STARLINK

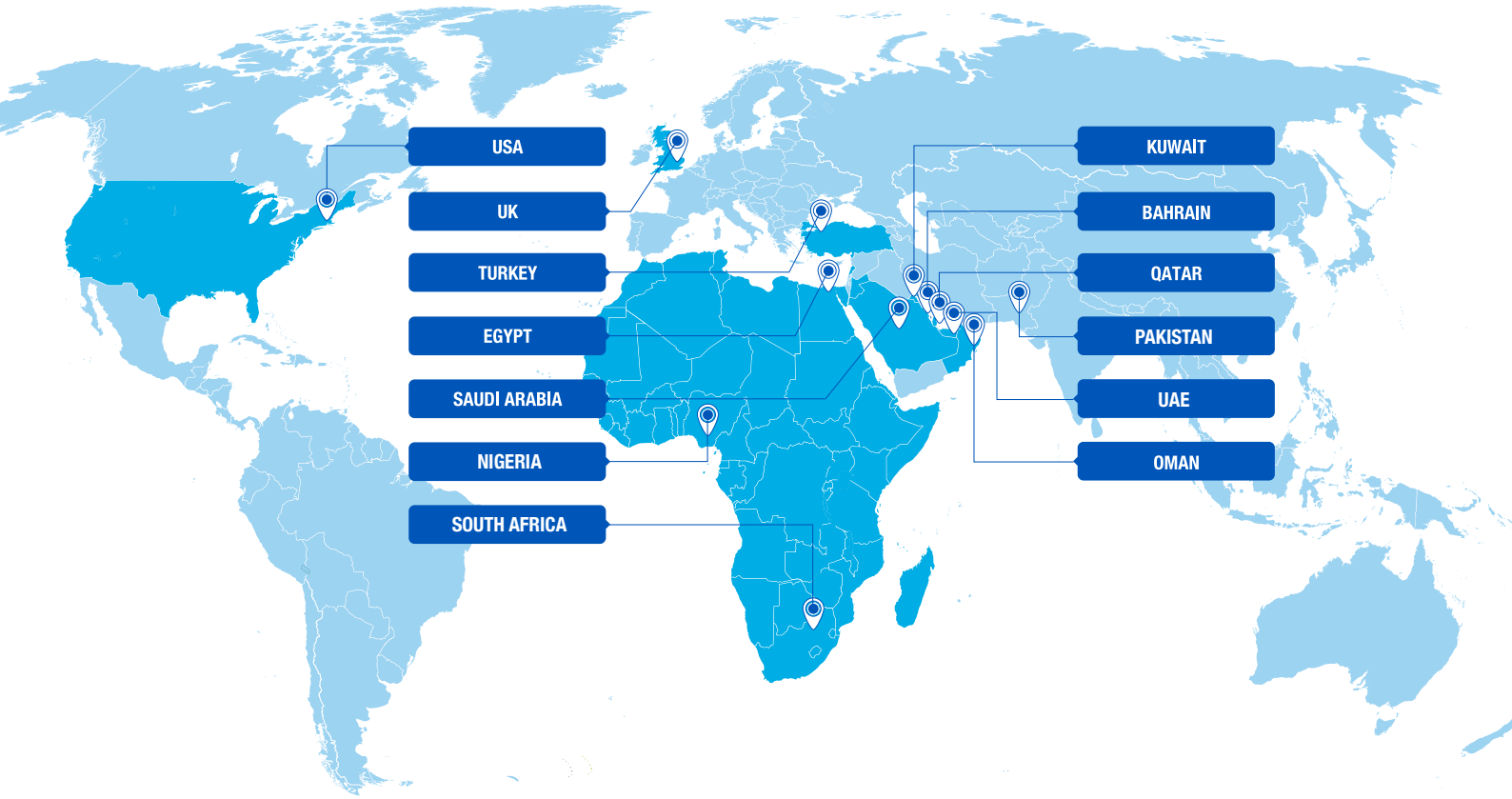
TRUSTED SECURITY ADVISOR

TRUE VALUE-ADDED IT DISTRIBUTOR

ACCELERATE

AT THE SPEED OF STARLINK

About Us



Who We Are

StarLink is acclaimed as the largest and fastest growing "True" Value-Added IT Security Distributor across the Middle East, Turkey and Africa regions with on-the-ground presence in 11 countries.

With its innovative Security Framework and Vertical Security Trend Matrix StarLink is also recognized as a "Trusted Security Advisor" to over 1000 enterprise and government customers that use one or more of StarLink's best-of-breed and market-leading technologies, sold through our Channel network of over 250 Partners.

The StarLink Solutions Lifecycle helps Channel Partners differentiate offerings, and assists customers to identify key risks and define priorities for addressing IT Security gaps relating to compliance and next-generation threat protection.

Overview

StarLink Vertical Security Trend Matrix

In recent years we have seen many changes in IT security. In an attempt to keep up with new and increasing threats to enterprise and government entities, traditional approaches to IT Security have limited impact. Organizations are dedicating more resources to IT Security and risk but attacks and vulnerabilities are increasing in frequency and sophistication.

The StarLink Vertical Security Trend Matrix provides Security leaders in the key verticals of Government, Telco, Oil & Gas and Banking, insight into how the latest IT Security trends cater to their respective industries, in order to address today's compliance and next-generation threat protection requirements.

The top 5 IT Security trends are namely, Behavioral Analytics, Internet of Things, Cloud, Mobile and Incident Response.

Overview

StarLink Security Framework

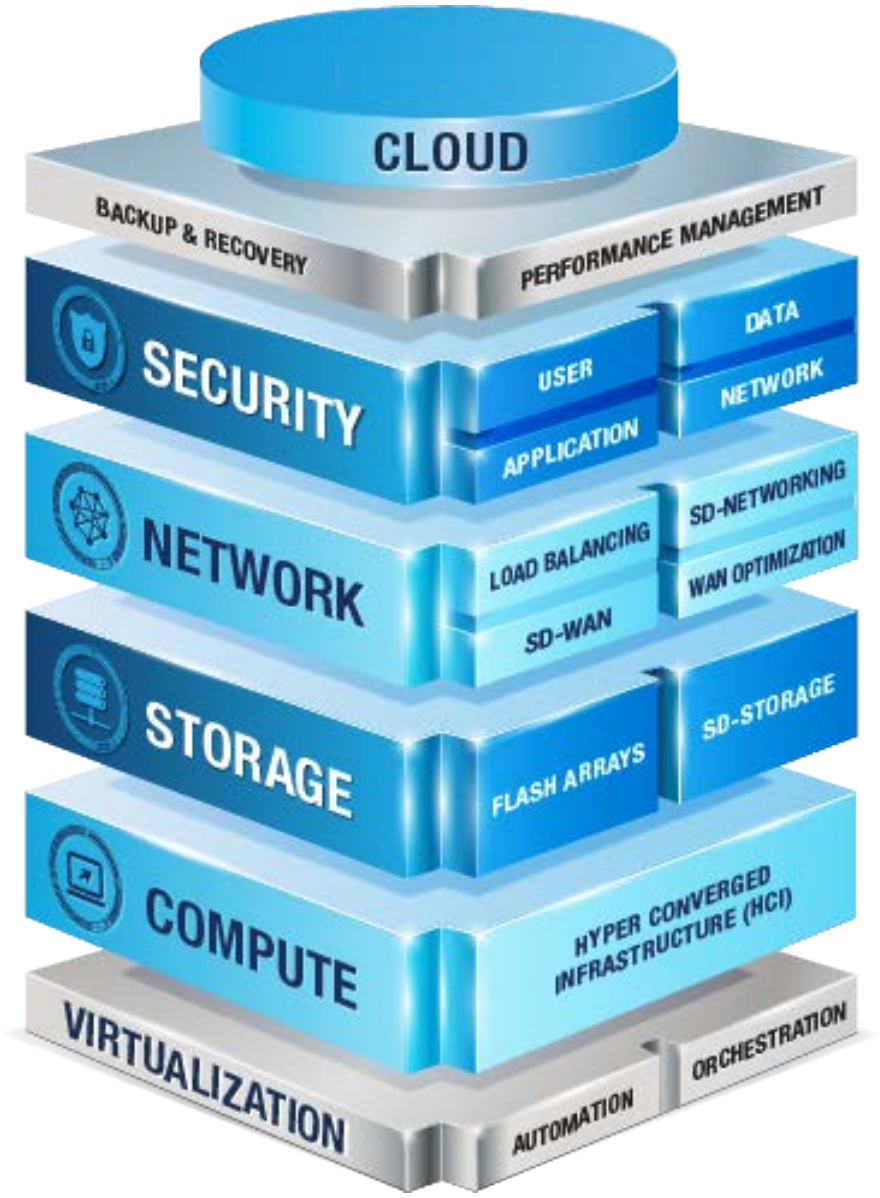
IT Security is a fragmented market, proliferated with many point products that are designed to address specific risks, and which may meet targeted compliance goals, but these solutions typically fail to provide a comprehensive, integrated picture of the threat landscape.

Instead of organizations becoming more relevant and agile in their response to security challenges, increased complexity is created that can overwhelm IT Security teams. The challenge is compounded by patient attackers, sophisticated advanced threats, and the increasing use of cloud and mobile technologies, which expand the potential attack surface.

To successfully deliver security capable of addressing today's risks, organizations need to take a holistic approach to IT Security. The StarLink Security Framework provides a strategic approach that cuts through the clutter and is designed to simplify risk management and ensure that all critical controls for effective enterprise IT Security are in place.

StarLink delivers real value to customers and partners with its vendor-agnostic and technology-centric Security Framework. Decision-makers can quickly and easily visualize multiple security domains to help understand, prioritize and mitigate risk. The innovative defense-in-depth Security Framework helps customers define their strategic objectives, top-down. Customers are able to comprehensively achieve their IT security vision, from the User to the Network to the Application and finally to the Data.

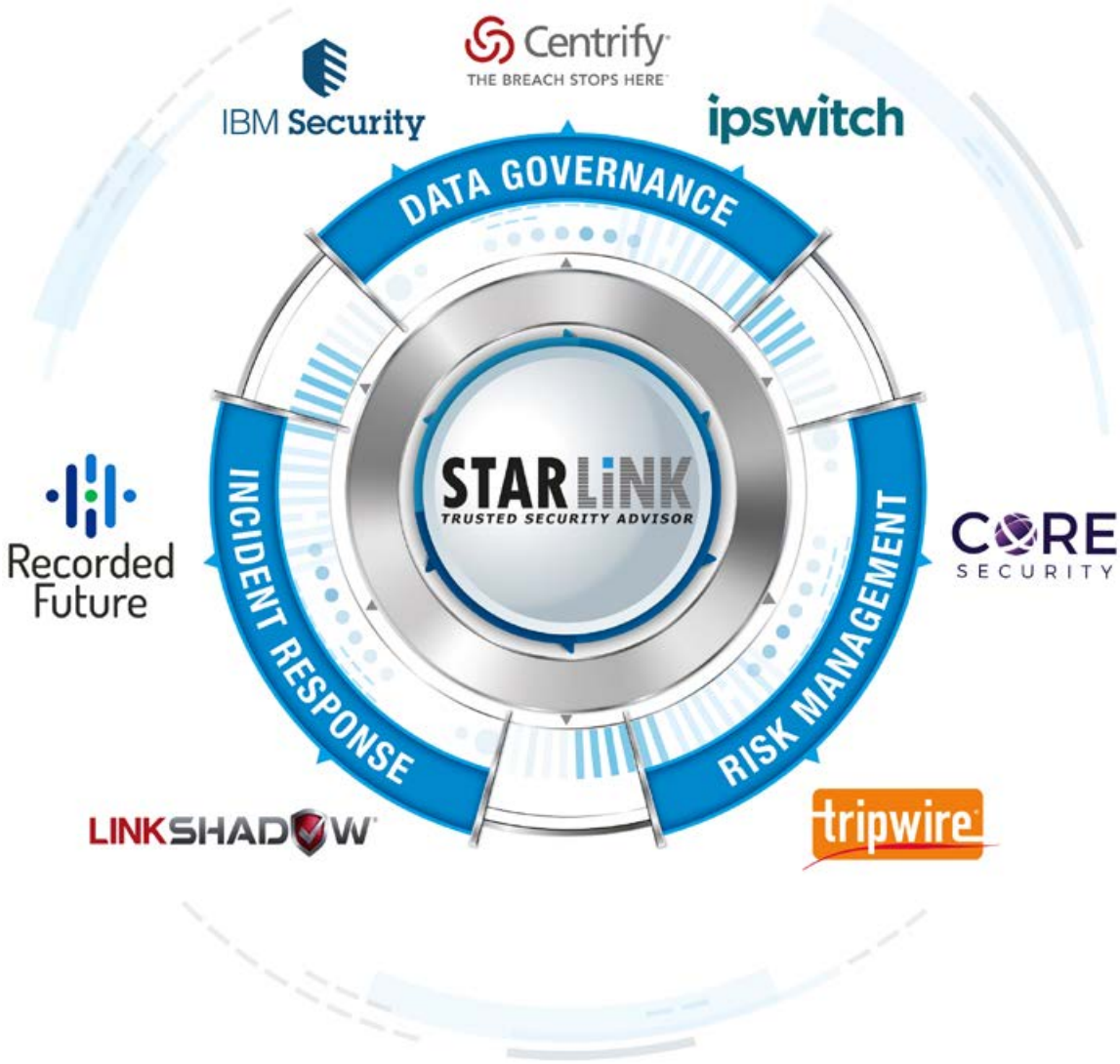
Overview



SDDC Technology Architecture

The software-defined data center (SDDC) is now a key focus area for most organizations. The shift in the datacenter paradigm is about reducing costs and providing service agility. To maximize data center ROI, key Security factors needs to be fundamentally considered including lateral movement of malware, network security virtualization, orchestration, people and process.

Simultaneously, with the surge in cyber threats including DDoS, against the cloud and IoT, as well as, ransomware leading to disruptions in IT and OT networks, plus mobile attacks and vulnerabilities on the rise, customers will be increasingly looking at automation and machine learning.



StarLink Solutions Lifecycle

IT security challenges can no longer be addressed by point products. Such products typically fail to provide a comprehensive, integrated picture of the threat landscape, each returning its own results but missing the opportunity to put results into context, falling short of enterprise-wide insights, and increasing the complexity of managing the IT security platform. At the root of the problem is the fact that most point solutions operate in silos; they typically do not integrate with other products in the security infrastructure. It becomes difficult for the security team to see through the noise and understand where real threats and real vulnerabilities are hidden.

An integrated approach requires capabilities to achieve compliance, as well as, to monitor for and prevent attacks on the network, on the endpoint and across other IT assets. Detected security concerns must be investigated quickly with tools that can integrate context from across the environment with the passing of security information, alerts and policies between security domains. Once this analysis is complete, security gaps can be bridged, and ongoing protection can be implemented. This methodology allows for faster, more effective identification and mitigation of potential security threats, as well as, helps in identification of behavior anomalies, risk prioritization, and increased visibility and control.

StarLink's portfolio has evolved into a uniquely integrated Solutions Lifecycle consisting of Data Governance, Risk Management, and Incident Response. Each of these solutions comprise of vendors' core competencies, and feed into each other giving customers the ability to quickly understand their IT Security gaps, and set priorities accordingly, starting from achieving effective application performance and traffic visibility, to implementing critical controls, to verification of those controls, to zero-day malware protection, to sensitive data consumption, to remediation of next-generation threats, and then back around again, while centrally consolidating visibility of all machine data to generate valuable insights.

Solution

Data Governance

Where is my Sensitive Data?

Data Governance enables the organization to control access to sensitive data by understanding user privileges, securing privileged access and monitoring changes to directories, files, data repositories and databases, as well as, user activity. This in turn leads to alerts ensuring that sensitive data is only accessed by authorized users by providing comprehensive real-time visibility into all activities. Furthermore, classification mechanisms are put in place to guarantee that sensitive data cannot be leaked to unauthorized users. Finally the required processes and procedures to achieve continuous compliance are automated so that human error or risk of insider threats are minimized.

Integrated Security Solution

IBM Security

ibm.com/security

IBM integrated security intelligence protects businesses around the world.

IBM offers a deep enterprise security portfolio customized to your company's needs. Unmatched in ability to help you disrupt new threats, deploy security innovations and reduce the cost and complexity of IT security, IBM can safeguard your most critical data from compromise.

From infrastructure, data and application protection to cloud and managed security services, IBM has the expertise to help safeguard your company's critical assets. We protect some of the most sophisticated networks in the world, and employ some of the best minds in the business.

Identify - Build a secure enterprise with increased visibility

Risk Management and Compliance Services help you evaluate your existing security practices—including payment card industry (PCI) security, identity and IT regulatory compliance needs and gaps—against your business requirements and objectives. Our skilled security specialists provide recommendations to help you make more informed decisions about allocating your resources to better manage security risks and compliance. We can deliver a wide range of capabilities—from security program development, to regulatory and standards compliance, to security education and training.

Protect - Arm yourself to prevent attacks before they start

IBM identity and access management services target virtually every aspect of identity and access management across your enterprise, including user provisioning, web access management, enterprise single sign-on, multi-factor authentication, and user activity compliance. We offer a range of service options — from migration to consulting to fully managed services — that leverage IBM's leading security tools, technologies, and expertise. Our security specialists work with you to address your individual needs and provide the solutions that best match your business and security objectives.

Respond - Stop attacks in their tracks and mitigate exposure

IBM's Cybersecurity Assessment and Response services are designed to help you prepare for and more rapidly respond to an ever-growing variety of security threats. Our seasoned consultants deliver cybersecurity assessments, planning and response services, with proven expertise from mainframe to mobile.

Identity and Acccess Management

Centrify

THE BREACH STOPS HERE

centrify.com

Centrify is the leader in securing enterprise identities against cyberthreats that target today's hybrid IT environment of cloud, mobile and on-premises. The Centrify Identity Platform protects against the leading point of attack used in data breaches — compromised credentials — by securing an enterprise's internal and external users as well as its privileged accounts. Centrify delivers stronger security, continuous compliance and enhanced user productivity through single sign-on, multi-factor authentication, mobile and Mac management, privileged access security and session monitoring. Centrify is trusted by over 5000 customers, including more than half of the Fortune 50.

WHAT WE DELIVER

Stronger Security + Continuous Compliance + Enhanced User Productivity

- Single sign-on
- Active directory bridging
- Privileged access security
- Multi-factor authentication
- Mac management
- Session monitoring
- Provisioning
- Enterprise mobility management
- Shared password management

Secure Managed File Transfer & Large-File Email Bypass

ipswitch

ipswitch.com

MOVEit Managed File Transfer: Today's businesses share more information electronically than ever before between their business partners, customers, and employees. Ipswitch's MOVEit Managed File Transfer (MFT) System is the best way to reliably move that information in a timely, controlled, and secure manner to improve business productivity, meet SLAs and compliance requirements, and gain visibility and control of file movement.

MOVEit File Transfer: MOVEit File Transfer server is the reliable and secure hub that IT needs to transfer the organization's business files. With its broad protocol support, MOVEit File Transfer server connects with any system, server or client. Using the latest security technologies, it protects files both in transit and at rest. And as part of the MOVEit Managed File Transfer System, MOVEit File Transfer gives IT the visibility and control they need to confidently meet SLAs and compliance requirements.

MOVEit Central: MOVEit Central enables you to easily automate your file-based workflows. MOVEit Central provides a simple but powerful user interface for defining business workflows that's easy enough for anyone on your IT team to use because no scripting is required. The heart of MOVEit Central is a reliable workflow engine that ensures the predictable, secure delivery of your business files. Plus, a powerful centralized console ensures you'll have visibility and control over all file movements. That is why hundreds of companies, including many in healthcare and finance have turned to MOVEit Central to automate their file-based workflows and confidently meet their SLAs and compliance requirements.

MOVEit Mobile: IT departments want to give users the ability to transfer work files using their mobile devices while keeping the enterprise security they rely on with MOVEit. They want to allow users to upload and download files from either iOS or Android phones and tablets. Most importantly, they want to extend the secure, compliant, file-based processes to people when they are mobile. MOVEit Mobile enables mobile workers to reliably and productively participate in file-based business process workflows, while providing IT the security, visibility and control required to confidently run their business and meet compliance requirements.

MOVEit Ad Hoc: To get their work done employees are circumventing IT by turning to new, web-based consumer services to send and receive files, creating control, visibility, and security challenges for the business. MOVEit Ad Hoc Transfer offers employees and businesses a better alternative.

For employees, MOVEit Ad Hoc Transfer enables easy transfer of files of any size using a familiar interface: either Microsoft Outlook or a web browser. For IT, MOVEit Ad Hoc Transfer provides the comfort of knowing sensitive business files are being sent and received through a secure, enterprise-class Managed File Transfer system. Plus, the system relieves your email and storage systems from the burden of transferring and storing large files.

Risk Management

Is my sensitive data at risk?

Risk Management ensures continuous monitoring of the entire corporate network and generates lists of vulnerabilities and deep risk metrics prioritized by importance for the IT Security decision maker. To ensure that the vulnerabilities are in fact relevant and do exist in context for the organization, it is then critical to automate the penetration testing of each of the vulnerabilities so that the list can be narrowed down to what is truly important to look at right away. It is also crucial to automatically produce a visual network topology map in order to understand how vulnerabilities at the network level, due to security configuration not being compliant in some areas of the network, can affect other areas of the network. This enables organizations to create threat models to proactively understand where threats can come from. Finally, many modern threats today, whether they be internal or external, can impact the entire network stack, and require effective traffic visibility and network forensics capabilities.

Vulnerability Aggregation, Penetration Testing & Validation

coresecurity.com

Core Security is the leading provider of predictive security intelligence solutions for enterprises and government organizations. Built on the success of CORE Impact, the world's leading penetration testing tool, we help more than 1,400 customers worldwide proactively identify critical risks and match them to unique business objectives, operational processes and regulatory mandates. Core Security partners with a variety of complementary technology vendors to provide prebuilt integration and interoperability. Our patented, proven, award-winning enterprise solutions are backed by more than 15 years of applied expertise from CoreLabs, the company's innovative security research center.

Core Security : The Power of Thinking Ahead

As the leading provider of predictive security intelligence solutions, Core Security answers the call of organizations demanding a proactive approach to eliminating business risk. Our solutions empower customers to think ahead, take control of their security infrastructure and predict and prevent IT security threats.

Organizations have to predict security threats – not just react to them

Today, the majority of security spending is focused on solutions that take defensive or reactive approaches to threats. As a result, security teams are saddled with overwhelming amounts of disparate security data, tools that don't communicate and alerts that sound only after the damage has been done. Organizations that seek to survive and thrive must go on the offensive and predict and preempt threats before it's too late.

Core Insight Enterprise

- Enterprise-class predictive security intelligence platform
- Business risk identification, validation and prioritization
- Continuous threat simulation
- Continuous, proactive threat simulation
- Dashboard view of an organization's security risk profile
- Attack path discovery and remediation modeling

Core Impact Professional

- Automated, on-demand penetration testing
- Vulnerability validation from all leading scanners
- Multi-threat surface investigation
- Regulatory compliance verification

Vulnerability Management & Security Benchmarking

tripwire.com

Tripwire is the leading provider of Information Risk & Security Performance Management solutions to more than 6,500 businesses and government agencies worldwide. Tripwire solutions enable enterprises of all sizes to 1) automate compliance and reduce risk, and 2) measure and compare the performance of their IT security program with their own goals and industry peers.

Tripwire delivers an integrated and open solution connecting Tripwire and third-party security products to leverage all available information to protect IT assets and high value data. Tripwire offers the industry's first security performance management application for CISOs - that gives CISOs a metrics language to communicate their company's security performance just like the CFO describes financial performance. From Vulnerability Management to agentless compliance policy auditing and file integrity monitoring,

Tripwire provides best-in-class products for reducing information risk and aligning security strategies with business initiatives. Tripwire delivers solutions for your business' security and compliance needs – regardless of size or industry.

How Tripwire secures your organization:

- Configuration Policy Auditing shows compliance against internal or international policies/baselines and alerts on deviations
- Vulnerability Management prioritizes remediation of vulnerabilities across the entire technology stack
- File Integrity Monitoring warns on unauthorized changes
- Web Application Scanning finds flaws across your websites
- Security Performance Management consolidates and compares security metrics from your security solutions

Tripwire is headquartered in San Francisco, CA, with regional offices throughout the United States, London and Toronto.

Incident Response

Has my sensitive data been breached?

Incident Response involves the monitoring and detection of security events, and the execution of proper remediation. Breaches can be mitigated with real-time, dynamic threat protection across the different stages of the kill chain. To be prepared to respond to modern malware in real-time and disrupt adversary behavior, sandboxing, endpoint detection, and threat intelligence are critical to identify and block cyber threats. Simultaneously self-learning intelligence of network nodes and users, as well as, behavioral analytics on endpoints, enable the validation of emerging zero-day threats that bypass other security controls, by correlating this information in order to identify outliers that indicate in-progress attacks. Finally, effective investigation and analysis of intrusions gives organizations the ability to pinpoint the root cause, the scope of the breach, the data loss, and the steps required to contain the breach, and enhance the adaptive threat response process to achieve automation.

The Next-generation Cybersecurity Analytics

LINKSHADOW

linkshadow.com

LinkShadow is designed to manage threats in real-time with attacker behavioral analysis which is meant for organizations that are looking to enhance their defenses against advanced cyber-attacks, zero-day malware and ransomware, while simultaneously gaining rapid insight into the effectiveness of their existing security investments.

AttackScape Viewer

TrafficSense Visualizer

ThreatScore Quadrant

Identity Intelligence

Asset AutoDiscovery

BlockCount Ratio

Real-time Threat Intelligence

Recorded Future

recordedfuture.com

Recorded Future arms you with real-time threat intelligence so you can proactively defend your organization against cyber-attacks. With billions of indexed facts, and more added every day, our patented Web Intelligence Engine continuously analyzes the open Web to give you unmatched insight into emerging threats. Recorded Future helps protect four of the top five companies in the world.

Overview of your threat environment tailored to your organization and industry.

Why Recorded Future

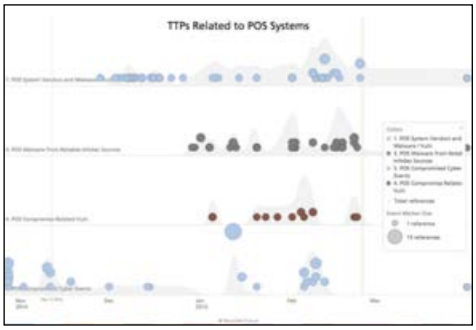
Faster Analysis:
Spend less time collecting data and supercharge your analytic capacity.

Cut the Middleman:
Direct access to billions of data points from the open, deep and dark Web for superior context.

Real-Time Monitoring:
Alerts to direct threats. Share live reports. Enrich your SIEM.

Relevant Intel:
Tailored to your environment, technology infrastructure, and corporate profile.

"Recorded Future gives us incredible context and insight into potential threats."
Dave Ockwell-Jenner, Sr. Manager, Security Threat & Operational Risk Mgmt., SITA



A timeline view enables analysts to visualize emerging trends for proactive security.

Customer Success Services

Customer Success Services

Customers implementing IT Security technologies depend on expert technical services and support professionals that understand the challenges being addressed and the business impact, and then provide action in a timely manner to achieve successful deployments.

StarLink Customer Success Services comprises of a highly skilled team of IT Security Consultants offering remote and onsite advanced technical services to customers via Channel Partners.

In order to ensure continued customer success, SCS also offers a centralized approach to provide simplified and preventive IT sustenance post project closure.

The SCS portfolio includes Security Consulting Services, 24x7 Technical Support, Certified Training Services, Managed Security Services, Security Outsourcing Engineering.