Managed Detection and Response

Threat detection is a top priority for everyone.

The state of cybersecurity technology and the vernacular we associate with it seems to be constantly changing. The scope of services an MSSP once offered has had to evolve to meet the continuous shift of tactics used by cyber criminals. What was once "Managed Security" has now become so much more in order to make a positive impact inside an organization's security operations. The industry has moved away from simply identifying vulnerabilities and reacting to attacks.

While the need for advanced solutions grows, the unique challenges facing the cybersecurity industry persist. Security teams across the board, regardless of size or maturity level, face similar struggles when it comes to protecting their organizations from outside threats. Volta solves these challenges for security teams by providing a fully flexible MDR solution to defend data, detect threats, and respond to incidents.

KEY CHALLENGES

+ The sheer amount of attacks to defend against.

+ A wide spread of disparate products to tackle specific vector vulnerabilities.

+ The appropriate amount of expert staff to battle the bad guys.

ONE UNIFIED SERVICE TO: **REDUCE RISK** | **RESPOND TO THREATS** | **STOP ATTACKS**

Volta's Dual MDR Model

We have redefined our approach to MDR in order to meet our clients' needs with a key efficiency; flexibility of deployment. We know that not every organization has the same toolbox, budget, and maturity level. That's why we provide a dual model approach to MDR. We can bring our own tools to the table in a turnkey solution, or you can bring your own.

VOLTA SECURITY STACK

Take advantage of a turnkey approach to detecting and responding to threats, powered by Volta's platform of best-in-breed security assets. We integrate network visibility, endpoint detection and response, deception technology and analysis into a full cloud offering. If you're just starting the journey towards more advanced defense tactics, the Volta Platform provides a seamless transition into enterprise-grade technology. We partner with industry leaders to cover every threat surface in order to bring a world-class security tool kit to your infrastructure.

BYOT (BRING YOUR OWN TECHNOLOGY)

Volta's BYOT approach covers organizations who have already made substantial investments in a variety of security products and platforms. We find it limiting to solely offer a closed box solution which doesn't allow our clients to utilize the tools they've implemented. It undercuts the significant strides they've already taken. Our open MDR model works with the products and infrastructure already in play within your security program. Volta's expert analysts pull your current security products into our platform and commence preventing, hunting, detecting and responding to threats 24x7x365.

KEY CAPABILITIES OF VOLTA MDR MODELS	STACK	BYOT
24x7 Threat Detection and Response	✓	✓
Integrated tech stack w/ Endpoint, Intrusion Detection, Behavioral Monitoring	✓	
A unified security operations platform	✓	
Conduct network map + vulnerability assessment scans	✓	
Thorough analysis of network traffic and metadata	✓	✓
Access to technologies included in the platform	✓	
Intelligence-based Threat Detection	✓	✓
Team of seasoned "experts" available via phone, email, text	✓	✓
Built natively in the cloud for the cloud/Fully hosted and managed by Volta	✓	
Assistance in compliance preparation	✓	✓
Optional Deception Technology available	✓	
Optional Vulnerability Assessment Scans on customer defined cadence	✓	✓
Unify visibility across your network, endpoints, applications and the cloud		✓
Maximize ROI on existing security investments		✓
Natively monitors: + AWS and Microsoft Azure public clouds + Windows and Linux endpoints in the cloud and on prem + Virtual on-premises IT on VMware / Hyper-V + Physical IT infrastructure in your data center + Other on-premises facilities (offices, retail stores, etc.) + Cloud applications like Office 365 and G-Suite		✓
Install time typically 24 hours		✓
Create Incident Response Plan or update IRP currently in place		✓

What sets us apart?

SKILLS TRANSFER

We are more than capable of being your entire security team, but we also encourage knowledge transfer between our experts and your technical staff. We want to inspire our clients to strengthen their defenses with the most formidable infrastructure plans available. That process starts with sharing knowledge from the decades of combined experience among our team.

CUSTOMIZED ALERTS

Anyone can install a security stack in their environment and receive the same canned report with hundreds of false positives or thresholds that don't matter to their business. Having a security provider do an automated dump and then email it to you doesn't improve the situation in the slightest. At Volta, we customize and tune alerting through human review and consultation with our customers. We help you distill down the alerts into what really impacts your business, and we respond to those incidents with human intelligence.

FLEXIBLE DEPLOYMENT

Our flexible deployment model sets us apart from other cyber security firms in the region. Clients value this process because it allows them to choose the best option for their unique needs. From known malware, to new and advanced threats, Volta is ready to protect your organization by preventing, detecting, investigating and acting against threats all year around, 24 hours a day, 7 days a week.