VMware Contexa™—the Threat Intelligence Cloud

VMware Contexa—
A full-fidelity threat intelligence cloud that sees what others don't and stops what others can't.

See More. Stop More.

With Contexa, VMware reframes traditional security analytics as enriched threat intelligence at global scale. Contexa processes data to produce threat intelligence based on the inner workings of applications and networks. VMware Security leverages the context, this distributed threat intelligence rooted in full-fidelity data, to apply policy at distributed control points, improving lateral security and stopping attacks.

Enterprises of all sizes rely on VMware Security and Contexa to protect users, endpoints, networks, and workloads. Each day, protected organizations benefit from the billions of security events and network flows that Contexa processes.

Contexa sees more and stops more.

The Challenge

The gap between adversaries and defenders has never been larger. The space is increasing faster and faster. This gap has been caused by two trends, and it has outpaced traditional boundary controls and outstripped all human capacities. Technical architectures have transformed, and user behaviors have changed. The shape and scale of the attack surface have shifted dramatically.

First, information technology has become so dynamic as to become incomprehensible at human speed. In the past, managed users on managed devices connected to three-tier applications that were separated from the Internet by a clearly defined DMZ and well-defined boundaries: Is anyone still enjoying such simplicity? The days of static server workloads with fixed addresses in one location are gone. Heavyweight network VPNs are literally antiques—standardized in the mid 90s with widespread adoption in the early 2000s. Since then, the attack surface has exploded in every dimension: users, endpoints, networks, and workloads. Bumps in the wire cannot meet the need anymore.

Second, today, adversaries are funded by nation states—if they are not nation-state actors, then they are using tools and techniques developed within nation-state labs. These well-tooled adversaries are motivated by commercial gain or politics. The black hat "as-a-service" era has arrived: with very little effort, criminals and cyberterrorists can order up a ransomware campaign against a target. We are defending businesses

vmware®

and assets, and it is an unfair match-up without a new set of tools and a new approach. Practitioners feel understaffed and outgunned. But this situation is not merely a training or hiring issue. We cannot hope to train and hire our way through this challenge.

And still: we are charged with providing conditional access by user and device to micro-segmented networks and the workloads and workspaces they connect. We must manage access to workloads and manage risk, detecting indicators of compromise and responding based on the perceived threat. And that is not enough: we must operate security controls in automated and orchestrated environments that span traditional boundaries of control.

Every Packet. Every Process.

We cannot play peek-a-boo with threats. We cannot simply bolt on appliances in a few places within the fraction of infrastructure that we happen to control. The solution we require is complete visibility and automated responses, not mere inspection at a few points between network switches, not just some data, and not only during transit. The scale of such an approach outstrips human capacities. We need data analytics to inform automated analysis and to triage detected threats, and to support investigation of potential incidents.

We need all the data. To operate so pervasively, we need to automate the collection of full-fidelity telemetry on each endpoint and within each workload. We need to inspect and control the network data, including east-west communication, even that communication between services running within a single physical server. We must then automate the analysis and investigations—with an aperture into every packet and every process. Human intelligence must be applied exactly when and where it is needed. There simply is not a way for human security engineers to manually monitor threats to our systems and applications anymore. The deeper the visibility we have and the more observability that software exposes, the greater the need for automation grows.

To close the gap between adversaries and defenders, while simultaneously making services more available, we must reduce the risk that results from such access. We must ensure that workers and developers can work efficiently and that systems can deliver services effectively. So, we must blend automated signal collection and analysis with human intelligence. Only then can we effectively scale cloud-native operations, accelerate the enterprise cloud transformation, and empower the hybrid workforce in a manner that manages risk and protects information and infrastructure. We need to collect data, analyze data from many sources, and then distribute that resulting context, the threat intelligence, to control points. The resulting analysis, the threat intelligence, must be quick to access and easy to use. Such intelligence must be actionable and drive confident decisions where automation cannot complete the job alone. This is Contexa, the VMware Threat Intelligence Cloud.

Contexa Produces Threat Intelligence

Contexa is rooted in virtualization—of compute and networks—and the technologies that support such virtualization. Contexa contributes to improving security on networks and on endpoints, within workloads and within modern applications built on containers. Contexa leverages full-fidelity data, applies analytics in-context, and then VMware Security enforces automated action at control points. VMware Contexa establishes intelligence by taking in information from a variety of systems and sources and building a shareable context. Such intelligence can expose threat actors moving within new distributed attacks chains and be used to halt them. Contexa receives data from and shares analysis with other systems. This enables security analysts and security engineers to make intelligent decisions—delegating some of those decisions to machines.

Living Off the Land

Attackers have responded to traditional controls built for the 2000s. Attackers must now forage to move from system to system across networks. We have employed effective countermeasures, such as micro segmentation, creating ultra fine-grained controls that can be automated. We have, to a significant degree, limited movement. VMware Security then advanced network security by adding advanced IDS/IPS, network sandboxing, and Network Traffic Analysis (NTA) directly into the virtualization layer with NSX. VMware Security further improved security for endpoints and workloads with Carbon Black, which provides intelligent solutions for protection, detection, response, and identifying risk.

VMware Security secures users where they work and secures the systems used to deploy and run workloads. VMware has extended security controls to containers and cloud-native networks by adding advanced protections within containers, runtimes, and the VMware service mesh. Protective measures can be applied before an application is deployed. East-west traffic between every single process can be inspected, analyzed, and controlled. Advanced security controls and inserting protection everywhere that virtualization happens makes it increasingly difficult for attackers to move and compromise systems, starving them. The automated collection and analysis of endpoint, network, and threat data powers a fast and graduated response to threats.

These workloads and containers run business-critical modern applications that are necessarily exposed to the Internet and require a careful approach to security. VMware's software-based, elastic advanced load balancer and web application firewall make it significantly easier to protect these web apps. Modern defenses are already built in. Such elements are the distributed control points powered by Contexa. The control points, in concert with the service mesh, derive consistent visibility and detection capabilities and ensure the legitimacy of each and every API call between applications. This threat intelligence extends from endpoints to workloads to modern applications and across different multi-cloud environments.

What's After Micro-segmentation and Advanced Threat Protection?

As protections cut off illegitimate channels, attackers are forced to hide within application traffic or hijack legitimate channels. Contexa enables analytics to assess the risk of such traffic and then share that assessment with security analysts or other systems. For example, watchlist hits, events and alerts can be shared in near-real time within external systems, enabling automated workflows without having to perform one-off API calls. With Contexa, security context can be delivered to third-party solutions and to data lakes reliably and at global scale. That shared context arrives ready for consumption, rooted in high-quality data and delivered from the threat-intelligence cloud.

Such intrinsic security, based on complete endpoint and network data, contrasts with approaches that sample data and filter metrics. Such incomplete approaches often focus on physical infrastructure and neglect virtualization. Still others add network traffic analysis, but only at specific points of ingress or egress, relying on expensive taps and low-quality flow metrics. Incomplete approaches are blind to the network or work within closed systems, degrading network analytics and making information sharing, whether for evidence preservation or improved analytics, impossible. Poor network data or incomplete endpoint telemetry and black-box threat intelligence each leave attackers a place to hide.

Discovers Threats and Executes a Graduated Response

The fusion of high-fidelity signals from a variety of sources enables human eyes to focus on the right alerts and effectively halt threats and protect resources with a graduated response and without trading off business agility. Contexa discovers

vulnerabilities, detects threats, and quashes lateral movement, but it cannot do so alone. Contexa works with distributed control points within user endpoints, virtual machines, containers, and runtimes. Contexa also works with virtualized networks and the container service mesh. Contexa processes inputs from a wide range of sources. These inputs are processed by machine intelligence and the analysis is supervised by human analysts within the VMware Threat Analysis Unit. The Threat Analysis Unit researches and analyzes the evolving tactics, techniques, and procedures of threat actors.

Employing deep understanding of these tactics and leveraging real-time analytics in combination with machine learning, the Threat Analysis Unit prevents and detects attacks. This combination of machine automation and human intelligence enables Contexa to support security that increases operational confidence and enables further security automation, while leaving the system open for customization and enabling information sharing with other systems or business processes. Contexa delivers high confidence detections. This precise fusion of world-class threat research together with powerful artificial intelligence stops more attacks in less time.

Delivers Threat Intelligence from the Cloud, for Every Cloud

The combination of machine learning that acts on full-fidelity data from a variety of sources with reasoned application of human intelligence drives unique insights within the VMware Threat Intelligence Cloud. The result is Contexa threat intelligence. Contexa encapsulates the complexity of such analytics. The cloud collects data from a variety of sources that can be extended. By understanding applications and networks from within and by delivering intelligence and control to each application environment, Contexa enables you to close the adversarial gap and realize a scalable zero-trust architecture, simply and securely managing any app on devices anywhere.

You can start benefiting from Contexa by adopting VMware security in a variety of areas within your cloud. Contexa can meet you where you are and extend your security capabilities today:

- If you are securing multi-cloud workloads, you can easily extend powerful built-in protection for vSphere and VMware Cloud to public cloud deployments to increase visibility and control, prioritize and reduce vulnerabilities and misconfigurations, and deliver context-rich security insights for cloud teams.
- If you are focused on securing modern applications, Contexa can shift security left with security posture management and compliance monitoring for Kubernetes. You can simplify “encrypt-everything” architectures and deliver API security while benefiting from cloud workload protection that can run in your private cloud or within Amazon Web Services.
- If you are charged with securing a hybrid workforce and providing users the freedom to choose the right device for their job, you can securely deliver and manage applications on devices anywhere, transforming your security with intelligent endpoint protection.

As an enterprise expands with VMware Security, Contexa gets smarter. Contexa works with the tools that employees want and protects the endpoints and workloads that they require to get work done. Whether your security team is globally distributed or an army of one, Contexa sees what others can’t. All protected organizations benefit from the billions of security events and network flows Contexa sees daily.

The company that pioneered modern virtualization, now protects VMs like no other—and provides innovative protection for modern applications.

VMware Contexa: See More. Stop More.