LOGICALIS
Architects of Change

CISCO Partner
Global Gold Integrator

Datasheet

Cisco XDR Activation

Cisco Extended Detection and Response (XDR) is a cloud-native platform experience that's embedded within every Cisco Secure product. Logicalis can help you activate XDR and integrate it with your security infrastructure.

New threats arise daily. Today's organizations have been transforming their businesses so quickly that they've often built complex security architectures with limited visibility into those threats. In addition, multiple and disparate security products make it nearly impossible for security teams to correlate threats between them and limited security resources result in manual and ad hoc processes for investigating and resolving threats. It's no wonder that businesses struggle to holistically manage their security environments.

Today's organizations need an easier way to integrate their security products for greater interoperability and manageability. They need a window into their networks to quickly detect and investigate potential threats. And they need to quickly and efficiently remediate threats, while cutting time and cost.

XDR: The free tool that delivers profound value

XDR is a cloud-native platform experience that's embedded within every Cisco Secure product and connects those products to your security infrastructure.

Integrated and open for simplicity, XDR unifies visibility in a central location, enables automation for greater operational efficiency, and strengthens security across your network, endpoints, cloud, and applications. The result? Simplified security with a single, consolidated view.

Logicalis can help you activate XDR and integrate it with your security infrastructure.

How Logicalis helps you activate XDR to accelerate threat response

Once we've activated XDR and integrated it with your security infrastructure, you'll see all your security technologies on your dashboard, along with a list of your existing product applications and recommendations for new apps. You'll also find security infrastructure integrations that can maximize your investments via common workflows, as well as third-party integrations that can be activated and appear within your dashboard. XDR not only bolsters your threat intelligence, but it also reduces costs and saves time.

Looking for ROI metrics? You can customize ROI metrics based on what's important to your business, such as policies and processes to protect your organization.

Need to automatically respond to events? With XDR Orchestration, Logicalis can help you create workflows from a library of pre-built playbooks. Or you can build your own. Simply name the workflow and then use drag-and-drop functionality to build out the framework of the playbook. Assign tasks and properties to groups and drag and drop them into the workflow. Validate the workflow and your playbook is ready to start automating responses to events.

Finally, you can aggregate device insights from multiple device managers and other security products into one comprehensive view. These contextualized insights give your team the information needed to identify gaps in control coverage, build custom policies, and explore opportunities for playbook-driven automation.

Decrease the cost and risk of a breach with XDR

Even better, XDR enables organizations to detect, investigate, and resolve security incidents faster and with more complete insight, reducing their risk and the cost of a data breach, as well as the likelihood of a breach.

	Year 1	Year 2	Year 3
Cost of a breach	↓40%	↓45%	↓50%
Likelihood of a breach	↓35%	↓40%	↓45%

It was also found that, after using XDR, customers reduced analyst effort per incident by 90% and gained greater insights on security threats in their corporate environments.

Benefits

- **Automate routine tasks –** Automate tasks using prebuilt workflows that align to common use cases or build your own workflows with a low- to no-code, drag-and-drop canvas.
- **Comprehensive device inventory –** Get a comprehensive device inventory with the contextual awareness needed to identify gaps in coverage and simplify security investigation.
- **Faster threat response –** Detect, respond, and recover faster with superior insights and context and accelerate threat investigations and incident management by correlating global intelligence in a single view.
- **Better cyber insurance –** Improve access to and qualify for cybersecurity insurance—and lower premium costs—with a more hardened security posture.
- **Realigned resources –** With less time needed to detect, investigate, and resolve incidents, you can shift incident response to less experienced analysts and give senior analysts more time to address more strategic needs.

Services

XDR Activation Service – For existing Cisco Secure customers or those new to Cisco Secure, this 16- to 20-hour engagement is delivered via Logicalis and NterOne, a Cisco Digital Solutions Integrator. It includes:

- Cisco XDR Overview and its outcomes
- High level Architecture
- Cisco Security integrations and enhanced Telemetry.
- Third Party Integrations : Telemetry and enrichment.
- Understanding APIs: Core of XDR
- Device Inventory Assessment and Posturing.
- Customized Control Center
- Threat Detection with diverse intelligence:
- Behavioral Analytics – Network/Endpoint Detection
- Cloud Alerts : Public cloud detection
- Global Threat Alerts : Firewall Detection
- Incident creation, detection and response w.r.t attack chain.
- Automation and Orchestration Response Workflows

If you would like to inquire more about **Cisco XDR** please contact your Logicalis Account Executive.

LOGICALIS
Architects of Change