e92cloud

Automated, integrated visibility that's built for the cloud.

Defending the network has never been more challenging. The explosion of remote working alongside accelerated migration to cloud environments has left IT teams needing to redefine their network perimeter, and cover a wide variety of disparate environments while experiencing more data and alerts than ever before. The challenge of using that information to protect against an ever evolving threat is significant, let along turning the tide on the unknown attacker.

The demand to do more with less has never been greater – and the need to empower SOC teams is essential in turning defence into attack.

A new approach is needed, to move from a traditional defence model and utilise the intelligence and data that the network holds. Leveraging the next generation of tools that integrate, rather than simply adding point solutions as additional layers, this model provides the visibility that enables organisations to automate and accelerate detection and response.

92cloud

Cloud grows, activity grows, alerts grow

Cloud migration spending is growing at six times the pace of general IT spending. 3 out of 4 security teams agree their cloud infrastructures generate more security alerts than similar on-prem environments.

The reality is that legacy SIEM solutions weren't built to scale like that – and nor was the licencing.

The cloud offers the ability to scale IT on-demand, and that means more activity, alerts and threats your SIEM needs to manage too.

The attack surface has just exploded

Previously, the threat vector covered your network. Then devices, and spread to cloud apps.

When the network is in the cloud, that's the new attack surface.

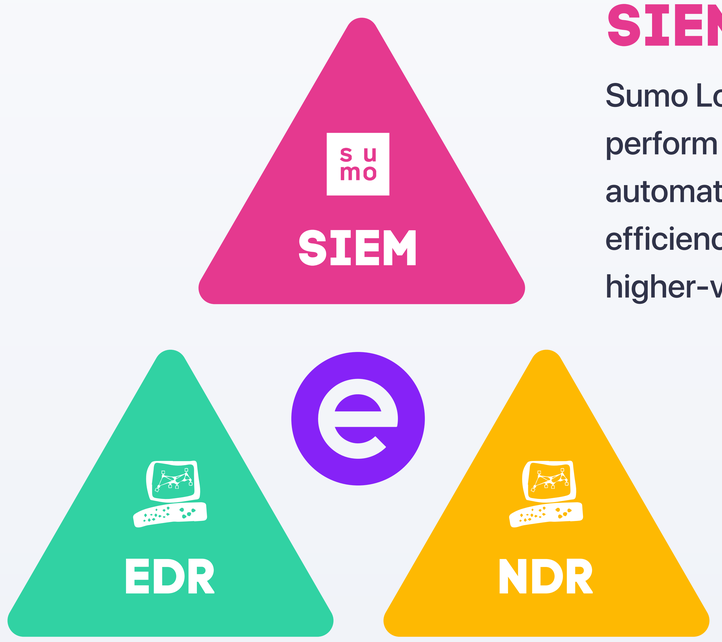
With apps, data and workloads now across private, public and hybrid cloud environments, your SIEM needs to cover a broader attack surface and range of sources than ever.

Too many alerts, too little time. Or analysts

83% of security teams report their staff experience alert fatigue and 75% determine they'd need to hire three or more analysts to conquer all their daily alerts.

But with the expanding volume of data from multiple sources, human resources can scale quickly enough. Manual identification, analysis and remediation can't stop the threats or protect the network.

The SOC Visibility Triad from e92cloud brings together the most advanced solutions from Check Point and Sumo Logic, with integrations that enable the SOC team to have complete visibility of their network.



SIEM

Sumo Logic fuses analytics and automation to perform security analyst workflows and automatically triage alerts—increasing human efficiencies and enabling analysts to focus on higher-value security functions.

EDR

Real-time response and remediation to threats at the endpoint, combined with malware protection

NDR

Deep insights and analysis into network traffic, to detect a breach or attack

e92cloud

Cloud-Native SIEM

SIEM is the foundation of the SOC Triad, providing the essential data and insights for organisations to build a cybersecurity strategy built data and intelligence. However organisations with legacy SIEM products, face common technology limitations that burden a SOC's efficiency and ability to mitigate risk.

Sumo Logic SIEM is cloud-native, and built to with elastic scalability to grow with your business. Covering on-premise, hybrid and multi-cloud deployments, it provides a single point of intelligence and actionable insights with data from wherever it sits, for total visibility.

The platform is created to support Security by Design – ensuring security is built in for DevSecOps, operations, data and application teams – while the AI and ML engines provide Continuous Intelligence to empower data-driven decisions and automating attack response.

- **Collect & centralize: More than 150 applications and integrations make it easy to aggregate data**
- **Search & investigate: Real-time analytics to detect and remediate attacks and breaches, reducing compliance costs**
- **Monitor And Visualize: Customizable dashboards align teams with data visualization for logs, metrics and performance**
- **Alert And Notify: Machine-learning algorithms work 24/7 with instant alerts**

2020 State of SecOps and Automation Report >

"cloud-native" vs. "cloud-based" PDF >

sumo logic

e92cloud

Automating Endpoint Security (EDR)

The endpoint remains the starting point for threat defences – typically 70% of cyber-attacks start on the endpoint. With the endpoint now very often the complex, distributed and diverse network edge, it's more important than ever to provide advanced threat protection.

EDR extends endpoint protection to an rated, layered approach to endpoint protection that combines real-time continuous monitoring and endpoint data analytics with rule-based automated response. It moves cybersecurity to a proactive state, identify threats and automating remediation before the point or attack or compromise, and providing essential insights to the SIEM, enabling advance warning of an attack or breach.

Check Point Sandblast Agent enables organisations to automatically triage potentially suspicious or malicious events, helping the SOC team prioritise their time. In turn, this supports more proactive threat hunting, sometimes even on security incidents normally blocked so that potential intrusions or Indicators of Compromise (IOCs) can be identified. Finally, the Sandblast Agent EDR can provide comprehensive data to enable the SIEM to provide more intelligent, actionable insights about potential threats.

- **Improved Visibility, through continuous data collection and analytics to provide full visibility of the endpoint**
- **Rapid Investigations, to provide essential context and accelerate remediation**
- **Remediation Automation based on defined rules or playbooks for incident response, reducing the load on analyst**
- **Contextualized Threat Hunting, using deep visibility to investigate potential infections before the attack starts or propogates**

SandBlast Agent PDF >

5 Must-Have Endpoint Protections Video >

Check Point
SOFTWARE TECHNOLOGIES LTD

e92cloud

Zero Day Protection for the Network, Now (NDR)

Every day, over 8,000 new cyber threats are discovered – from zero day exploits to social engineering attacks. Yet still the prevalent approach of network defence is to protect + defend – when the likelihood is that no one is unbreachable, and traditional solutions will only identify half of those new threats.

NDR provides a new approach, focusing on detecting threats and attacks and then being able to accelerate the detection, response and remediation to stop the attack before it's started. Integrating with SIEM and complimenting EDR at the endpoint, NDR provides autonomous threat management that ends routine maintenance and manual intervention or configuration.

Check Point Sandblast Network provides the most advanced zero-day protection, powered by the most advanced threat intelligence and AI to detect unknown threats before they execute. It's built to deliver real-time prevention, and pre-empts users through eliminating threats regardless of activity of behaviour.

Check Point
SOFTWARE TECHNOLOGIES LTD

- **Best Zero-Day Prevention: Powerful threat intelligence and AI technologies prevent unknown cyber threats**
- **Streamlined Security Management: Single click setup, with out-of-the-box profiles optimized for business needs**
- **Seamless Productivity: Delivering a prevention-first strategy with no impact on user experience**

Cyber Security in the Age of Coronavirus PDF >