GravityZone XDR

Extended Detection and Response

The frequency of cyberattacks, and the level of their sophistication, have increased exponentially. Entire businesses have been taken offline after simply clicking a URL in an email. Advanced persistent threats can go undetected for months while they siphon data from businesses, plant ransomware, and delete files from critical systems. Adding to the challenge, the emergence of work-from-home and hybrid working models have introduced new attack vectors that cyber criminals can exploit. While cyber-crime prevention technologies have improved, security experts recognize that 100% prevention is unattainable because attackers continue to evolve in their tactics, techniques and procedures. Given this reality, information is the best tool security teams have to reduce the time to detection and, ultimately, diminish the risk of damage and improve cyber resilience.

The need to collect and analyze disparate security information has led to the evolution from EDR (endpoint detection and response) to XDR (extended detection and response) technologies. XDR is designed to expand the capabilities of EDR by allowing for more data sources to be ingested, and providing a clearer picture of the steps in an attack and identifying more efficient ways to respond.

The increased, multi-vector complexity of cyber-attacks has led to the development of XDR technology. Effective XDR must have the following capabilities:

- Gather data from sources that can function as points of compromise in a cyber-attack.
- Have advanced machine learning and AI to parse through the data to reveal actionable information.
- Avoid alert fatigue by eliminating unnecessary noise from the attack investigation.
- Provide security teams with tools to take immediate action

How XDR Extends Detection and Response Beyond the Endpoint

GravityZone XDR combines Bitdefender's award-winning detection and prevention technologies with powerful sensors covering systems, productivity applications, cloud workloads, identity, and networks. With GravityZone XDR, security teams have expanded visibility into the entire lifecycle of an attack — from initial point of compromise, through lateral movement and more. GravityZone XDR provides detailed root cause analysis and extended visibility

At-a-Glance

GravityZone XDR analyzes and detects attacks across an organization's infrastructure and applications with more accurate detection and rapid response. Covering systems, productivity applications, cloud workloads, identities, and networks, GravityZone XDR helps security teams focus on the key areas being targeted by cybercriminals. Providing analytics and rich security context for correlation of disparate alerts, quick triage of incidents, and attack containment through automated and guided response. All without burdening the security teams with unnecessary alert fatigue — delivered from a single, intuitive management console.

Key Capabilities

- **Detect cyberattacks across systems, productivity applications, cloud workloads, identity, and networks**
- **Provides a root cause analysis for security teams to review**
- **Visualize the complete attack chain in an easy to digest format to identify weak points in the security chain**
- **Quickly take response actions** – delete malicious emails, isolate hosts, disable user accounts, and more
- **Thwart attacks before they happen with award-winning prevention capabilities**

"GravityZone XDR excels at connecting and correlating incidents over time throughout our entire operations and we experienced immediate value. The benefit of having a single-vendor solution with out-of-the-box detection capabilities for identifying and investigating known and unknown threats and providing our analysts with the knowledge of what and how an incident happened with the best ways to respond cannot be overstated."

Mahmood Haq, chief information security officer, MyVest

into threats that extend beyond the endpoint. With the capabilities found in GravityZone XDR, security teams have immediate access to correlated event sources, underlying data, and rich context so they can quickly identify the chain of actions associated with cyberattacks across their environment. GravityZone's advanced machine learning and AI provides security teams with visibility into behavioral patterns that allows for meaningful action. This technology reduces the risk of false positives and minimizes alert fatigue.

GravityZone XDR injests data from several different systems:

• On-premises and cloud endpoints and servers

• Microsoft Office 365™ productivity applications and email

• Cloud workloads such as Amazon Web Services®

• Microsoft® Active Directory® for identity managementNetworks
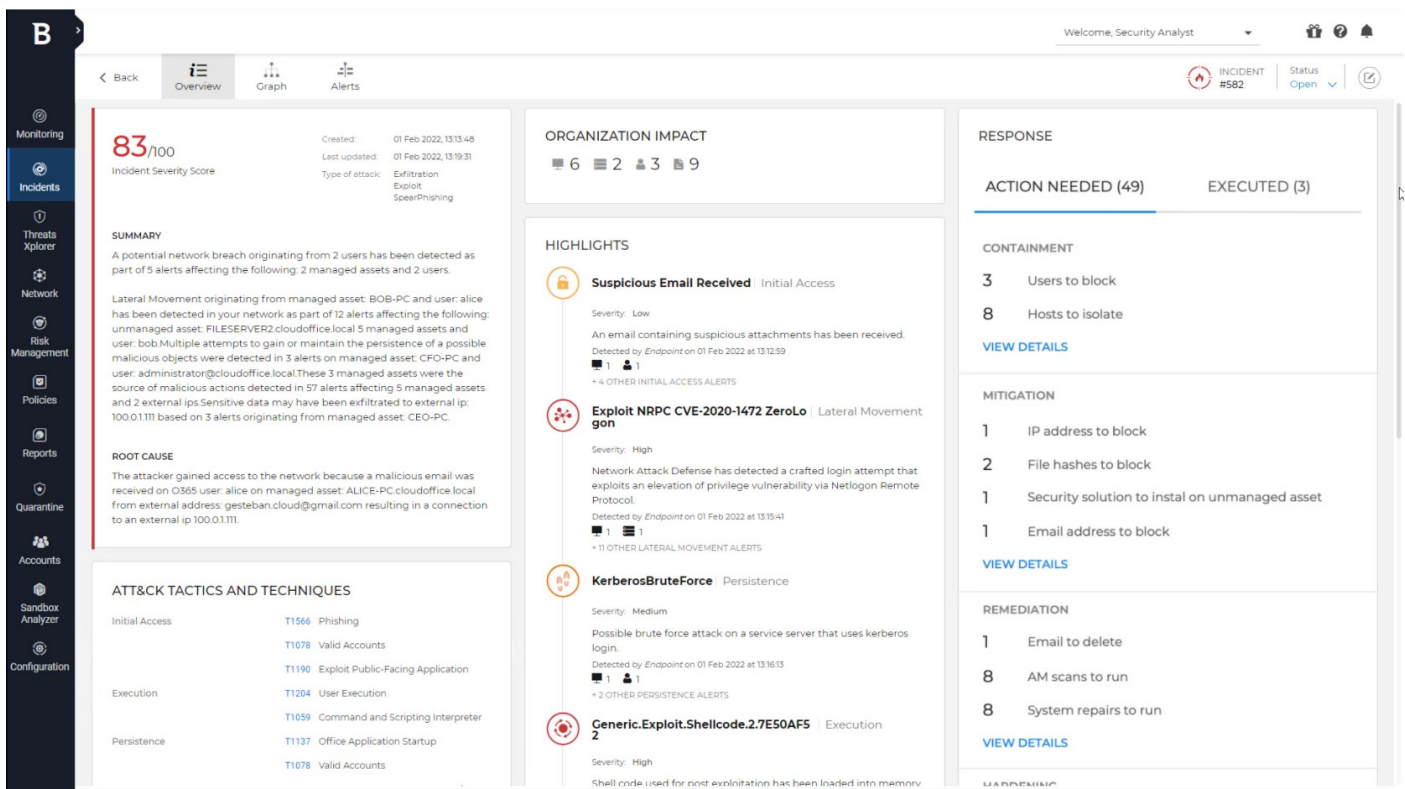All of the security tools covering these environments are manageable from the single, intuitive, GravityZone console.

Figure 1: GravityZone XDR provides security teams with detailed information on attacks. This enables rapid understanding of security incident and event details, potential organizational impact, likely root causes, and recommended actions.

How XDR Improves Detection and Response

GravityZone XDR leverages GravityZone Business Security Enterprise with one or more XDR sensors. GravityZone provides industry-leading cybersecurity technologies – endpoint protection, endpoint detection and response, user and endpoint risk analytics, network attack defense, web content filtering, tunable machine learning, sandbox analysis, flexible policy management, extensive reporting, and more —via a single, intuitive, cloud-based management console. With XDR sensors, Bitdefender extends its detection capabilities beyond the endpoint.

GravityZone XDR supports four additional types of sensors. These sensors ingest information from multiple sources and feeds it into an advanced machine learning engine. GravityZone XDR analyzes the machine-learning processed data and compiles a detailed timeline of the attack, which is presented in the Incident Advisor. With GravityZone EDR, security teams are already able to take response actions involving isolating a host, uploading files to the GravityZone sandbox for further analysis, terminating processes, and opening a remote shell on endpoints. GravityZone XDR expands those response actions with the inclusion of each of those sensors as described below.

Productivity Applications Sensor

The hijacking of Microsoft Office 365 accounts is considered one of the ultimate prizes for cyber-criminals. They often use phishing attacks to lure victims into exposing their valuable Office 365 credentials. Insight into such behavior is invaluable to security teams. GravityZone XDR detects attacks against or originating from Office 365 accounts and emails.

The Productivity Applications Sensor pinpoints particularities in Office 365 accounts that may be associated with cyber-criminal activity. The sensor detects the following actions:

• Disabling Office 365 anti-phishing protection.

• Questionable user creation behavior, such as a newly created user excluded from multi-factor authentication requirements.

• Uploading documents with suspicious macros to SharePoint and OneDrive.

• Uploading executable files to Office 365 accounts.

• Suspicious access requests, such as a user being given access to multiple files or directories on different SharePoint sites in a short period of time.

The sensor also detects anomalies in user behavior that deviate from a normal baseline. It can identify when a user had an unusual number of administrative activities or document manipulations in a given day, for example, when such actions stray from the user account's normal practices.

The detection of suspicious Office 365 behavior extends to email as well. The Productivity Applications Sensor identifies the following questionable activity inside Microsoft Exchange Online™:

• Exfiltration emails used to download files from a compromised user's account.

• Spearphishing emails — designed to deceive users into exposing their account credentials.

• Suspicious mailbox permission activity; for example, if a user received permission to access several different mailboxes in a short period of time.

• A user account deleting a large number of emails in a mailbox that the user does not own.

Along with identifying this suspicious behavior, GravityZone XDR helps security teams take actions to protect their businesses. With the Office 365 Sensor, security teams can delete emails across Office 365 organizations and suspend Office 365 accounts, all from the GravityZone dashboard.

Cloud Sensor

With the XDR Cloud Sensor, GravityZone XDR monitors activity that may indicate whether the security of cloud environments, such as Amazon Web Services® (AWS), has been compromised. The sensor monitors for multiple indicators of attack.

The Cloud Sensor recognizes anomalies by, first, establishing a baseline of normal behavior and then identifies when detected actifities deviate from the baseline. GravityZone detects when a user performs an action outside of the baseline, when a file with a suspicious extension has been uploaded and deviates from the baseline behavior, when a cloud function performs an action outside of the usual scope of activity, and other cloud-specific detections.

In addition, the Cloud Sensor identifies suspicious activity associated with many granular cloud service functions such as AWS Lambda®. The sensor detects when an attacker has executed a Lambda function that triggers a suspicious action. For example, it can distinguish when suspicious automatic code execution has been performed, such as using a Lambda function to create an access key to backdoor an AWS Identity and Access Management (IAM) user. As another example, when a Lambda function is used to update a security group to allow ingress on a port, GravityZone XDR will identify this as a maneuver that may allow an attacker to access the cloud instance.

The GravityZone XDR Cloud Sensor detects other suspicious behavior such as when an unfamiliar user or host removes the default encryption from an AWS Simple Cloud Storage (S3) bucket. By performing this action, the attacker exposes all encrypted objects (using server-side encryption) in that S3 bucket. XDR detects when an attacker disables or removes monitoring services such as stopping Amazon's logging service, CloudTrail, or deleting logs from the AWS monitoring service, CloudWatch. It also identifies when an attacker has performed reconnaissance events against an S3 bucket. GravityZone XDR can also reveal when a user has logged in from multiple regions simultaneously, a typical indicator of a compromised account.
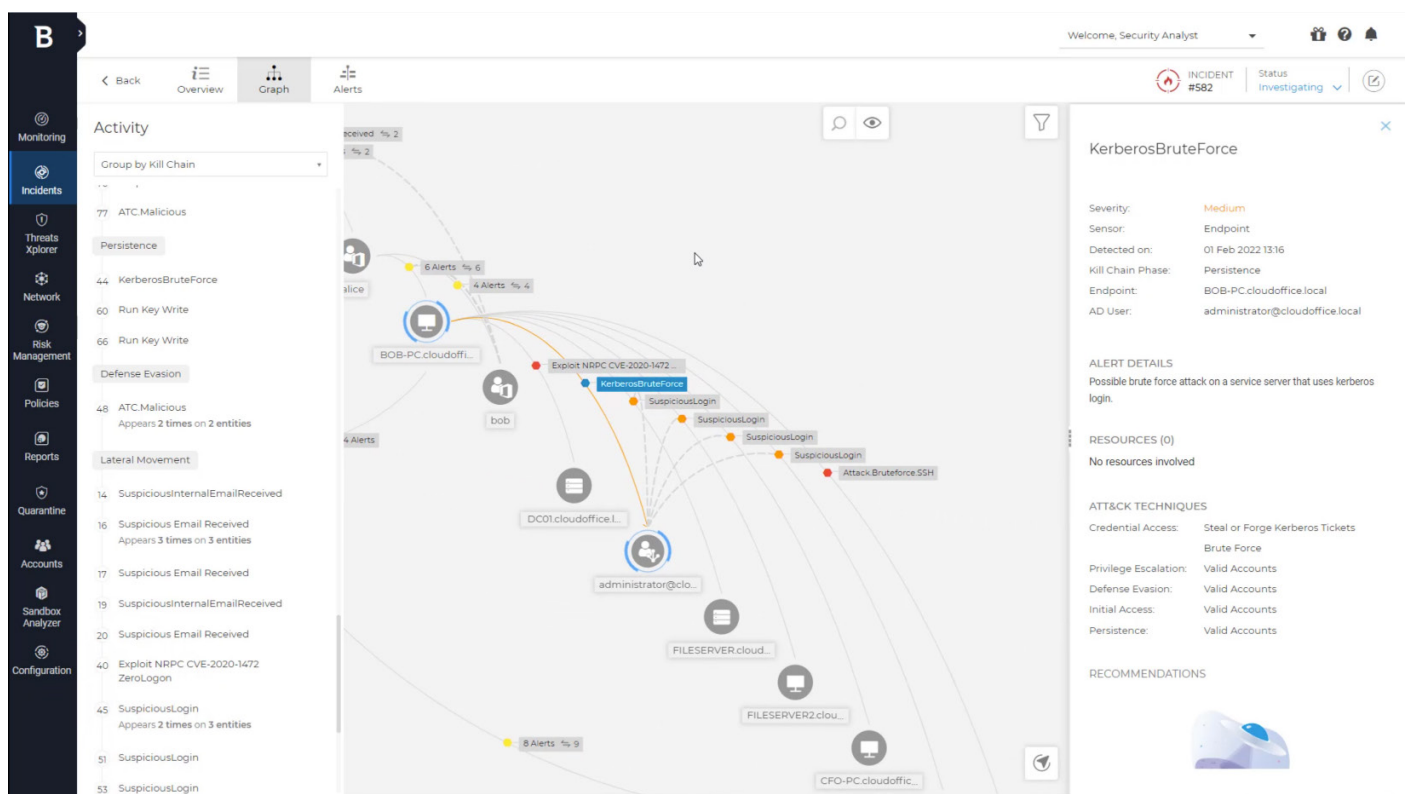

Figure 2: Security teams can review detailed information on every aspect of an attack in the Extended Incidents view. Our sensors monitor and correlate activity across various data sources to provide the details on each point of an attack in an easily understandable format. Activity can be sorted by time or kill-chain depending on how security teams prefer to analyze attacks.

Identity Sensor

The Identity Security is a critical component in enabling greater cyber resilience. Identifying suspicious authentication activity for applications, DevOps tools, databases, systems, cloud environments, and other critical resources helps prevent or mitigate the potential damage of a cyber-attack. Once the Identity Sensor is connected to Active Directory, it detects activity associated with

attacks that attempt to use compromised accounts, tokens, and objects. This includes not only end user accounts but system and API accounts.

The Identity Sensor detects attacks targeting the Kerberos network authentication protocol. Among the detections supported is the ability to detect when a Kerberos login is used to perform brute-force attacks against a system. During a brute-force attack, the malicious actor attempts to use rapidly generated passwords or encryption keys to gain system access. The sensor also detects additional Kerberos-related activities including use of stolen Kerberos tickets to move laterally across a network, requesting tickets with weak encryption—a common sign of malicious intent— and replay attacks. Replay attacks involve stealing packets from the network to forward them to a service or application.

The Identity Sensor also recognizes suspicious logins after a brute-force attack has been detected. The sensor identifies when an attacker registers a rogue Active Directory Domain Controller and uses it to inject malicious objects on other domain controllers within the same Active Directory infrastructure. It identifies when an attacker performs various activities on an Active Directory object and authenticates to remote systems using stolen credentials.

The powerful detection component of the GravityZone XDR Identity Sensor is complemented by capabilities that enable security teams to take meaningful action; for example, security teams can disable an Active Directory account or force a password reset directly from the GravityZone management console.

Network Sensor

The GravityZone XDR Network Sensor is a virtual appliance that monitors network traffic for signs of an attack. Malicous actors often attempt to expand their attack by moving across a company's network from one system to the next. The Network Sensor helps security teams identify when an attacker attempts to move laterally across their network. It can pinpoint when an attacker attempts to exfiltrate data to locations outside the organization. The XDR Network Sensor detects port scanning techniques and network-originated brute force attacks.

The GravityZone XDR Network Sensor combined with GravityZone Network Attack Defence – a core component of Bitdefender's endpoint protection— helps thwart network-based attacks while also providing valuable visibility to security teams to reduce cyber attack's impact and overall time-to-resolution.

World-Class Security Tools Paired with Security Expertise

GravityZone XDR provides businesses with a complete cybersecurity solution that combines award-winning prevention technology with sophisticated detection and response capabilities that provide meaningful information during and after a cyber attack. GravityZone XDR supports detection and response for systems, productivity applications, cloud workloads, identity, and networks, giving cybercriminals nowhere to hide. For businesses that would like to extend their teams with 24x7 security operations, Bitdefender offers Managed Detection and Response (MDR) services that leverage GravityZone XDR. Our MDR staff are highly experienced, certified professionals with over 100 years of combined cybersecurity expertise across commercial enterprises and government intelligence services. With MDR, you get the best combination of security capabilities and expertise to provide the best protection against today's multi-vector cyber threats.
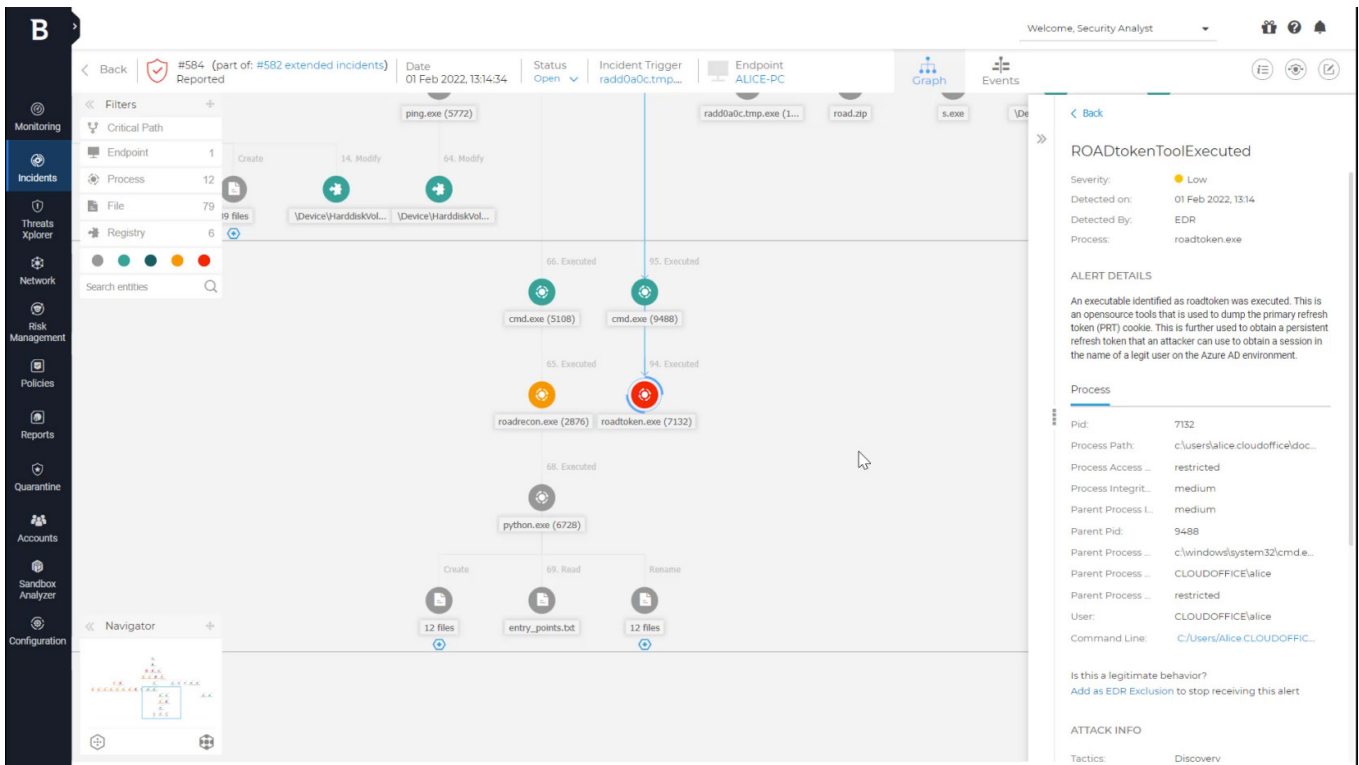
Figure 3: GravityZone XDR provides detailed attack visualizations to help security teams review the critical path of each and every attack. They can review a comprehensive analysis of every individual file involved in an attack and take response actions such as blacklisting a file, uploading it to the GravityZone sandbox for further analysis, isolating the host, and more.

Bitdefender
BUILT FOR RESILIENCE

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, business, and government environments, Bitdefender is one of the industry's most trusted experts for eliminating threats, protecting privacy and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers over 400 new threats each minute and validates around 40 billion daily threat queries. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence, and its technology is licensed by more than 150 of the world's most recognized technology brands. Launched in 2001, Bitdefender has customers in 170+ countries with offices around the world.

For more information, visit https://www.bitdefender.com.

3945 Freedom Circle

Ste 500, Santa Clara

California, 95054, USA