FORTINET

WHITE PAPER

Take Control of Security Operations with Consolidation and XDR

The constantly evolving cyber threat landscape and steady stream of cybersecurity technologies designed to address it are challenging for smaller IT security teams. The complexity of multiple products from multiple vendors, along with the volume of alerts generated, can easily overload organizations, especially given the systemic shortage of cybersecurity skills.

An average midsize organization uses a dozen (or more) security tools from a range of different vendors, which together generate thousands of alerts each day. It's not surprising that nearly half of security leaders "report complexity of their environment as among the most challenging aspects of security."[1] And over three-quarters of organizations admit their security architectures are disjointed due to nonintegrated security products.[2] Teams have multiple management portals to inspect, and they must manually connect the data from each of them. As a result, they respond more slowly to alerts, have time for fewer investigations, and run a greater risk of missing an attack in progress.

Making security management and threat mitigation even more difficult is that cybersecurity skills are scarce. It's estimated that it would take an additional 4 million cybersecurity professionals to close the cybersecurity skills gap.[3]

Reduce Complexity

Gartner reports 80% of organizations plan an active security vendor consolidation strategy now and in the future.[4] Goals of consolidation are typically to improve operational efficiency or cyber-risk posture, while reducing costs or staffing needs. In doing so, they must consider the pros and cons of a platform vs. point-product approach. For most organizations, consolidation is likely to happen around a small number of strategic platforms that are supplemented by select point products rather than an "all-or-nothing" structure.

Consolidation

Rather than immediately trying to consolidate down to a single vendor, an easy first step is to consolidate around a small number of strategic security-vendor platforms (possibly complemented by a select few point-product vendors if needed). Natural groupings (and platforms) have traditionally been endpoint and network, with cloud and identity management platforms increasingly added to the mix.

Every security strategy must make sure to cover all attack vectors, especially as the digital attack surface continues to expand and networks evolve. While most attacks ultimately seek out the endpoints—end-user computing, servers, even Internet of Things (IoT)—there are multiple paths cyber criminals take to reach them. The majority of malware is delivered by email with most of the remainder downloaded from the internet, but web applications are the number one source of actual data breaches.[5] And applications can be hosted by the customer on-premises or in the public cloud. And/or, they may use Software-as-a-Service (SaaS) providers. If security controls do not span the entirety of the network, threats will slip through the cracks.

Not only do organizations need to worry about the growing number of attack surfaces but also each stage of attack. Many of today's cyber threats are multistage, making them more challenging to detect, but also offering multiple opportunities to detect and prevent them. Deploying technologies at multiple Cyber Kill Chain stages establishes defense in depth, strengthening benefits gained by security vendor consolidation.

Detect and Respond To Threats Faster

However, as a leading analyst noted, security is a relatively "young" industry and it is still maturing. In fact, it is only now that multiple security platforms—network, email, endpoint, cloud, and more—are coming together under the extended detection and response (XDR) conceptual architecture.

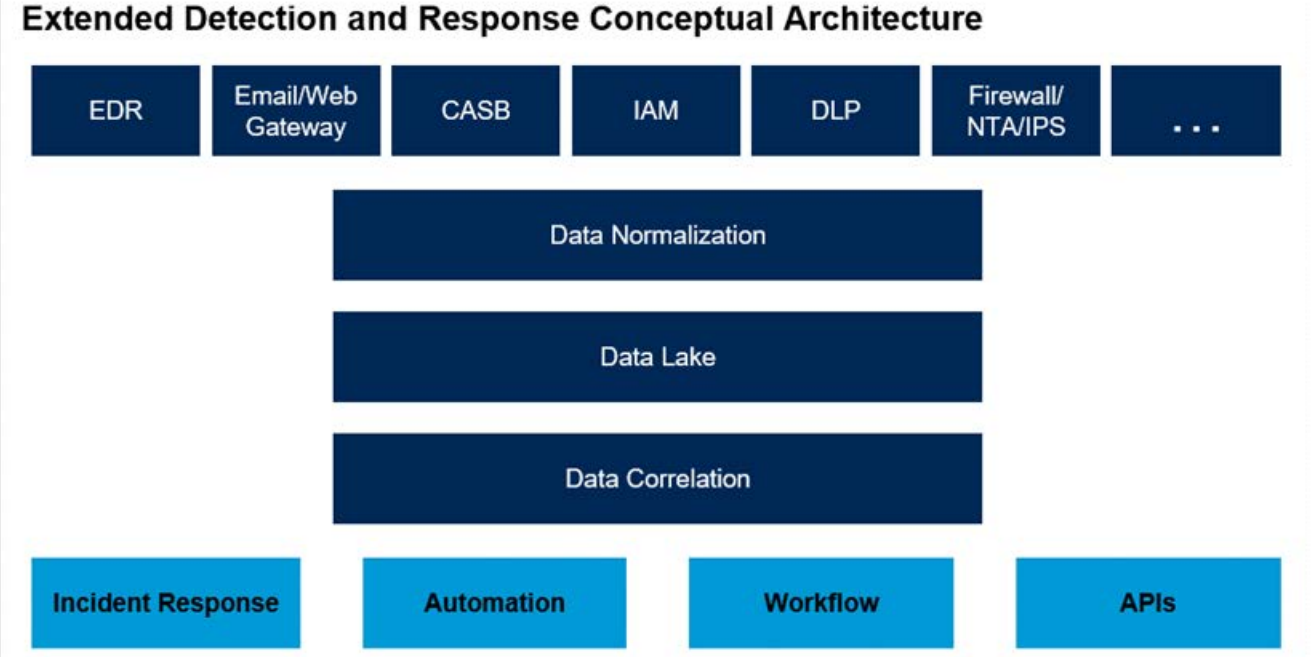

Figure 1: Gartner innovation insight for XDR, March 2020.

An effective XDR solution is able to collect, normalize, and correlate data across security controls. It can help security teams detect threats faster, aid investigations, and speed response.

However, given the emerging nature of the XDR concept, approaches vary. They vary in terms of the breadth of security controls feeding into the data lake, in terms of whether they assist or automate investigation, in terms of the degree of automation vs. orchestration of response, and in terms of effectiveness of the system overall as well as each security control you have to consolidate.

Summary

The early results are in. With consolidation and an effective XDR solution, organizations can greatly improve security posture and improve operational efficiency. For details on what to look for in an XDR solution, read our checklist: "Top 5 Considerations When Selecting an XDR Solution."

[1] "Center Security On Advanced Technology: How A Technology-Led Strategy Helps CISOs Successfully Secure Their Organizations," Forrester, July 2017.

[2] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, May 23, 2019.

[3] "(ISC)² Estimates Cybersecurity Workforce at 2.8 Million," (ISC)², November 6, 2019.

[4] John Watts and Peter Firstbrook, "Security Vendor Consolidation Trends: Should You Pursue a Consolidation Strategy?" Gartner, July 30, 2020.

[5] "2020 Data Breach Investigations Report," Verizon, May 2020.

December 16, 2020 1:06 AM

859744-0-0-EN

D:\Fortinet\White Paper\Red White Paper\FortiXDR - TOF PoV\wp-FA-take-control-of-security-operations-with-consolidation-and-xdr-12152020\wp-FA-take-control-of-security-operations-with-consolidation-and-xdr-12152020