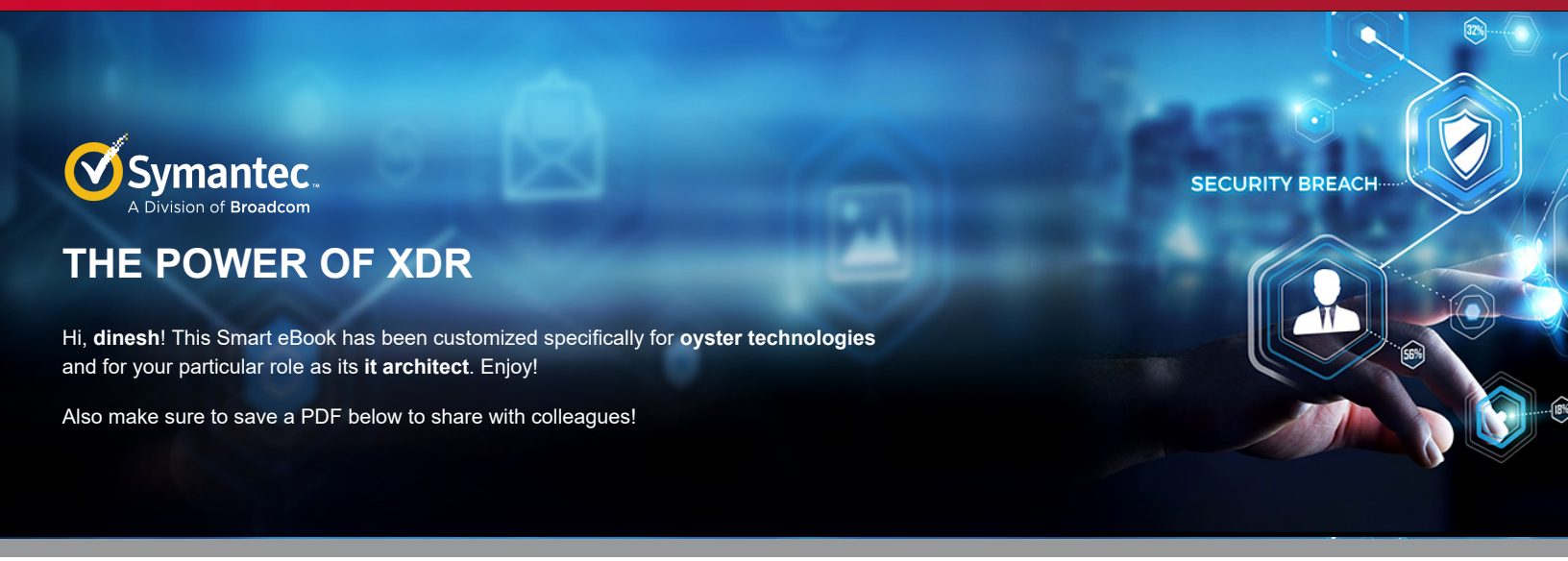


THE POWER OF XDR

Hi, **dinesh**! This Smart eBook has been customized specifically for **oyster technologies** and for your particular role as its **it architect**. Enjoy!

Also make sure to save a PDF below to share with colleagues!

Are you actively integrating?

Enterprises like oyster technologies are increasingly under threat from sophisticated attacks. As a it architect whose responsibility it is to get the right set of tools into the hands of increasingly smaller teams, freeing them from the data noise to ensure optimal productivity and protection, what are you doing about it?

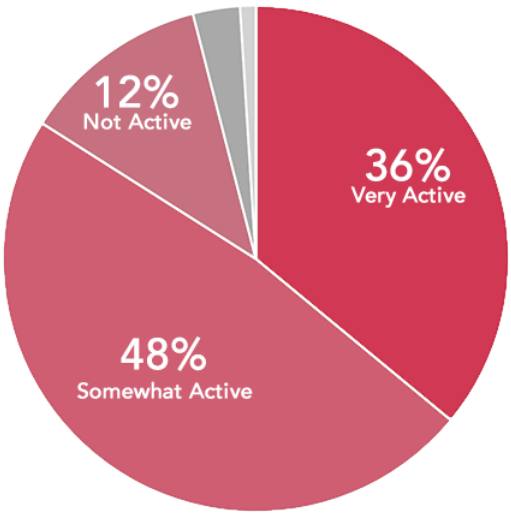
According to the Enterprise Strategy Group, only 36% of enterprise companies are actively integrating the disparate security analytics and operations tools necessary to address threats like these.

Where does oyster technologies fall in that spectrum? Make a selection in the interactive graph input to see…

Next, spend a moment looking through your Smart eBook below. We lay out the challenges faced by enterprises like yours, the specific needs you have in addressing them, and the solutions and unique value we bring to the table with our Extended Detection Response (XDR) solutions.

After all, Symantec is the leader in threat detection security. We've been hunting sophisticated threats for a long time now. So we know exactly how to help you and your team keep oyster technologies safe from attacks and perceived threats that could damage your infrastructure.

Enterprise Strategy Group Survey
Where does oyster technologies fall?



Why XDR?

Visibility Into All Control Points

Unknown Threats Become Known

Automated Remediation

Advanced Persistent Threats

Lack of Control Point Visibility

Overwhelmed SOC

The Challenge

Security teams at enterprises like oyster technologies face multiple challenges when attempting to detect and fully expose the extent of an advanced attack including manual searches through large and disparate data sources, lack of visibility into critical control points, alert fatigue from false positives, and difficulty identifying and fixing impacted endpoints.

And while 92% of security professionals say that improving threat detection is a high priority in their organization, 44% of IT professionals report their organization still takes months to act on insights derived from data analytics or initiatives.

Extended Detection and Response (XDR) gathers information from cross-control points, normalizes the data, correlates it, automatically remediates a known threat on affected devices across multiple control points, and delivers deep insights of unknown threats to the Security Operations Center (SOC), enabling SOC investigators to focus on only the most urgent threats.

The following sections present some specific needs that you likely have in your role as a it architect – and the kinds of solutions to those needs that XDR provides.

Your Specific Needs

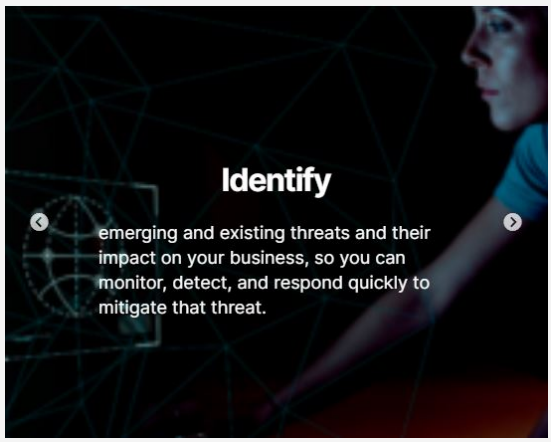
These kinds of sophisticated threats can dwell in your environment an average of 190 days while proactively attempting to evade detection. So to ensure that oyster technologies is fully protected, each stakeholder in the security team has specific areas of focus and responsibility, all of which have to come together for success.

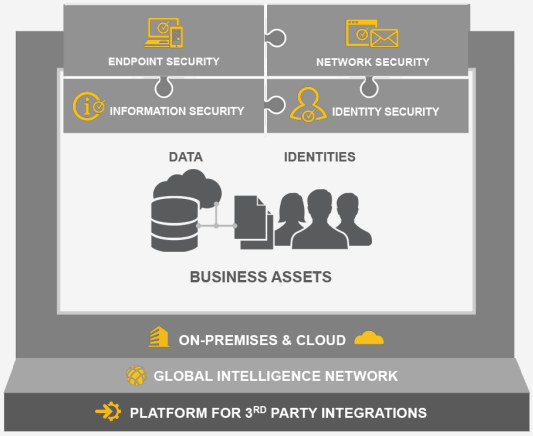
For example, in your role as a it architect it's up to you to do more with less every day. For example, you have to ensure that your ever-shrinking teams have the right tools to not only maintain data security – but to improve it. This means tools that free up staff to focus more on security projects and less on decentralized data noise, and that align business requests with your current set of team skills.

Facing a list of needs like this, and knowing that you have to get it right every time, the question becomes this: What solution covers all these needs and gives you the confidence in your role that oyster technologies is truly protected?

The answer is Integrated Cyber Defense, which quickly and easily enables XDR. Here's why…

The it architect must…





Our Solution: Integrated Cyber Defense

Symantec Integrated Cyber Defense (ICD) enables Extended Detection and Response (XDR). Like XDR, ICD lets an enterprise leverage telemetry from all threat vectors, normalize and correlate it across control points. Symantec integrates our industry-leading solutions in Endpoint, Web, Email, Network, Cloud, InfoSec, and Identity into a single, dynamic ecosystem that keeps your business better protected.

Symantec Integrated Cyber Defense delivers Endpoint Security, Network Security, Information Security and Identity Security across on-premises and cloud infrastructures, to provide the most complete and effective asset protection in the industry.

As a it architect this means you can optimize the efforts of smaller teams and reduced skill sets without sacrificing enterprise-wide security. Your Level 1 analyst can now do Level 2 work. For example, XDR provides correlation of telemetry from all control points, applying artificial intelligence and machine learning to analyze threat intelligence. And with Symantec Integrated Cyber Defense, we've done the work to ensure that needed integrations are already complete or easy to implement.

Why Symantec?

Symantec is an industry-leader in all primary security categories such as endpoint, identity, email, web, information security, network, and cloud. And we've been in that position for more than 10 years running.

But more specifically for you as a it architect we provide tight integration across all attack vectors and within key underlying security technologies through ICDx, which lets you streamline integrations and logs so you can normalize and correlate threat data for richer threat intelligence, higher fidelity alerts and faster response.

Select the button below to continue your personalized journey…

SCHEDULE A PERSONALIZED DEMO

Symantec™
A Division of Broadcom