LOGPOINT

INSIDER THREAT

The cyberthreat landscape is continuously evolving, so companies don't only have to look outside their walls to find threats, sometimes they are already inside. And whether they are result of intentional, accidental or malicious actions, the misuse of authorized access poses a big menace to organizations. By spotting behavior that deviates from the standard baseline, analyst usually detect these insider threats. But this is task is almost impossible to accomplish using only human means. With Logpoint UEBA, you can easily detect suspicious user behavior and other entities such as applications, networks and external threats across all data sources in your network. Fully integrated with Converged SIEM, Logpoint UEBA provides unparalleled time-to-value for your business, along with reducing investigation and response time.

About UEBA

Advanced attacks and pervasive threats to your organization often rely on compromised credentials or coercing users into performing actions that damage enterprise security. To identify these types of attacks, you need a powerful solution that allows analysts to quickly determine normal versus abnormal activity on your network. Unfortunately, the cybersecurity tools and the attack detection mechanism are becoming obsolete, as attackers are able to bypass the perimeter defense used by many companies.

These types of security incidents are costly. The average cost of a data breach is close to $4 million or even higher in sensitive industries such as healthcare or finance. On top of the costs associated to the data breach, organizations often also have to face different legal fees and the cost related to restoring the company's reputation.

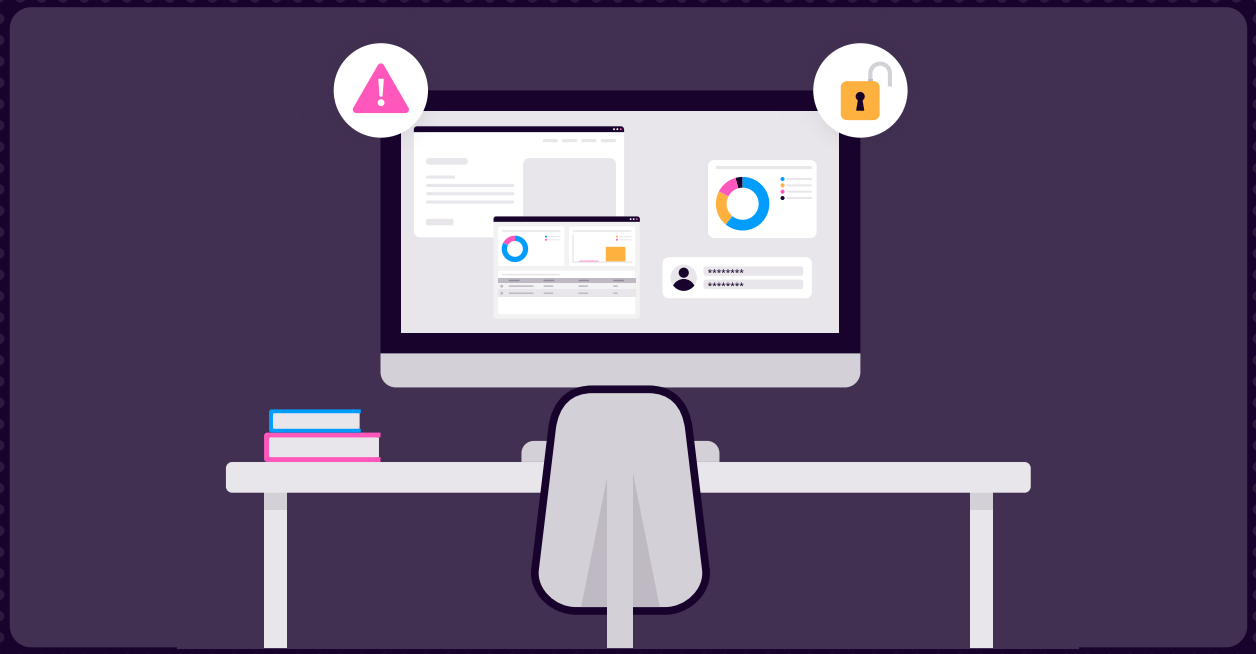
UEBA, short for User and Entity Behavior Analytics is a security process focusing on monitoring both suspicious user behavior as well as other entities such as cloud, mobile or on-premise applications, networks and external threats. Without behavior analytics, SOC teams need to create complicated, preset rules to define what is normal, abnormal and permitted. Using machine learning, Logpoint UEBA builds organization-specific baselines for normal behavior for each user and entity in the network. By evaluating activity against these baselines, UEBA detects any unusual behavior and frees up time for security analysts to focus on finding real threats.

Logpoint's UEBA module has industry leading time to value for customers, allowing same-day, zero-professional service deployments and immediate insights. This is possible since the UEBA engine benefits from being built on top of the most flexible and scalable SIEM solution on the market. This white paper focuses on highlighting how UEBA extends your SIEM's Threat Hunting capabilities.

Insider threats or user-based threats are threats originating from users inside your organization such as current or past employees or outside contractors. Although not all users trigger the attack vectors knowingly, they are still one of the main failing point in a security team's fight against cyber attacks. When it comes to user-based threats, we distinguish threats caused by users knowingly triggering the attack vectors and threats caused by users unknowingly triggering the attack vectors. In the first case, the attack can be initiated by the user itself, or by an outside attacker. In the latter case, they are initiated by an outside attacker luring the user to click a link or download a file. Here we can talk about phishing attacks or spear phishing attacks depending on whether the event is generic or specific.

When it comes to defending your organization against insider threats, there are two important defense mechanisms to consider: Rule based approach and Model based approach. The first is a traditional approach where logs are evaluated against a set of pre-defined rules based on historical data. As any change in the attack type requires re-writing the rules, one might easily see why a rule-based approach is becoming obsolete, especially when dealing with large volumes of data.

A model-based approach is on the other hand a probabilistic approach where threat models are mapped to the MITRE ATT&CK framework. A new event is considered risky if it deviates from the entity or its peer group. The strength of a model-based approach against a rule-based approach is that models can be automatically adjusted in case of any change of behavior.



Did you know?

More than half of organizations have experienced an insider threat in the last year, and 8% have experienced more than 20. And 74% of organizations say insider attacks have become more frequent, and admit they are at least moderately vulnerable or worse to insider threats.

Cybersecurity Insider: 2023 Insider Threat Report [Gurucul]

The Power of SIEM, SOAR and UEBA

The rules- and thresholds-based approach of most SIEM vendors and other existing security tools produces too many false positives and a flood of alerts. When a SIEM solution, enhanced with top-notch security analytics, supports analysts in threat hunting, time spent on eliminating false positives is drastically decreased, empowering your team to focus on threats which really matter. Having SIEM as a data source supported by security analytics not only provides a more valuable than ever pool of log data, but it also enables your SOC team to work smarter, not harder by cutting the detection and response time in half. UEBA easily connects to Logpoint's Converged SIEM platform through a plugin.

As a result, there is no need to do any mapping or customization which lowers time to value dramatically. The deployment architecture is easily scalable for increasing the number of entities and data volume. Our common taxonomy readily gives access to over 400 machine learning models for all devices. Detected anomalies are used as enrichment sources. Since logs and raw logs can easily be investigated based on the detected anomalies, investigation and forensics can take place immediately.

By leveraging ML and big-data analytics capabilities, built on Logpoint's unique one taxonomy, UEBA creates baselines for every entity in the network, without following predefined rules or signatures. By evaluating activity against these baselines, UEBA detects any unusual behavior and frees up time for security analysts to focus on finding real threats and defining rules. With UEBA, suspicious user behavior can be detected in the cloud, on-premise and inside business applications - out of the box.

But the ultimate difference will unfold once you start viewing the information with dashboards in the Converged SIEM platform by leveraging the UEBA analytics through alerts and risk scores. Outputs from the UEBA module can be correlated with original and non-UEBA SIEM events, making the original events more insightful than ever. With Logpoint's Converged SIEM, you can statically or dynamically enrich the original log data using the information from the Machine Learning technology and thus, discover suspicious user behavior in the SIEM.

The high-risk activities along with contextual information are then presented to the analyst for further investigation using the Logpoint alerts to enable faster and more informed decisions. Incidents can be visualised using dashboards and search templates for validation. The advanced analytics allows your cybersecurity team to work smarter by accelerating detection and response to threats without increasing the workload of your security analysts.

Sounds good, but is my data safe?

UEBA is delivered as a service which means that the identification of anomalies takes place in Logpoint operated and hosted servers.

For your added security, data is encrypted before it leaves your network. The encryption key stays within your network and no clear-text data is ever visible to Logpoint staff. Any key value pair leaving the network is encrypted and all processing takes place on encrypted values. The system may observe an abnormal access pattern but it will not be able to identify the true identity behind the user.

The observation is sent back to your Logpoint server and decrypted - ultimately revealing the identity to your analysts and no one else.

Powered by SOAR, the investigation and response of user anomalies can be done automatically through out-of-the-box playbooks, saving time and effort to analysts. Whenever an alert is raised due to suspicious activity, the SIEM creates an incident, triggering the launch of a playbook. The playbook will run the first queries, extract all the necessary data, and investigate both the alert and user. SOAR will take care of triaging the alert and respond in case of an actual threat. It can even manage whitelists for the entire detection process of user anomalies.

Wide coverage of use cases

Common taxonomy readily gives access to over 400 machine learning models for all devices. Even better, if historical logs are available, baselining can start immediately.

Prevent Insider Threats With UEBA

Key User And Entity Based Threat Use Cases

1. **Account compromise**

   Stop unauthorized account usage by anyone other than the account holder. This way you will never have to worry about your executives getting spearfished by outsiders attempting to infiltrate your organization.

2. **Account misuse**

   Monitor how your employees behave in your system and detect any unauthorized account usage by an account holder.

3. **Internal reconnaissance**

   Gather evidence on your network resource to be alerted if any of them are behaving differently than expected.

4. **Infected host**

   Stop attackers from gaining information about targeted computers or networks that can be used as a preliminary step toward a further attack seeking to exploit the target system.

5. **Lateral movement**

   Restrict unauthorized movement within your environment. With UEBA common lateral movement methods can be easily detected.

6. **Insider fraud**

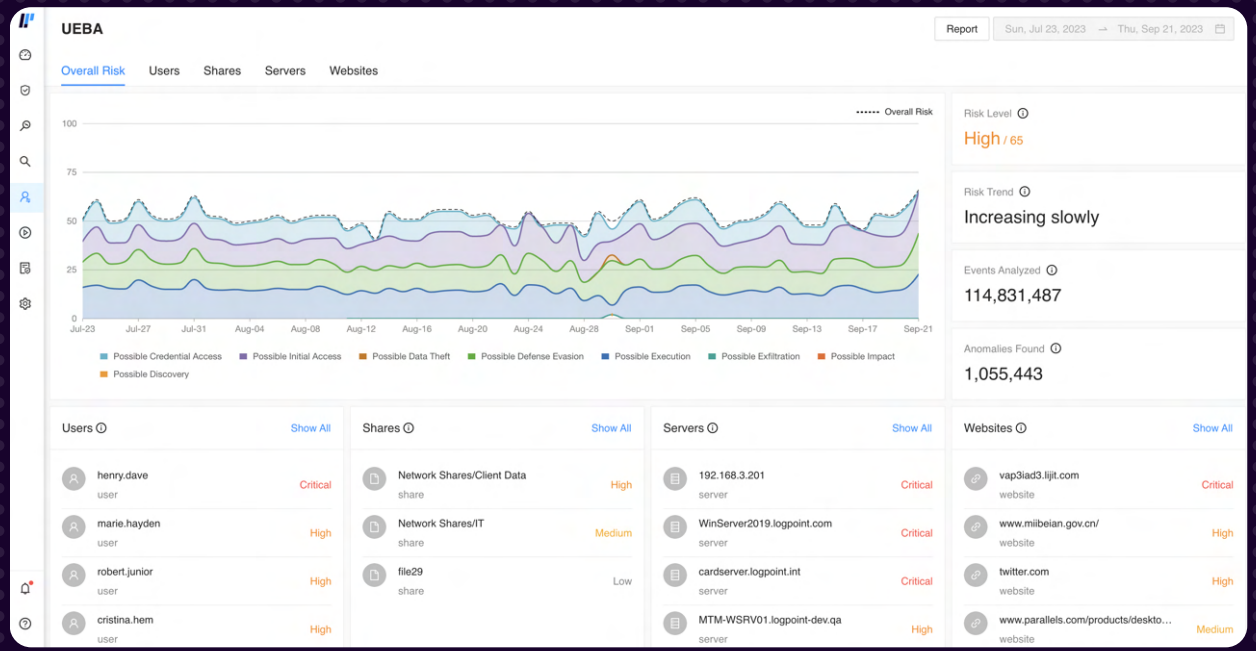
   Prevent professional attackers, insiders, or customers from illegally acquiring assets such as money for personal use or profit.

7. **Data staging/ data exfiltration**

   Get real-time alerts about unauthorized data transfers within your network. Whether the transfer is manual or carried out by someone with physical access to a computer or is automated.

Faster Implementation

Get up and running faster with Converged SIEM with UEBA. Without the need to tune and tweak static detection rules, it is faster to setup a Logpoint Converged SIEM instance.



The Overview page:

This gives you on overview of the level of risk your organisation is exposed to. This is a good place to get a general overview of your current risky entities and to start an investigation if any of your users or entities are showing an increased risk score

Scenario: An Example Of How UEBA Can Empower You To Detect Insider Threats In Your Organization

After finding out that their contract will be terminated, an infuriated admin in your organization decides to engage in an insider attack against your organization to retaliate. To do so, they decide to create a new user account and log in to one of the organization's cloud storage solutions.

1. **Credential access**

   The detector that identifies the accounts with a long period of no previous activity fires an anomaly based on how this account has not previously been seen on the network.

2. **Credential access**

   The newly created user has no previous login attempts. Therefore, the detector fires an anomaly that is based on a sudden increase in login attempts per hour compared to the user itself.

3. **Collection**

   The newly created account then attempts to access the cloud resource. This information is received by a detector aimed at detecting the first time a user accesses a repository. As the user is completely new, the only files that they have accessed are most likely local and limited to their specific role, so the attempt at accessing a specific, remote cloud enabled directory immediately fires off an anomaly and raises the user's risk score.

4. **Collection**

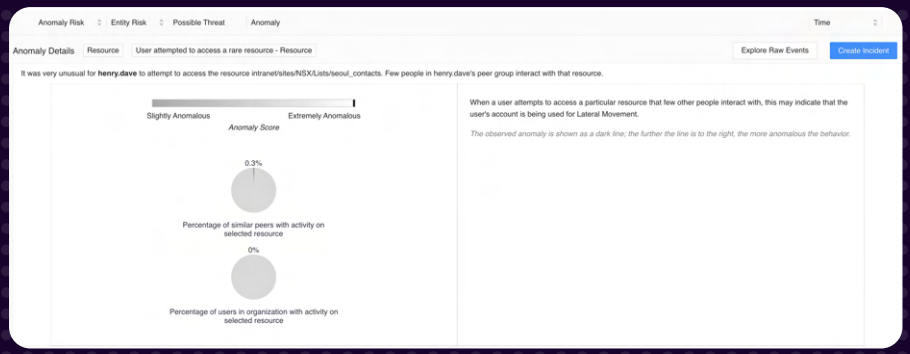
   As the malicious insider accesses the files that they would like to exfiltrate, they inevitably access many, if not all of the files for the first time. The dedicated UEBA module instantly detects that the newly created user had accessed information in the R&D repository and copied 17 files oneby- one to different newly created folders within an hour. Knowing that these actions differ a great deal from the normal business behaviors in the organization, Logpoint UEBA further elevates the user's risk score.

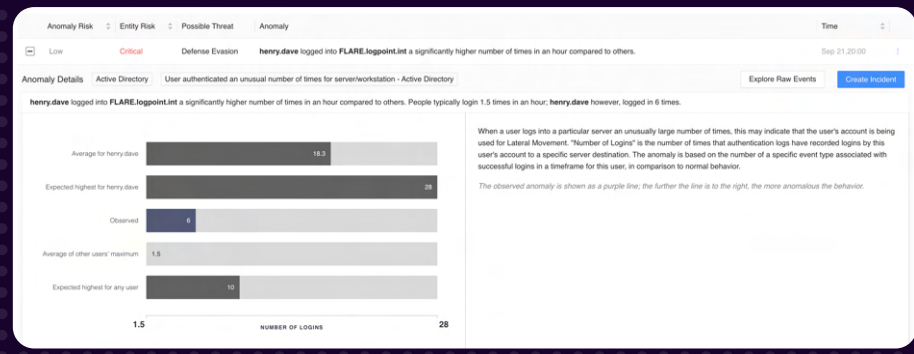
5. **Collection**

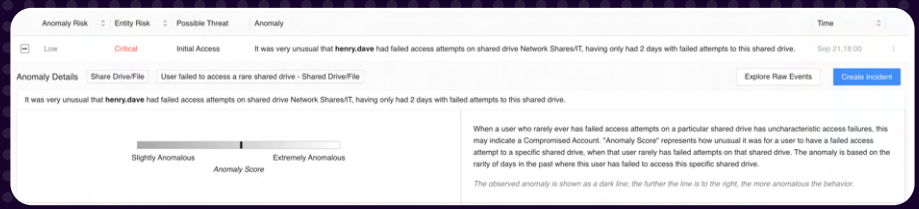
   The employee then decides to finally move the files they have staged for exfiltration to a final pre-exfiltration location. This information is received by the detector aimed at detecting unusual amounts of data uploaded by the user. There is a matching detector that also aims to recognize unusual download amounts and it is likely that both would be activated

Strengthen your security posture

The use of user behavior monitoring is accelerating; 94% of organizations deploy some method of monitoring and 93% monitor access to sensitive data.

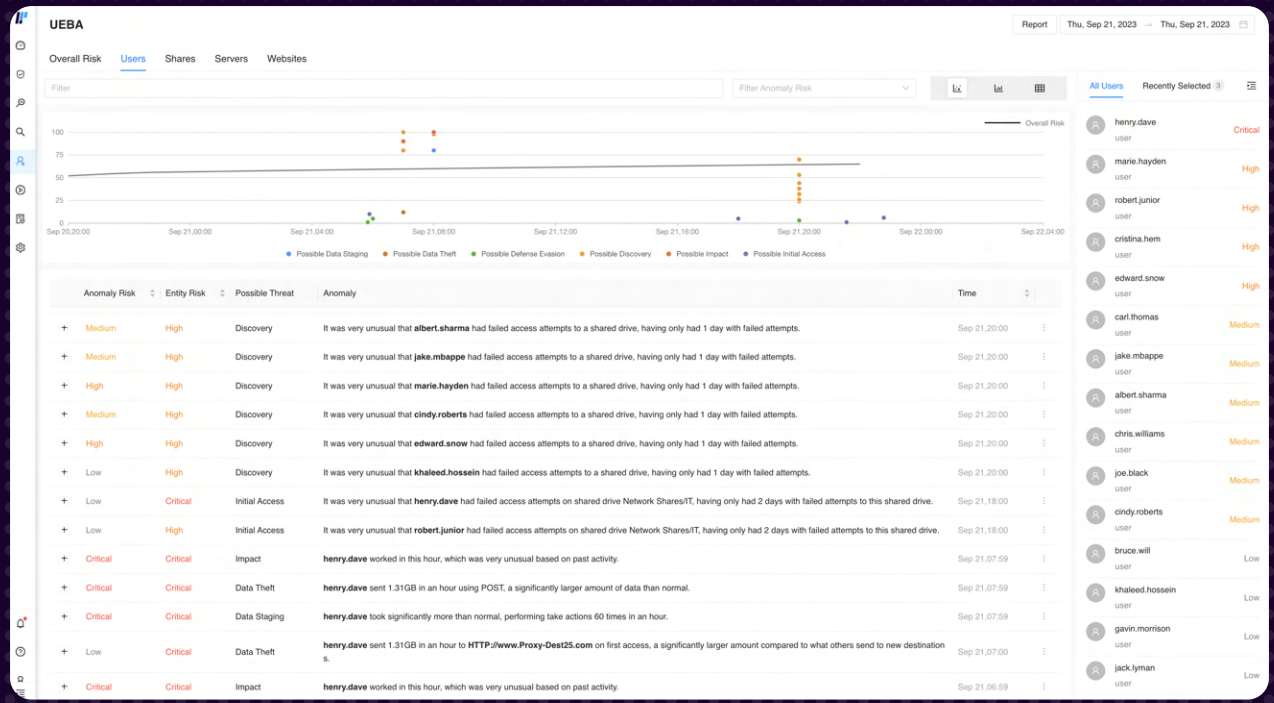






Context on unusual user behavior

By further investigation, the UEBA module provides your analyst with detailed context on why the user's behavior is highly unusual based on their individual baseline and peer behavior.



Risk behavior timeline

With Logpoint, you can easily filter out the events causing the increased risk score, along with the number of events arranged into a transparent timeline of risky behavio

Scenario: An Example Of How UEBA Can Empower You To Detect Insider Threats In Your Organization

After finding out that their contract will be terminated, an infuriated admin in your organization decides to engage in an insider attack against your organization to retaliate. To do so, they decide to create a new user account and log in to one of the organization's cloud storage solutions.

6. Exfiltration

The movement of files can also bedetected by a detector looking at data movement towards various domains and detecting irregular ones, based on both the user's and the organization's previous activities. Not only can this identify unusual traffic internally, but also the movement of data to an external location

7. Exfiltration

Finally, the malicious soon-to-beformer employee attempts to email the zip files containing the sensitive data. This action triggers a final tranche of detectors, the ones that detect unusual email destination and unusual email attachment size.

Summary

If malicious employees attempt to jeopardize the integrity of your organization in a similar manner, Logpoint UEBA can lend you significant assistance in detecting, tracking, and documenting every stage of the attack no matter at what point of the ATT&CK framework the attacker happens to be. Investigation can start as soon as UEBA detects the initial anomalous user creation. Even in this stage, it's possible to stop the attack by singling out the account and confirming whether its creation conforms to the policies. In the following stages, it is simple for an analyst to identify unusual behavior based on the anomaly. Finally, even if the attacker has already succeeded in damaging the organization, it's still possible to mitigate due to the awareness of timing, method, and entities involved that Logpoint UEBA provides

UEBA Platform as a service

Logpoint UEBA is uniquely available as a service, thus removing unnecessary hassles for hardware and deployment.

Summary

If malicious employees would attempt to jeopardize the integrity of your organization in a similar manner, Logpoint UEBA would help you detect and catch the insider attack in the very first stages so that you can take counter measures immediately. Investigation can start as soon as UEBA detects the Possible redential Access (to be aligned with the new example). To combat the risk, your analysts can quickly start incident response by deactivating the user, and any other measures outlined in the reponse manual. You can similarly analyze the potential threats in every stage of the attack and perform defensive actions based on what the situation requires.

Conclusion

With Logpoint UEBA, you can easily detect both suspicious user behavior as well as other entities such as cloud, mobile or on-premise applications, networks and external threats – out of the box.

Logpoint UEBA analytics' high fidelity threat scoring can reduce the time to respond to attacks, placing the advantage of time back into your hands. By taking advantage of advanced Machine Learning we enable your security teams to identify unusual patterns and act before the infrastructure is compromised.

Unlike any other UEBA solution, the Logpoint UEBA module will work instantly across all supported data sources in your network. There is no need for time-consuming and expensive integrations, and our UEBA module will provide unparalleled time-to-value for your business, along with vastly cutting the investigation time by your security team

Leveraging Logpoint's user centric approach, with licensing on Logpoint UEBA, you can pick and choose the most important users and entities in your organization, so you only monitor where it really matters.

Automated threat detection:

Utilizing machine learning and behavioral analytics can counter the shortage of experienced Cyber Security analysts and optimize the use of your existing resources.

Reduce risk:

Compromised user accounts are the keys to the kingdom resulting in the most damage from any breach, early detection of a compromised user and/or credentials is essential in mitigating risk and data loss.

Reduced mean time to respond:

Logpoint UEBA analytics high fidelity threat scoring can reduce the mean time to respond to attacks, placing the advantage of time back into your hands.

About Logpoint

Logpoint is the creator of a reliable, innovative cybersecurity operations platform — empowering organizations worldwide to thrive in a world of evolving threats. By combining sophisticated technology and a profound understanding of customer challenges, Logpoint bolsters security teams' capabilities while helping them combat current and future threats. Logpoint offers SIEM, SOAR, UEBA, SAP security, and EDR capabilities in a complete platform that efficiently detects threats, minimizes false positives, autonomously prioritizes risks, responds to incidents, and much more. Headquartered in Copenhagen, Denmark, with offices around the world, Logpoint is a multinational, multicultural, and inclusive company. For more information, visit logpoint.com

Contact Logpoint

If you have any questions or want to learn more about Logpoint and Converged SIEM, our security operations platform, don't hesitate to contact us at logpoint.com/en/contact

Book a demo and talk to an expert

We will show you around, hear more about your needs and requirements, and discuss how Logpoint can add value to your organization.

Book a demo

LOGPOINT

LOGPOINT.COM