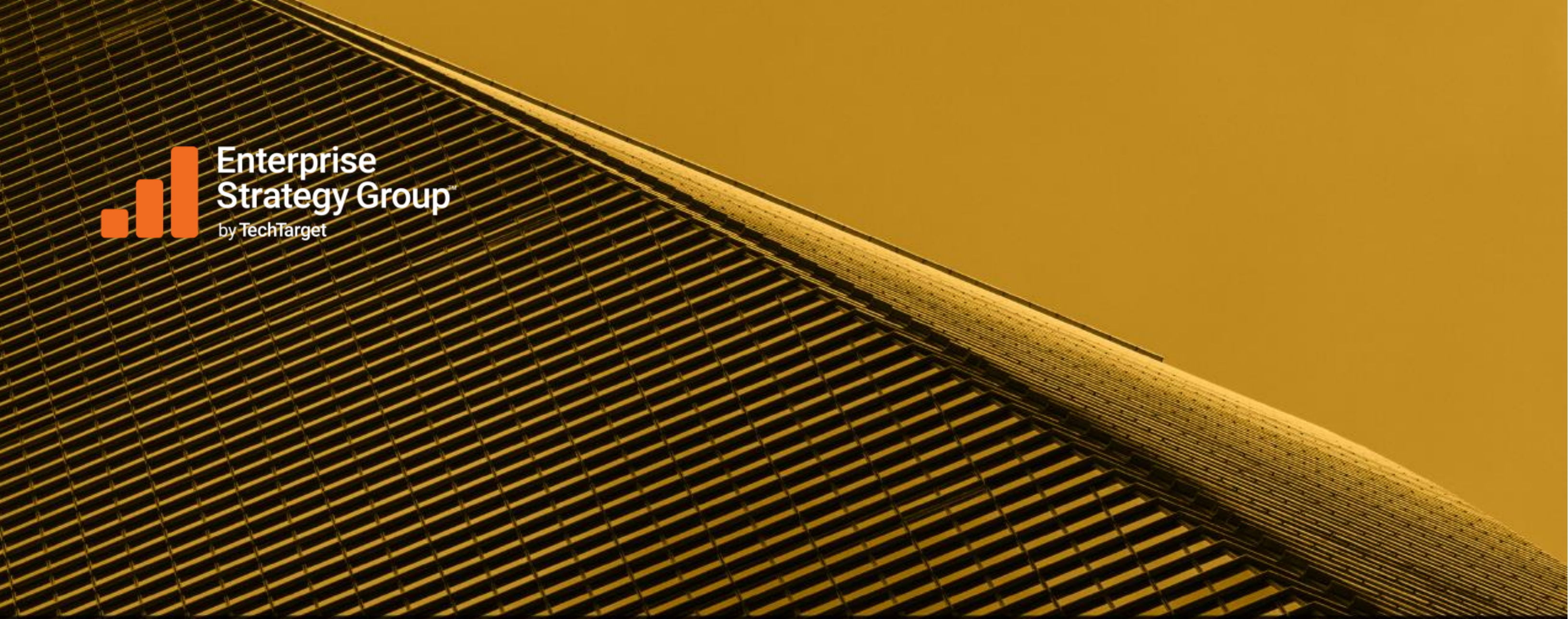


TECHNICAL VALIDATION

FortiXDR Endpoint Protection in the Google Cloud Security Ecosystem

Leveraging the Google Platform to Accelerate the Delivery of Differentiated Security Offerings

By Tony Palmer, Practice Director, and Justin Boyer, IT Validation Analyst,
Validation Services
Enterprise Strategy Group

July 2024

Contents

Introduction

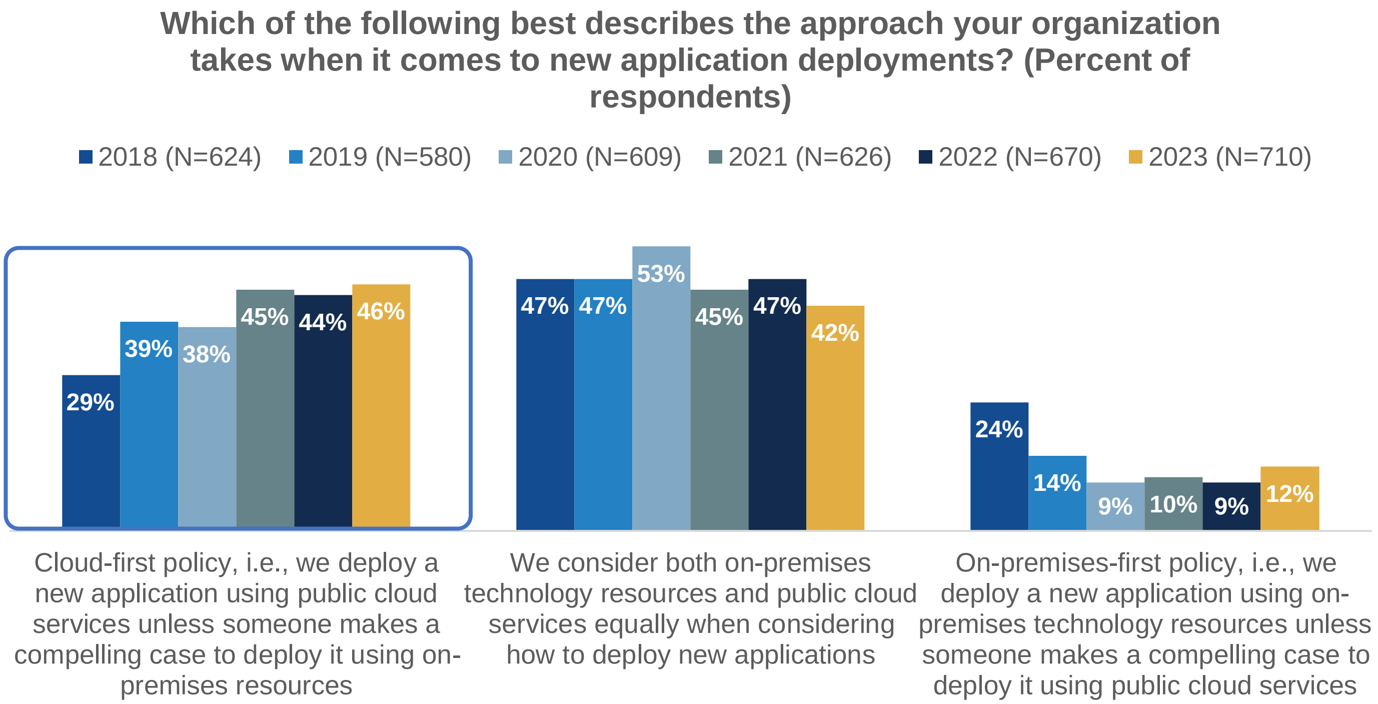
This Technical Validation from TechTarget's Enterprise Strategy Group documents our evaluation of the Google Cloud Security Ecosystem and Fortinet's FortiXDR endpoint security platform. Our analysis focused on how the Google Cloud enables a cybersecurity independent software vendor (ISV) like Fortinet to provide differentiated security offerings and capabilities, accelerate time to market, and help their customers secure their cloud applications.

Background

Momentum for digital transformation is accelerating. Organizations are under increasing pressure to improve productivity and drive innovation to serve their customers and are leveraging cloud services to meet that demand. In fact, 86% of organizations run production workloads on public cloud infrastructure/platforms,[1] and organizations are increasingly adopting a cloud-first policy for new applications (see Figure 1).[2]

Cloud services enable teams to modernize their application development processes for greater operational efficiency, which helps them meet their digital transformation objectives, including becoming more operationally efficient, providing a better customer experience, using technology that enables collaboration, and improving product development.[3]

Figure 1. Cloud-first Policy for New Applications on the Rise



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Organizations recognize the growing complexity across their IT environments, and the ongoing cybersecurity skills gap is not making things any easier. In fact, 42% of respondents told Enterprise Strategy Group that cloud

[1] Source: Enterprise Strategy Group Research Report, *Application Infrastructure Modernization Trends Across Distributed Cloud Environments*, March 2022.

[2] Source: Enterprise Strategy Group Research Report, *2023 Technology Spending Intentions Survey*, November 2022.

[3] Ibid.

computing security was one of the most difficult roles for them to fill.[4] Organizations are looking for ways to efficiently manage risk to support the demands of their businesses with the move to the cloud.

This has serious implications for cybersecurity solution vendors. Organizations with mission- and business-critical workloads in the cloud need to be confident that they can control and secure their environment, and trust in their technology partners is key. Organizations, including ISVs, need access to sophisticated tools to enhance their development efforts across the development lifecycle, and they should be looking for a cloud partner that can provide capabilities and expertise that add value. The right cloud partner provides infrastructure as well as network analytics, visibility, integration opportunities, and complementary security capabilities so customer developers and ISVs can focus on their core mission without worrying about tooling and support infrastructure.

The Google Cloud Security Ecosystem

Google Cloud is designed, built, and operated with security as a primary design principle to help protect its customers against threats in their environments. Google layers on security controls to enable organizations to meet their own policy, regulatory, and business objectives. Application development teams can leverage elements of Google's compliance framework in their own compliance programs.

Google Cloud secures more than 3 billion users globally. To accomplish that, Google's cloud infrastructure doesn't rely on any single technology to make it secure. The Google Cloud stack builds security through progressive layers designed to deliver true defense in depth and at scale:

- Google Cloud's hardware infrastructure is designed, built, controlled, secured, and hardened by Google.
- Google Cloud's infrastructure—designed from the ground up to be multi-tenant—uses a zero-trust model for applications and services, with multiple mechanisms to establish and maintain trust. This means that only specifically authorized services can run, and only specifically authorized users and processes can access the services.
- Data is automatically encrypted at rest and in transit and is distributed for availability and reliability to help protect against unauthorized access and service interruptions.
- Strong authentication protects access to sensitive data with advanced tools, such as phishing-resistant security keys to verify identities, users, and services.
- Google's network and infrastructure have multiple layers of protection that guard customers against denial-of-service attacks.
- At the top of the stack, Google develops and deploys infrastructure software using rigorous security practices, employing round-the-clock operations teams to detect and respond to threats to the infrastructure from both internal and external threat actors.

Google Cloud aligns with the needs of security ISVs to help them deliver better, more capable offerings—and deliver them faster. Google Cloud's economies of scale, software-defined infrastructure, simplicity, shared responsibility, automation, and global reach help ISVs accelerate time to market and optimize the delivery of new products, enhancements, and updates, so customers get newer features, faster.

Google operates from the precept that clients are always in control of their data and is committed to transparency in data handling. Google's privacy commitments and data processing addendum clearly state that Google does not use cloud customer data for advertising, any AI model, or product improvement. Google adheres to its clients' data storage, processing, and management preferences so that organizations control what happens to their data. In addition, all Google customers benefit from the privacy protections and fine-grained security controls built into Google Cloud by default.

[4] Ibid.

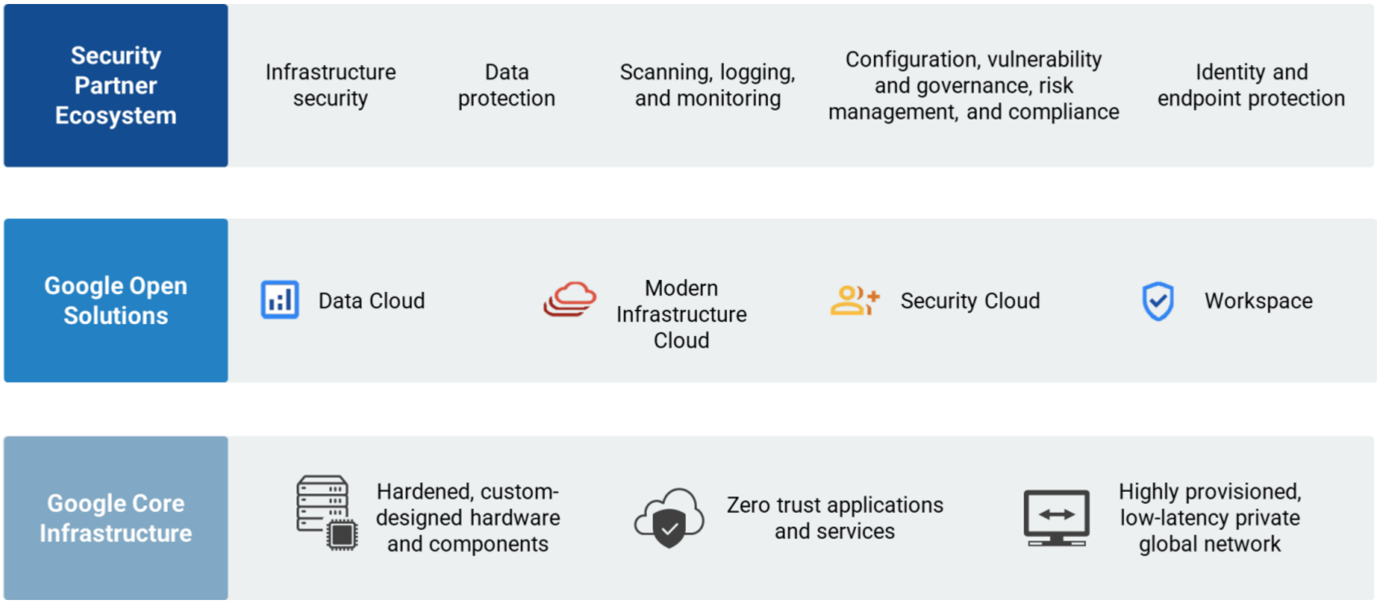
Google's products regularly undergo independent third-party audits, with over 2 million control instances audited annually. Google maintains certifications, attestations of compliance, or audit reports against standards and regulations enforced across the globe. Google Cloud supports customer risk management and regulatory compliance needs with dedicated teams, offering compliance validation, support for due diligence, and security assessments, with an ongoing commitment to continuous assurance.

Google Cloud hardware infrastructure is custom-designed by Google to precisely meet stringent requirements, including security. Google's servers are designed for the sole purpose of providing Google services. Its servers are custom-built and don't include unnecessary components that can introduce vulnerabilities. The same philosophy is imbued in Google's approach to software, including low-level software and its operating system, which is a stripped-down, hardened version of Linux. Google designs and includes hardware specifically for security. Titan, its custom security chip, is purpose-built to establish a hardware root of trust in its servers and peripherals. Google also builds its own network hardware and software to optimize performance and security. Finally, Google's custom data center designs include multiple layers of physical and logical protection. Owning the full stack enables Google to control the underpinnings of its security posture with far greater precision than is possible with third-party products and designs. Google can take steps immediately to develop and roll out fixes for vulnerabilities without waiting for another vendor to issue a patch or other remediation, greatly reducing exposure for Google and its customers.

Google was an early proponent, designer, and practitioner of zero-trust computing. Google developed foundational concepts that underpin zero-trust architectures with its BeyondCorp and BeyondProd models. Operating this way has helped to protect its internal operations over the last decade. Google's zero-trust architecture ensures that only the individual with the correct identity, accessing only the machines specifically authorized by the correct code, is accessing only the data they are authorized to, in the correct context. BeyondProd uses these same core principles to enable partners and Google Cloud customers to protect their operations in the same way, focusing on their own assets and resources and the entities and groups accessing them.

Layered over this foundation of trust are the tools and technologies that Google Cloud provides its partners—which they formerly had to build in-house—to augment their capabilities. The Security Ecosystem uses Google Cloud capabilities to provide trusted security in the cloud, on premises, at the edge, and everywhere in between (see Figure 2).

Figure 2. Google Cloud Security Ecosystem Overview



Security Partner Ecosystem
Infrastructure security
Data protection
Scanning, logging, and monitoring
Configuration, vulnerability and governance, risk management, and compliance
Identity and endpoint protection

Google Open Solutions
Data Cloud
Modern Infrastructure Cloud
Security Cloud
Workspace

Google Core Infrastructure
Hardened, custom-designed hardware and components
Zero trust applications and services
Highly provisioned, low-latency private global network

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Google's **Data Cloud** enables organizations to digitally transform with a unified, open, and intelligent data cloud platform:

- Data Cloud enables organizations to **manage every stage of the data lifecycle**, including databases, business intelligence, data warehouses, data lakes, and streaming on a unified data platform.
- Data Cloud is **open and standards-based** for portability and flexibility, with an extensive partner ecosystem designed for multi-cloud environments.
- Data Cloud incorporates **built-in artificial intelligence and machine learning (AI/ML)**, with comprehensive tools and processes. Organizations can leverage pre-trained models accessed via APIs and low-code custom training to solve real-world problems quickly with integrated analytics and an AI platform, BigQuery ML. ML model development and experimentation is fast-tracked with Vertex AI, an end-to-end ML platform.
- Security AI Workbench provides **generative AI for security solutions**. Security AI Workbench is a platform that enables security partners to extend generative AI to their products, bringing threat intelligence, workflows, and other critical functionality to customers while retaining enterprise-grade data protection and sovereignty.

Google's **Modern Infrastructure Cloud** gives partners and customers the freedom to securely innovate and scale across data centers, edge locations, and the cloud on a transformative, open platform that is designed to be easy:

- Google has a long history of leadership in **open source** development, including projects like Kubernetes, TensorFlow, and others. Open source gives organizations the flexibility to deploy—and, if necessary, migrate—critical workloads across or off public cloud platforms.
- Google Modern Infrastructure Cloud gives organizations the **flexibility to build and run apps anywhere**. Anthos—the modern application platform that extends Google Cloud services and engineering practices to hybrid and multi-cloud environments—delivers portability that helps teams modernize apps more quickly and establish operational consistency across them.
- Modern Infrastructure Cloud provides **autonomy and control over infrastructure and data**, enabling organizations to manage all their apps—both legacy and cloud-native—while meeting sovereignty, regulatory, and policy requirements.

Data protection is core to everything Google does. **Security Cloud** helps partners and customers protect what's important with advanced security tools:

- The **Google Cybersecurity Action Team**, Google's security advisory team, has the singular mission of supporting the security and digital transformation of governments, critical infrastructure, enterprises, and small businesses.
- Google **BeyondProd** helps create trust between microservices—beyond what is possible with traditional network perimeter protections, such as firewalls—using characteristics such as code provenance, service identities, and trusted hardware. This trust extends to software that runs in Google Cloud and software that is deployed and accessed by Google Cloud customers.
- **Google Workspace** has its own ecosystem of cybersecurity partners to extend its native security capabilities. This provides an opportunity for security ISVs to reach Google Workspace enterprise customers. Google Cloud is committed to helping customers achieve their security and risk-mitigation goals, while enabling partners to deliver applications and capabilities that give customers greater security, agility, and resilience—all with significant cost savings. Google Cloud's best practice guidance and tools deliver Workspace capabilities securely and at scale.
- Google has produced numerous **foundational innovations**. Google invented now-standard technologies such as Kubernetes and was an early proponent, designer, and practitioner of zero-trust computing.
- **Support for DevSecOps** includes secure software supply chain.

Google Cloud Enables Advanced Detection and Response with FortiXDR

Ransomware and other malware have continued to plague organizations of all sizes and security capabilities. Enterprise Strategy Group research found that 52% of survey respondents consider ransomware to be among the top three threats to their organization's viability.[5] Additionally, 51% of survey respondents indicated that their current security tools struggle to detect and investigate advanced threats.[6] Fortinet partners with Google Cloud to help organizations meet these challenges through their FortiXDR platform.

Enterprise Strategy Group Technical Validation

Enterprise Strategy Group examined how Fortinet's FortiXDR, summarized in Figure 3, works with Google Cloud to help organizations protect their cloud workloads and endpoints from threats.

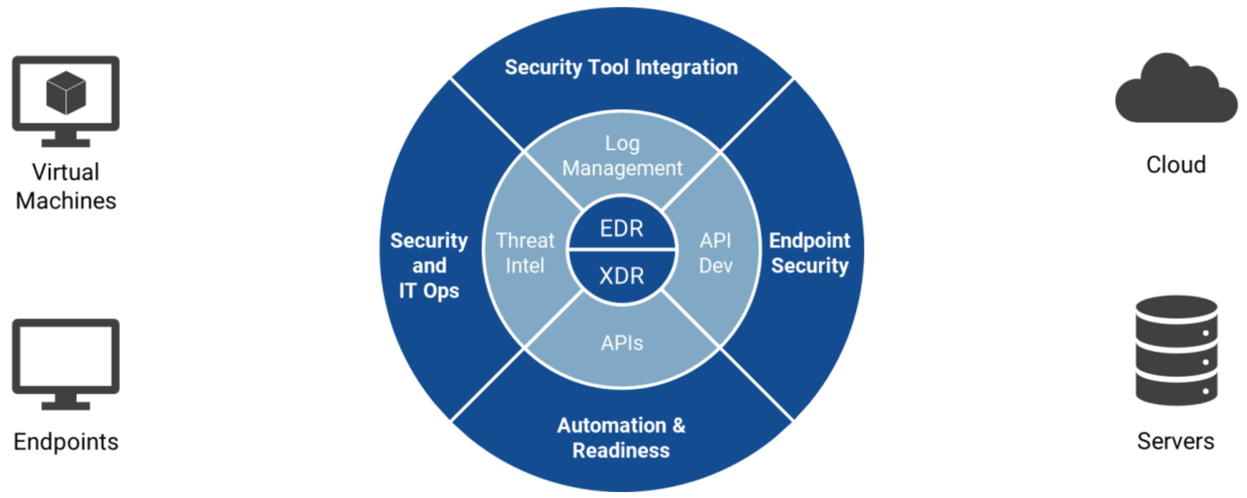
FortiXDR Endpoint Protection

FortiXDR is a cloud-native endpoint security platform, built on top of FortiEDR, that protects endpoints from compromise, working in conjunction with Fortinet Security Fabric and Google Cloud Security Command Center (SCC). It features a lightweight, kernel-based agent that provides visibility into potential attack paths with threat hunting from the workstation to the cloud workload. Operating at a lower level within the system also provides resistance against evasion tactics used by malware to avoid detection.

FortiXDR provides full feature parity across operating systems, accommodating both legacy and current platforms, such as older Linux flavors, Windows XP, and Server 2003. It proactively detects malware, such as ransomware, by monitoring code execution in a protected environment before allowing it to run in a production environment.

The FortiXDR platform incorporates automated response capabilities driven by analytics provided by an organization's data lake architecture as well as by Google Cloud. It can perform extended response remediation actions, such as automatically generating firewall rules to block traffic from malicious IP addresses, blocking phishing emails, initiating quarantines, and taking other measures to isolate compromised endpoints and halt the spread of attacks. FortiXDR also includes a free-to-use REST-based API, empowering organizations to develop custom integrations and implement additional automations as necessary.

Figure 3. FortiXDR Overview



Source: Fortinet and Enterprise Strategy Group, a division of TechTarget, Inc.

[5] Source: Enterprise Strategy Group Research Report, *Ransomware Preparedness: Lighting the Way to Readiness and Mitigation*, December 2023.
[6] Source: Enterprise Strategy Group Research Report, *SOC Modernization and the Role of XDR*, October 2022.

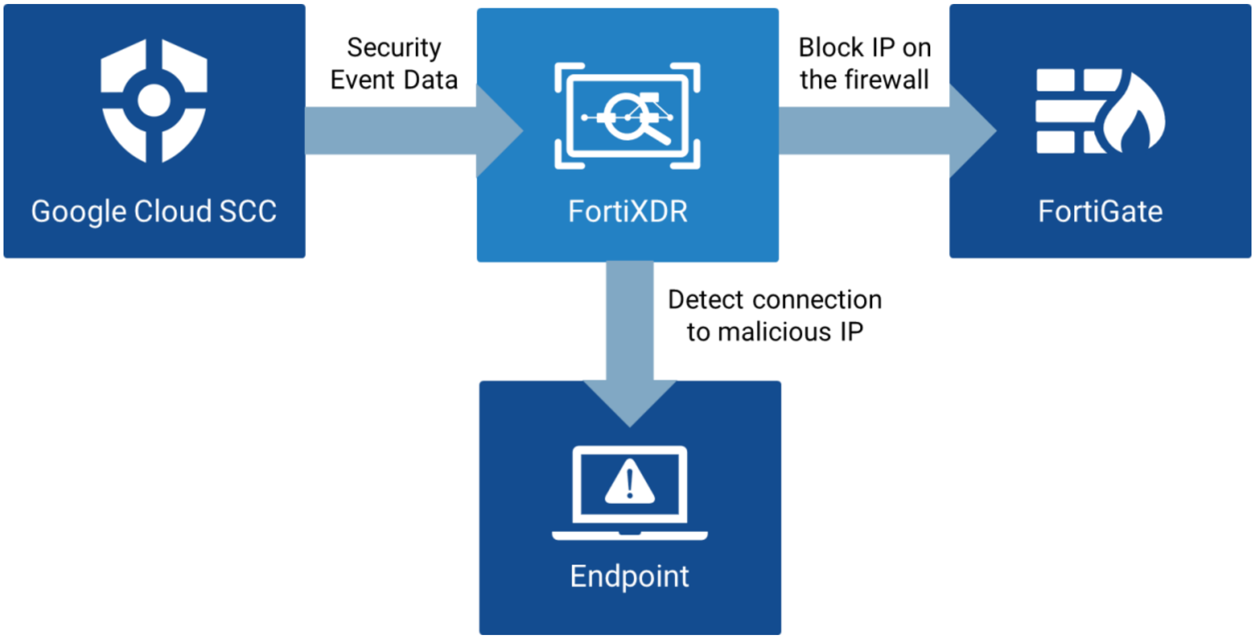
FortiXDR Partners With Google Cloud to Provide Security Benefits

FortiXDR integrates with several tools, including Fortinet Security Fabric, to correlate data to better detect and respond to attacks. As an example, by integrating with Google Cloud's SCC, FortiXDR can ingest critical data that is used to defend the enterprise.

SCC strengthens FortiXDR's ability to identify and respond to potential cyberthreats and shares valuable threat intelligence, including indicators of compromise (IOCs), affected devices, and file identifiers (hashes). FortiXDR analyzes Google Cloud SCC's vast pool of security event data to pinpoint potential attacks and conduct threat hunting to look for additional IOCs across the connected ecosystem.

Figure 4 illustrates the example Enterprise Strategy Group explored, in which a browser attempted to connect to a malicious IP address. FortiXDR automatically stopped this communication by adding a firewall rule to block the IP address. FortiXDR features a broader range of automated actions, which include removing suspicious files, isolating compromised devices, and running custom scripts for remediation.

Figure 4. FortiXDR Automatically Blocks Connections to a Malicious IP Address



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Through this partnership, FortiXDR provides strong endpoint protection without the added cost of additional data lakes and home-grown threat intelligence due to its multi-data-lake architecture that doesn't require replication.

Why This Matters

As attacks become more sophisticated and difficult to detect, many modern organizations are looking for ways to defend their endpoints without manual intervention. Extended detection and response (XDR) are among the top three strategies of organizations when asked how they plan to fortify their security operations.[7] Modern XDR platforms must collaborate well with third-party sources and correlate and act on data quickly, before a successful compromise can do heavy damage.

Fortinet's FortiXDR provides an integrated, evasion-resistant XDR solution built to protect an organization's endpoints from compromise and lateral movement. Using automated response capabilities, lightweight agents, support for legacy operating systems, and strong integration capabilities, FortiXDR on Google Cloud offers a single platform that protects endpoints, servers, and virtual machines (VMs), both on premises and in the cloud, from advanced threats.

Fortinet partners with Google Cloud to better find and detect malicious activity and stop it. Google Cloud SCC shares security event information with FortiXDR, which then works within the Fortinet Security Fabric to detect attacks and automate response. This integration reduces the mean time to detect and respond to potential attacks. It also helps security teams increase efficiency and effectiveness, even as the IT environment grows more complex.

Building its solutions in partnership with Google Cloud means that Fortinet can secure its customers' endpoints without the need for multiple or duplicate data lakes, reducing total cost of ownership while maintaining a high standard of security. Integration with Google Cloud provides another source of data that FortiXDR can use to quickly diagnose and stop attacks before they irreparably damage customer data, an organization's IT infrastructure, or its brand.

[7] Source: Enterprise Strategy Group Research Report, *2024 Technology Spending Intentions Survey*, February 2024.

Conclusion

Cybersecurity threats continue to increase in complexity and sophistication, forcing organizations to keep up. Enterprise Strategy Group research shows that 75% of surveyed organizations have experienced a ransomware attack, successful or unsuccessful, in the last 12 months.[8] Modern, hybrid IT environments feature a disparate mix of endpoints, servers, and virtual machines, both on premises and in the cloud. This constantly changing attack surface has contributed greatly to the increased difficulty running an effective security operations team.[9]

Organizations need a better way to scale with modern development cycles to address security issues and stay ahead of threats. Many are forced to use multiple tools, placing a heavy burden on endpoints while increasing the work security teams need to do to find and remediate threats. Due to this burden, 44% of surveyed organizations are looking to use XDR to consolidate their tools into one platform.[10] Fortinet is using the power of Google Cloud to provide this consolidation, while supporting legacy systems as well as modern infrastructure.

Google's cloud infrastructure stack builds security through progressive layers designed to deliver true defense in depth, which is how Google Cloud secures more than 3 billion users globally. Enterprise Strategy Group validated that Google Cloud aligns with the needs of security ISVs and helps them deliver better, more capable offerings—and deliver them faster. The software vendors we interviewed confirmed that Google Cloud's economies of scale, software-defined infrastructure, simplicity, shared responsibility, automation, and global reach help them accelerate time to market and optimize the delivery of new products, enhancements, and updates.

Enterprise Strategy Group validated that Google Cloud and Fortinet work together to deliver robust XDR capabilities by utilizing the Google Cloud SCC as a back-end threat intelligence platform. Fortinet customers can leverage the event data that comes from the Google Cloud SCC to help map out attacks from the point of origin to the cloud workload, from which it can automate a response to neutralize it.

Google Cloud offers broad and deep infrastructure and security support for security vendors that are developing solutions to secure their customers' applications across the globe. Fortinet leverages Google Cloud to bring massive scale to their solutions while providing broader visibility, faster analysis, and more effective response to their customers. If your organization needs to improve its ability to detect and respond to advanced threats while reducing complexity, Enterprise Strategy Group recommends you take a close look at Fortinet on the Google Marketplace.

[8] Source: Enterprise Strategy Group Research Report, *Ransomware Preparedness: Lighting the Way to Readiness and Mitigation*, December 2023.
[9] Source: Enterprise Strategy Group Research Report, *SOC Modernization and the Role of XDR*, October 2022.
[10] Ibid.

Information contained in this publication has been obtained by sources TechTarget considers to be reliable but is not warranted by TechTarget. This publication may contain opinions of TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com