and automatically adjust access accordingly. This ensures that the right people, have the right access, to the right information – without putting your company at risk.

10. Radical openness that puts any vendor lock-in to shame

One of the most understandable concerns that Gartner puts forward in their analysis of XDR products is vendor lock-in. Rightly so. Integration is a difficult task in and of itself – making integrations that accommodate competitor technologies is difficult in a unique way. But the priority is, and always should be, the security of the customer.

SecureX was built with openness in mind and gives you the flexibility to bring your tools together, whether it's with integrations that are built-in, pre-packaged, or custom.

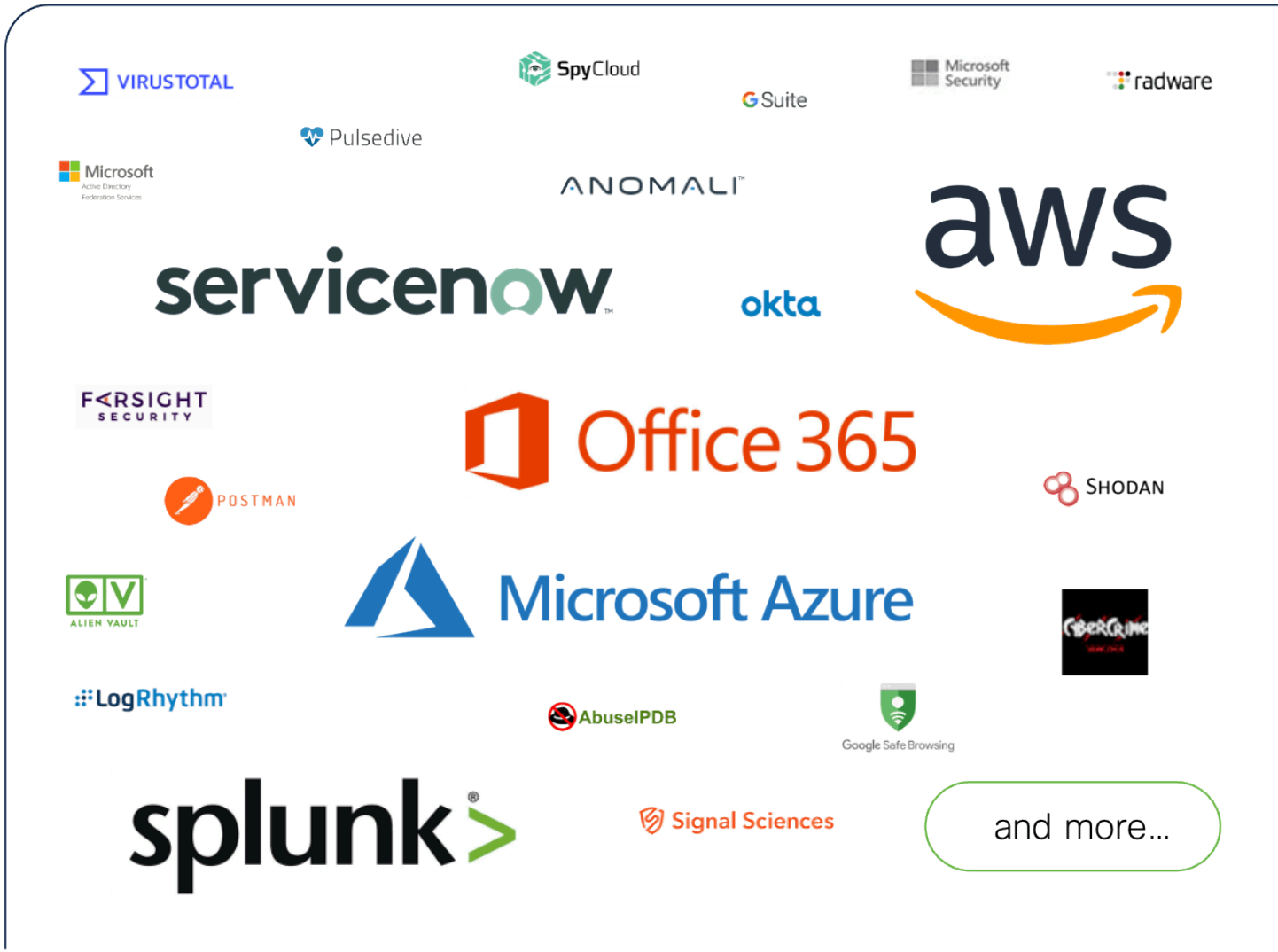
Cisco Secure enables three types of integrations

Built-in integrations - Developed by Cisco and select third-party technology partners, customers can instantly configure built-in integrations in SecureX.

Pre-packaged integrations - With Cisco or partner-developed packages, customers use ready-made scripts and customer-provisioned cloud infrastructure to configure integrations.

Custom integrations - Customers can leverage SecureX threat response APIs and APIs of other technology vendors for any custom integration.

Many tools integrate in one of these three ways, but we also have a browser extension available that enables you to take the integrated functionality of SecureX and extend it to any 3rd party, browser-based tool. Our technology partner ecosystem already includes intelligence sources, operational tools like SIEMs and SOARs, and visibility and protection solutions which help to augment the threat hunting and incident response power built in to SecureX. In fact, 82% of our current customer base agrees that our 3rd party integrations are already adding meaningful value to their investigative capabilities.



Interested in learning more?

5 questions to ask any vendor claiming to have an XDR:

1. How does your XDR unify my current solutions and their telemetry data?
2. Are your analytics able to bring together insights from across attack vectors?
3. Why will I make better security decisions with your XDR?
4. How completely can you automate security response across control points?
5. How can I leverage the security investments I've already made with your XDR?

Cisco has been working hard to deliver these realities for years.

We've covered an incredible amount of ground when it comes to integrating our solutions and still have a way to go.

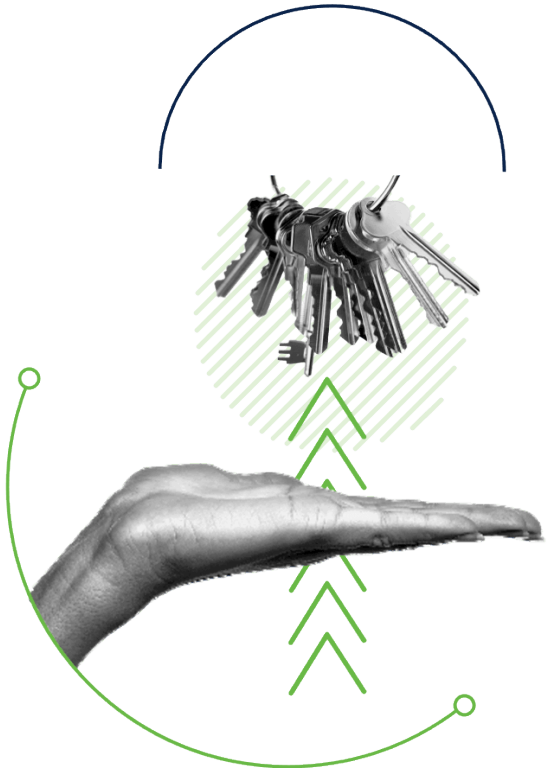
XDR might be a young technology, but most organizations currently have blind spots that XDR capabilities alleviate even if they are not 100% integrated.

With our platform approach you can simplify breach defense by natively connecting detection to response with additional capabilities integrated within the broadest range of security products. We've done tons of development work to help you identify malicious intent and risk exposure more accurately with machine learning-enhanced analytics across the most data sources. This means you'll be able to reduce threat dwell times by pinpointing their root causes with visual investigations and by connecting playbook-driven automation across all of your control points.

We deliver the broadest XDR capabilities on the market

We deliver the broadest XDR capabilities on the market because we've built detection and response into each element of the Cisco Secure portfolio.

As mentioned throughout this paper, NDR and EDR technologies are central in delivering these capabilities through our security platform, though customers also choose to extend detection and response to email security. The specific capabilities discussed in this paper are made possible by key Cisco Secure solutions – SecureX, Secure Network Analytics, and Secure Endpoint.



SecureX

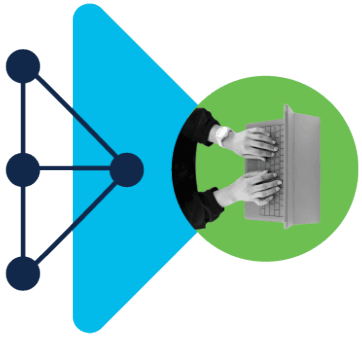
Learn more about our cloud native, built-in security platform and how to bring simplicity, visibility and efficiency to every operation.

For existing Cisco customers, activate your complimentary access to SecureX.

Secure Network Analytics

Learn more about our NDR solution and how to achieve scalable visibility and security analytics across your network and cloud.

Put your visibility to the test with a free, 2 week assessment.



Secure Endpoint

Learn more about how our EDR bolsters your endpoint protection and maximizes operational efficiency.

Start a free trial for Secure Endpoint.

cisco SECURE

Thank you for reading

10 ways Cisco delivers XDR capabilities today